2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?

Uchenna Jerome Orji
African Centre for Cyber Law and Cybercrime Prevention (ACCP)
Kampala, Uganda
jeromuch@yahoo.com

Abstract: Within the past decade, Africa has witnessed a phenomenal growth in Internet penetration and the use of Information Communications Technologies (ICTs). However, the spread of ICTs and Internet penetration has also raised concerns about cyber security at regional and sub-regional governance forums. This has led African intergovernmental organizations to develop legal frameworks for cyber security. At the sub-regional level, the Economic Community of West African States (ECOWAS) has adopted a Directive on Cybercrime, while the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have adopted model laws. At the regional level, the African Union (AU) has adopted a Convention on Cyber Security and Personal Data Protection. This paper seeks to examine these legal instruments with a view to determining whether they provide adequate frameworks for mutual assistance and international cooperation on cyber security and cyber crime control.

The paper will argue that the AU Convention on Cyber Security and Personal Data Protection does not provide an adequate framework for mutual assistance and international cooperation amongst African States and that this state of affairs may limit and fragment international cooperation and mutual assistance along sub-regional lines or bilateral arrangements. It will recommend the development of international cooperation and mutual assistance mechanisms within the framework of the AU and also make a case for the establishment of a regional Computer Emergency Response Team to enhance cooperation as well as the coordination of responses to cyber security incidents.

Keywords: *African Union, Computer Emergency Response Teams, dual criminality, Mutual Legal Assistance*

1. INTRODUCTION

Since the beginning of the 21st century, Africa has continued to witness a phenomenal growth in Internet penetration and the use of ICTs. Statistical data indicates that Internet users in Africa grew from 4,514,400 million people in 2000 to 297,885,898 million people in June 2014.[1] This phenomenal growth which is still in progress[2], has been linked to factors such as the liberalization of the telecommunications market in African States, the widespread availability of mobile technologies, and the increasing availability of broadband systems.[3] However, the spread of ICTs and Internet penetration in African states has also raised concerns about cyber security at regional and sub-regional governance forums. Consequently, some African intergovernmental organizations have developed legal frameworks for cyber security. At the sub-regional level, the Economic Community of West African States (ECOWAS) adopted a Directive on Fighting Cybercrime in August 2011, while the Common Market for Eastern and Southern Africa (COMESA) adopted a Model Cybercrime Law in October 2011. The Southern African Development Community (SADC) also adopted a Model Law on Computer Crime and Cybercrime in March 2012. At the regional level, the African Union (AU) has adopted the AU Convention on Cyber Security and Personal Data Protection in June 2014. Already, some African States have established national legal and policy frameworks for cyber security, while many others are developing such frameworks. However, a discussion of national cyber security initiatives is beyond the scope of this paper.[4] This paper seeks to examine Africa's regional and sub-regional legal frameworks on cyber security with a view to determining whether they can provide a basis for mutual assistance and effective international cooperation in the control of cyber crime and promotion of cyber security.

The paper will argue that the AU Convention on Cyber Security and Personal Data Protection does not provide an adequate legal framework for mutual assistance and international cooperation amongst African States and that this state of affairs may limit and fragment international cooperation and mutual assistance along sub-regional lines or bilateral arrangements. It will recommend the development of international cooperation and mutual legal assistance mechanisms within the framework of the AU and also make a case for the establishment of a regional Computer Emergency Response Team to enhance cooperation in the coordination of responses to cyber security incidents.

The paper is divided into five sections. The first section which includes this introduction will provide an overview of the concepts of cyber security, and international cooperation and also present a general background on Africa. The second section will critically examine the AU Convention on Cyber Security and Personal Data Protection to determine whether it provides an adequate framework for mutual assistance and international cooperation amongst African States, while also comparing the Convention with the Council of Europe Convention on Cybercrime. The third section will examine sub-regional cyber security frameworks such as the ECOWAS Directive on Fighting Cybercrime, the COMESA Model Cybercrime Bill and the

1 *See* Miniwatts Marketing Group, "Internet Usage and Population Statistics for Africa", (June 30, 2014), available at <http://www.internetworldstats.com/stats1.htm>.

2 *See* ITU Telecommunication Development Bureau, *The World in 2014 –ICT Facts And Figures*, available at <http://www.itu.int/en/ITU-D/Statistics/Documents/ICTFactsFigures2014-e.pdf>.

3 *See* GSMA, *The Mobile Economy Report 2013* (A.T. Kearney: London, United Kingdom, 2013) p.16.

4 For a discussion of cyber security initiatives in African States, *see* Uchenna Jerome Orji, *Cybersecurity Law and Regulation* (Wolf Legal Publishers: Netherlands, 2012) pp.401-485.

SADC Model Law on Computer Crime and Cybercrime to determine whether they also provide a framework for mutual assistance and international cooperation amongst Member States. The fourth section will propose both legal and other governance measures to strengthen mutual assistance and international cooperation on cyber security amongst African States, while the fifth section concludes the paper.

1.2. An Overview of Basic Concepts

1) Cyber Security

Cyber security is an information age terminology that was derived by merging the prefix – "cyber" with the concept of "security". The term is defined as "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assets".[5] Cyber security governance measures include technical, organizational, policy, and legal aspects.[6] The technical aspects of cyber security governance deal with the development and implementation of technical protection measures for computer systems and network infrastructure, while the organizational aspects deal with the development of institutional capacities to promote cyber security such as the establishment of law enforcement organizations as well as the development of institutional capacities such as the establishment of Computer Emergency Response Teams (CERTs) to provide critical services such as prevention and early warning, detection and management of cyber security incidents.

On the other hand, the legal aspects of cyber security governance deal with legal measures that aim to promote cyber security. Legal measures are usually considered as probably the most relevant aspect of cyber crime control.[7] Such measures include the establishment of laws prohibiting acts that violate the security or integrity or availability of computer data and systems or networks and attacks against critical information infrastructure. It also includes measures to facilitate cross-border cooperation on cyber security with respect to the prevention, investigation and prosecution of prohibited acts. The scope of cyber security laws may also extend to the criminalization of acts that do not affect the security of computers or data or networked information infrastructure such as online child pornography or online xenophobia[8]. Malicious acts that are prohibited by cyber security laws are commonly referred to as "cyber crime" or "computer crime". These terms are often used interchangeably to refer to instances where computer technologies are the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. However, there is no universally accepted legal definition of cyber crime or computer crime[9] and cyber security laws generally tend to avoid such explicit definitions.[10]

5 *See* ITU High Level Experts Group [HLEG] *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report* (ITU: Geneva, 2008), p.27. See Uchenna Jerome Orji, Cybersecurity Law and Regulation, at pp.10-16.

6 *See* Uchenna Jerome Orji, *Id*., at pp.17-42.

7 *See* Gercke Marco, *Understanding Cybercrime: A Guide for Developing Countries* (ITU: Geneva, 2009) p.84.

8 However, some countries regard the criminalization of the online dissemination of xenophobic materials as an impediment to free speech. *See* Kristin Archick "Cybercrime: The Council of Europe Convention", *CRS Report for Congress*, (September 28, 2006) p.3.

9 *See* Uchenna Jerome Orji, *Cybersecurity Law and Regulation*, pp.17-19.

10 *See* for *e.g.*, The African Union Convention on Cyber Security and Data Protection (Malabo, 2014) and the Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

2) International Cooperation

International cooperation implies the voluntary coordinated action of two or more countries occurring under a legal regime and serving a specific objective.[11] Within the context of cyber security, the concept broadly covers issues such as extradition and mutual legal assistance as well as general measures to ensure cross-border cooperation on cyber security issues. Such measures also include the sharing of information and resources either within a bilateral or multilateral framework with the aim of facilitating efficient responses to cyber threats.

3) Background on Africa

Africa comprises of 55 sovereign states and it is classified as the world's second largest and second most populous continent after Asia, with a terrestrial mass of 30, 2044, 049 million square kilometers and a human population of over one billion people.[12] The continent has five geographical sub-regions, comprising of: Southern Africa, Central Africa, East Africa, North Africa, and West Africa. The AU is the most prominent regional intergovernmental organization that unites African States and it comprises of 54 sovereign States with Morocco being the only sovereign State that is not a member of the union.[13] Some notable intergovernmental organizations that operate within Africa's sub-regions include: the COMESA[14] which comprises of 19 Member States, the ECOWAS[15] which comprises of 15 Member States, and the SADC[16] which comprises of 15 Member States.

2. THE AU CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION

The AU commenced the development of regulatory initiatives on cyber security towards the end of the last decade. A major factor that might have caused the AU's late development of cyber security initiatives could be traced to the low penetration of ICTs in Africa prior to the widespread proliferation of wireless technologies within the last decade. One of the first AU statements on the need to promote cyber security is found in the *AU Draft Report on a Study of the Harmonization of Telecommunication, and Information Communication Technology Policies and Regulation (2008)*.[17] The Report noted *inter alia* that emerging questions that needed to be addressed in the converged ICT environment include the "tracing and combating of cyber crime in all its forms (hacking, virus propagation, denial of service attacks, credit card fraud, etc)".[18] The Report also emphasized the need for the establishment of a harmonized regional policy and regulatory framework on cyber security.[19] Subsequently, 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

11 *See The Blacks Law Dictionary* (8th Edition: West Group, 2004) p.359.
12 *See* Matt Rosenberg, "Continents Ranked by Area and Population", <http://geography.about.com/od/lists/a/large.continent.htm>.[Accessed 25/03/2015]
13 <http://www.an.int/en/member_states/country profiles>.
14 <http://www.comesa.int/>.
15 <http://www.ecowas.int/>.
16 <http://www.sadc.int/>.
17 *See* 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).
18 *Id.*, p.49.
19 *Id.*, p.75.

adopted a set of declarations known as the *Oliver Tambo Declaration*[20]. The Declaration directed the AU to "jointly develop with the United Nations Economic Commission for Africa (UNECA), 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, cyber security, and personal data protection"[21]. It also recommended that AU Member States should adopt the Convention by 2012.[22]

In 2011, the efforts of the AU and UNECA led the development of a draft framework on cyber security known as the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa.[23] The Draft Convention was subsequently adopted by the AU Expert Group on Cybersecurity in September 2012.[24] This was also followed by its approval by the 22nd Ordinary session of the AU Executive Council in January 2013. After that the Convention was to be presented for legal validation by the AU Justice Ministers conference in October, 2013,[25] after which it was to be presented for adoption by the AU Summit in January 2014 and opened for signatures and ratification by AU Member States. However, the Draft Convention could not be presented for the AU's adoption in January 2014 as a result of technical delays[26] and also due to opposition from the civil society and the academia. Several petitions by civil society groups and members of the academia were forwarded to the AU Commission to prevent the adoption of the Draft Convention following concerns that some of its provisions may harm the right to privacy and freedom of expression.[27] Other concerns included lack of wide consultations[28] and the absence of some critical governance mechanisms[29]. The Center for Intellectual Property and Information Technology Law (CIPIT) at the Strathmore University, Kenya led the opposition to the Draft Convention and also established an online petition to prevent its ratification.[30] Following these developments the Information Society Division of the AU Commission gave further room for the consideration of those concerns till May, 2014.[31]

20 *See* Extra-Ordinary Conference of AU Ministers in Charge of Communication and Information Technologies, *Oliver Tambo Declaration* (Africa Union: Johannesburg, South Africa, 2-5 November, 2009).

21 *See, Oliver Tambo Declaration*, p.4.

22 *Id*.

23 *See* Draft African Union (AU) Convention on the Establishment of a Credible Legal Framework for Cybersecurity in Africa, AU Draft0 010111, Version 01/01.2011.

24 *See* 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>. [Accessed 25/03/2015].

25 *See* 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> [Accessed 25/03/2015].

26 *See* Craig Rosewarne and Adedoyin Odunfa, *The 2014 Nigerian Cyber Threat Barometer Report* (Wolfpack Information Risk and Digital Jewels: South Africa and Nigeria, April 2014) p.40.

27 *See* Gareth Van Zyl, "Adoption of 'flawed' AU Cybersecurity Convention Postponed", IT Web Africa, (21 January 2014), available at <http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed> [Accessed 25/03/2015].

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> [Accessed 25/03/2015].

29 *See* Uchenna Jerome Orji, "A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity", *Communications Law: The Journal of Computer, Media and Telecommunications Law*, (2012) Vol. 17, No.4, pp.128-130.

30 The CIPIT's online petition is titled: *Stop the ratification of the African Union Convention on Cybersecurity*, available at<http://www.thepetitionsite.com/takection/262/148/817/>. *See also* Gareth Van Zyl, "Kenyan bid to stop 'flawed' AU Cybersecurity Convention", IT Web Africa (28 October 2013), available at<http://www.itwebafrica.com/security/513-africa/231821-keyan-bid-to-stop-flawed-au-cybersecurity-convention> [Accessed 25/03/2015].

31 *See* Craig Rosewarne and Adedoyin Odunfa, *The 2014 Nigerian Cyber Threat Barometer Report*, p.40.

Later on 27th June 2014, the AU Heads of State and Government adopted a revised version of the draft Convention during the 23rd Ordinary Session of the AU Assembly in Malabo. The Convention which is known as the AU Convention on Cyber Security and Personal Data Protection[32] aims to harmonize the laws of African States on electronic commerce, data protection, cyber security promotion and cyber crime control. The Convention recognizes that cyber crime "constitutes a real threat to the security of computer networks and the development of the Information Society in Africa".[33] To a great extent, the Convention adopts a holistic approach to cyber security governance by imposing obligations on Member States to establish national legal, policy and institutional governance mechanisms on cyber security. This approach apparently goes beyond that of the Council of Europe Convention on Cybercrime which focuses on the criminalization of cyber crimes and the establishment of procedural mechanisms for law enforcement and international cooperation.[34]

A. International Cooperation within the Framework of the AU Cyber Security Convention

Article 28 of the AU Cyber Security Convention establishes some provisions to facilitate international cooperation on cyber security.[35] It also requires AU Member States to make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) for the purpose of promoting cyber security and tackling cyber threats.[36] However, the extent to which the provisions of Article 28 can facilitate cooperation and mutual assistance amongst AU Member States appears to be limited. The Convention emphasizes the need for States to adopt the principle of double criminality (dual criminality)[37] when rendering cross-border assistance on cyber security issues without creating any mechanisms for Member States to fulfill extradition and mutual assistance requests in the absence of an extradition treaty or mutual assistance arrangement on the basis of dual criminality. Thus, Article 28: 1 of the Convention provides that: "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*".[38] The application of the double criminality principle is also emphasized in Article 28: 2 of the Convention which provides that:

> "State parties that do not have agreements on mutual assistance in cyber-crime *shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal*

32 *See* African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014). [Hereafter AU Convention on Cyber Security].

33 *See* Preamble, AU Convention on Cyber Security.

34 *See* Uchenna Jerome Orji, "Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection", *Computer Law Review International*, (October, 2014), Issue 5, pp.131-132.

35 *See* Article 28 AU Convention on Cyber Security.

36 *See* Article 28: 4, AU Convention on Cyber Security.

37 "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.

38 *See* Article 28: 1, AU Convention on Cyber Security.

> *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".[39]

Thus, the Convention appears to establish a blanket requirement for the application of the double criminality principle between Member States, without creating a legal basis or framework on which States while relying on the principle can base their extradition or mutual legal assistance requests in the absence of an existing international agreement between the requesting Member State and the Member State to whom such request is being made to. This state of affairs is further compounded by the absence of an AU legal instrument for the rendition of extradition or mutual assistance requests between Member States. The apparent problem here is that an AU Member State that may have adopted and ratified the Convention into its national laws may not have an extradition or mutual assistance treaty with another AU State that is also a party to the Convention. As such, a request for extradition or mutual assistance may not be successful between two Member States to the Convention even where the requirements of the double criminality principle have been fulfilled. This apparently implies that States after establishing "uniform" national laws that would guarantee the application of the double criminality principle would then have to individually establish mutual legal assistance treaties amongst themselves. As such, each Member State of the AU will have to establish mutual assistance treaties with the other 53 sovereign States of the AU. This will require each State to engage in tedious and expensive negotiation processes of which success may not always be guaranteed. For example, under the Convention a small AU State such as Cape Verde may only be able to obtain a regional wide guarantee for mutual assistance and extradition where it has entered into extradition or mutual legal assistance arrangements with all the 53 other sovereign States within the AU.

The above state of affairs also creates an enabling environment for forum shopping by cyber criminals within Africa. In this respect, a Member State that does not have extradition or mutual assistance arrangements with all other AU Members may technically provide a safe haven for cyber criminals since an extradition request cannot be successfully made to such State from another Member State with which it has no extradition treaty. This would further be compounded where such State does not have capacity to investigate or prosecute cyber crime or where it is reluctant to prosecute. In that that situation for example, a cyber criminal that operates from such State and whose acts have effects in another Member State with which the host State does not have an extradition treaty may not be held accountable. The same also applies where a cyber criminal commits an offence in a Member State and then flees to another Member State that does not an extradition treaty with the State in which the offence was committed. In both situations, the Member State where the cyber criminal is located may not even prosecute since there is no obligation to extradite. As such the doctrine of *aut dedere aut judicare* (extradite or prosecute) would not apply.

The position is quite different under the Council of Europe (CoE) Convention on Cybercrime which establishes very elaborate procedures to facilitate international cooperation amongst Member States. Thus, while extradition principles established under article 24 (1) of the CoE Convention on Cybercrime provide that extradition arrangements between Member States shall be based on the principles of "dual criminality" (double criminality), Member States are

39 *See* Article 28: 2, AU Convention on Cyber Security.

however allowed to adopt the Convention as a legal basis for extradition proceedings in the absence of a treaty on extradition. This apparently recognizes the fact that extradition treaties may not exist between all Member States to the Convention. In this respect, article 24(3) of the CoE Convention 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".[40]

The Convention also provides that where a Member State refuses to grant an extradition request, that such Member State shall prosecute the offender at request of the Member State whose extradition request was refused.[41] Thus, the Convention entrenches the doctrine of *aut dedere aut judicare*. The Convention also recognizes the application of the double criminality principle in mutual assistance requests between Member States.[42] However, the Convention also establishes procedures for a Member State to render mutual assistance requests to another Member State where there is no existing international agreement or arrangement between them on the basis of a uniform or reciprocal legislation.[43] The Convention's international cooperation procedures are not meant to supersede the provisions of existing international agreements or reciprocal arrangements on mutual assistance and extradition[44] and neither are such procedures intended to create a separate general regime for mutual assistance that is parallel to the European Convention of on Mutual Assistance.[45] Nevertheless, the procedures provide a regime for international cooperation between Member States that lack such international cooperation arrangements and thus reducing impediments to international cooperation to the barest minimum.

3. COOPERATION UNDER AFRICAN SUB-REGIONAL LEGAL INSTRUMENTS ON CYBER SECURITY

A. The ECOWAS Directive on Fighting Cybercrime

In August 2011, the ECOWAS Council of Ministers adopted the Directive C/DIR.1/08/11 on Fighting Cybercrime at its Sixty Sixth Ordinary session at Abuja.[46] The Directive imposes obligations on Member States to criminalize cyber crime[47] and also establishes a framework to facilitate international cooperation on cyber security. In this respect, article 33(1) of the Directive provides that:

> "Where Member States are informed by another Member State of the alleged commission of an offence as defined under the Directive, such Member States "*shall cooperate in the search for and establishment of that offence, as well as in the collection of evidence pertaining to the offence*".[48]

40 *See* Article 24(3) CoE Convention on Cybercrime.
41 *See* Article 24(6) CoE Convention on Cybercrime.
42 *See* Article 25(5) CoE Convention on Cybercrime.
43 *See* Article 27 CoE Convention on Cybercrime.
44 *See* Explanatory Note, CoE Convention on Cybercrime, No.244.
45 *See* Explanatory Note, CoE Convention on Cybercrime, No.262-263.
46 *See* ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).
47 *See* Article 2 ECOWAS Directive on Cybercrime.
48 *See* Article 33(1) ECOWAS Directive on Cybercrime.

The Directive also provides that "such cooperation shall be carried out in line with relevant international instruments and mechanisms on international cooperation in criminal matters"[49]. Applicable ECOWAS instruments on international cooperation include: the ECOWAS Convention on Mutual Assistance in Criminal Matters[50] and the ECOWAS Convention on Extradition.[51]

The ECOWAS Convention on Mutual Assistance in Criminal Matters establishes a broad framework for the rendition of mutual assistance amongst ECOWAS States where there is an absence of applicable international agreement between them on the basis of a reciprocal legislation. Under the Convention, Member States are required to afford each other "the widest measure of mutual assistance in proceedings or investigations in respect of offences the punishments of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Member State".[52] Thus, within the framework of the Convention, every ECOWAS Member State has an obligation to render mutual assistance to all other ECOWAS States where such assistance is requested with respect an offence that constitutes a crime in both the requesting and requested Member States[53], regardless of the absence of an applicable bilateral mutual assistance agreement between the requesting and requested Member States.

The ECOWAS Convention on Extradition also establishes a broad framework for the rendition of extradition requests between ECOWAS Member States. Thus, the Convention requires Member States to render extradition requests on the basis of dual criminality regardless of the absence of a bilateral extradition treaty between the requesting and requested Member States.[54]

Accordingly, the existence of the above ECOWAS Conventions on mutual assistance and extradition creates a broad framework on which ECOWAS Member States that have established cyber security laws can render mutual assistance and extradition requests to other ECOWAS States on the basis of dual criminality and regardless of the absence of applicable bilateral mutual assistance or extradition treaties.

B. The COMESA Model Cybercrime Bill

In October 2011, the COMESA established a Model Cybercrime Bill[55] to provide a uniform framework that would serve as a guide for the development of cyber crime laws in Member States, however, the Bill does not establish any binding obligations on Member States to criminalize cyber crimes. The Bill largely adopts the language and model of legal instruments such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation. It also establishes an elaborate guide for the development of general framework to facilitate international cooperation[56], extradition[57], and mutual assistance[58] and provides

49 *See* Article 33 (2) ECOWAS Directive on Cybercrime.
50 *See* ECOWAS Convention on Mutual Assistance in Criminal Matters (A/P1/7/92) (29 July, 1992, Dakar, Senegal).
51 *See* ECOWAS Convention on Extradition (A/P1/94) (6 August, 1994, Abuja, Nigeria).
52 *See* Article 2(1) ECOWAS Convention on Mutual Assistance in Criminal Matters.
53 *See* Article 2(1) ECOWAS Convention on Mutual Assistance in Criminal Matters.
54 *See* Articles 2 and 3 ECOWAS Convention on Extradition.
55 *See* Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).
56 *See* section 41 COMESA Model Cybercrime Bill.
57 *See* section 42 COMESA Model Cybercrime Bill.
58 *See* section 43 COMESA Model Cybercrime Bill.

for the establishment of national 24/7 points of contact.[59] However, despite its framework on international cooperation, the Bill only serves as a mere guide or model for development of national cyber security laws in Member States. Thus, the Bill does not establish any international cooperation obligations on Member States and neither can it be used as a legal instrument for cooperation amongst Member States. Also unlike the ECOWAS, the COMESA does not have any existing legal frameworks to facilitate mutual assistance and extradition among Members. As such, COMESA Member States that have used the Bill to develop their national laws would still have to enter into separate bilateral arrangements with other Member States in order to obtain any form of international cooperation or mutual assistance.

C. The SADC Model Law on Computer Crime and Cybercrime

In March 2012, the SADC adopted the Model Law on Computer Crime and Cybercrime[60] to serve as a guide for the development of cyber security laws in SADC Member States. However, it does not impose any obligations on Members to establish cyber crime laws. It does not also establish any provisions to guide the development of international cooperation regimes in Member States and neither does it establish any international cooperation obligations on Member States. However, Members that have established cyber security laws may rely on the SADC Protocol on Mutual Legal Assistance in Criminal Matters[61] and the Protocol on Extradition[62] to obtain international cooperation from other Members. Under the SADC Protocol on Mutual Assistance, Member States are required to provide each other with "the widest possible measure of mutual legal assistance in criminal matters"[63]. The Protocol also requires that such assistance shall be rendered without regard to whether the conduct which is the subject of the mutual assistance request by a Requesting State would constitute an offence under the laws of the Requested State.[64] On the other hand, the Protocol on Extradition requires that SADC States can only obtain cooperation amongst themselves on the basis of dual criminality.[65]

4. PROPOSALS TO STRENGTHEN INTERNATIONAL COOPERATION ON CYBER SECURITY AMONGST AFRICAN STATES

The review in section 2 of this paper has shown that the AU Cyber Security Convention does not provide an adequate framework for international cooperation and mutual assistance amongst African States. The review in section 3 showed the existence of international cooperation and mutual assistance mechanisms within two African sub-regional groupings, the ECOWAS and the SADC. Consequently, Africa has a situation whereby there is no regional wide cooperation and mutual assistance on cyber security, thus resulting in the limitation and fragmentation of cooperation and mutual assistance along sub-regional and bilateral arrangements. While it is agreed that cyber threats that affect African States may also emanate from outside the continent, which also underscores the need for wide international cooperation amongst all States, however

59 *See* section 52 COMESA Model Cybercrime Bill.
60 *See* SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.
61 *See* SADC Protocol on Mutual Legal Assistance in Criminal Matters (Luanda, 3 October, 2002).
62 *See* SADC Protocol on Extradition (Luanda, 3 October, 2002).
63 *See* Article 2(1) SADC Protocol on Mutual Legal Assistance in Criminal Matters
64 *See* Article 2(4) SADC Protocol on Mutual Legal Assistance in Criminal Matters
65 *See* Article 3 SADC Protocol on Extradition.

the development of a framework for such global cooperation is beyond the AU and also beyond the scope of this paper. This notwithstanding, AU Member States should at least be able to obtain international cooperation amongst themselves to the widest possible extent. Thus, since the AU Cyber Security Convention is meant to serve as a treaty for the promotion of cyber security within Africa, the ideals of African unity and cooperation which inspired the founding of the AU[66] would not have been fulfilled if there is no explicit AU framework to facilitate international cooperation and mutual assistance amongst Member States. The Convention's emphasis on the use of existing channels of cooperation or bilateral or multilateral arrangements only narrows cooperation to multilateral or sub regional or bilateral arrangements, and thus resulting in a fragmentation of cyber security cooperation within Africa. Consequently, the absence of a broad AU framework to facilitate mutual assistance and international cooperation would limit the effectiveness of the Convention.

To address above state of affairs, it may be necessary for the AU to establish an additional protocol that would create provisions enabling all Member States to the AU Cyber Security Convention to adopt the protocol as a legal basis for the rendition of international cooperation such as extradition requests or mutual assistance in accordance with the principle of dual criminality where there is an absence of applicable treaties between Member States. The AU may also consider the establishment of explicit extradition and mutual assistance instruments to facilitate the rendering of extradition and mutual assistance requests within the African region with respect to cyber crime offences established under the Convention. This type of mechanism already exists in Europe in form of the European Convention on Extradition[67] and the European Convention on Mutual Assistance in Criminal Matters[68] which are also applicable under the Council of Europe Convention on Cybercrime.[69]

The AU Convention does not create a regional Computer Emergency Response Team (CERT) to facilitate cyber security efforts and coordinate responses to cyber security incidents at the regional level. Rather, article 28:3 of the Convention imposes obligations on Member States to "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)".[70] This provision is unique as there are no African sub regional cyber security instruments that require Member States to promote the establishment of a national CERT or CSIRT. However, the need for the establishment of a regional CERT or CSIRT is also imperative as its absence may result in poor cooperation or coordination of African cyber security efforts and responses to cyber threats at the regional level. In this respect it should be noted that a regional CERT has a broader scope of functions and responsibilities than a national CERT. A national CERT is usually responsible for coordinating emergency responses to cyber threats affecting national computer or information systems and

66 *See* Article 3 Constitutive Act of the AU (July, 2000).
67 *See* the European Convention on Extradition (Paris, 13 December 1957) [ETS No. 24].
68 *See* the European Convention on Mutual Assistance in Criminal Matters (Strasbourg, 20 April 1959) [ETS No. 30]. See also the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, (Strasbourg, 17 March 1978) [ETS No. 99].
69 *See* Article 39 Council of Europe Convention on Cybercrime.
70 *See* Article 28: 3, African Union Convention on Cyber Security and Personal Data Protection

also establishing best practices relating to the use of such systems within a State.[71] On the other hand, a regional CERT may perform the functions of a national CERT at a regional level and also facilitate cyber security cooperation between national CERTs.

There have been some efforts within the African information security industry to develop a CERT for Africa. However, although such industry initiatives have a great potential to enhance private sector participation in African cyber security, they may not be adequate for the purpose of coordinating national responses to cyber security or fostering cooperation amongst Member States. A legal basis may be found for the establishment of a network security agency within the AU framework under article 32 of the Convention which provides for an operational mechanism for the Convention. Some of the functions of the Convention's operational mechanism include:

a) Promoting the adoption and implementation of measures to strengthen cyber security in electronic services and combating cyber crime and human rights violations in cyberspace;
b) Advising African governments on measures to promote cyber security and combat cyber crime; and;
c) Analyzing the criminal behaviors of cyberspace users within Africa and transmitting such information to competent national authorities.[72]

Apparently, the above mandate may be broadly interpreted to create a regional network agency which is similar to the European Information Security Agency (ENISA). The ENISA was established in 2004 by the European Commission[73] to promote cyber security and critical information infrastructure protection. The Agency serves as a center of excellence for Member States of the European Union and European institutions on cyber security issues. Its responsibilities include providing advice and recommendations on cyber security and disseminating information on standards for best practices.[74] A regional network agency that is established under article 32 of the Convention may also function as a regional CERT where its mandate is enlarged to function as such. However, the establishment of an AU CERT would not be without some peculiar challenges such as lack of funding, differences in the legal systems of AU Members, and the ability of Member States to effectively cooperate in sharing information and critical resources. Some of such challenges were faced by the EuroCERT.[75]

CONCLUSION

The adoption of the AU Cyber Security Convention marks a significant milestone in African cyber security governance and underscores Africa's efforts to promote the development of a secure information society. This notwithstanding, the success of the Convention, to a great extent, will not only be determined by the number of AU Member States that eventually ratify the Convention, but also by the extent to which it can serve as a viable legal instrument for cyber

71 The responsibilities of a national CERT include: detecting, identifying or monitoring threats to cyber security and issuing early warnings of such threats; and publicizing 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.

72 *See* Article 32 African Union Convention on Cyber Security and Personal Data Protection

73 *See* Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency.

74 *See* <http://www.enisa.europa.eu/>.

75 *See* ENISA, *CERT Cooperation and its further facilitation by relevant Stakeholders* (ENISA, 2006,) pp.23-25.

security cooperation amongst Member States. However, despite its seeming comprehensive approach to cyber security governance, the Convention in present form offers no hope for broad international cooperation amongst all AU States. Consequently, there is need for the AU to consider the issues raised in this paper in order to prevent the limitation or fragmentation of Africa's cyber security cooperation to only bilateral arrangements or to sub-regional arrangements under the ECOWAS and SADC frameworks.