DOI 10.5817/MUJLT2018-2-1

THE AFRICAN UNION CONVENTION ON CYBERSECURITY: A REGIONAL RESPONSE TOWARDS CYBER STABILITY?

by

UCHENNA JEROME ORJI*

Following the liberalization of telecommunication markets in African States, and the increasing availability of wireless technologies and broadband capacity, the levels of Internet penetration and ICT access in Africa has continued to grow in a phenomenal manner since the beginning of the new millennium. Internet use statistics indicate that Africa's Internet user population grew from about four and a half million people in 2000 to about 400 million people in December, 2017. However, widespread ICT access and Internet penetration in Africa has also raised concerns over the need to promote cybersecurity governance and cyber stability across the continent. This prompted the African Union to establish a regional cybersecurity treaty, known as the African Union Convention on Cyber Security and Personal Data Protection, in June, 2014. The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. This article analyzes the nature and scope of the cybersecurity governance obligations under the Convention and examines how the adoption of the Convention can promote cyber stability in the African region. In so doing, the paper also examines the challenges impeding the application of the Convention as a framework for promoting regional cyber stability in Africa. The paper identifies the slow pace of Member State ratification and the absence of effective regional coordination as some of the major reasons why the Convention has not been effectively applied as a framework for promoting regional cyber stability. Therefore, the paper makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve

* jeromuch@yahoo.com, LL.B (Hons.) (University of Nigeria); LL.M (University of Ibadan); PhD (Nnamdi Azikiwe University Nigeria) Barrister and Solicitor of the Supreme Court of Nigeria.

the regional harmonization of cybersecurity governance frameworks, and harness the application of the Convention as a framework for promoting regional cyber stability.

KEY WORDS

African Union, Cyber Stability, Regional Cybersecurity Obligations

1. INTRODUCTION

Since the beginning of the 21st century, the African continent has continued to witness a tremendous growth in ICT and Internet penetration. Recent Internet use statistics indicate that Africa's Internet user population grew from about 4.515 million people in 2000 to 453.3 million people in December, 2017, representing approximately 35.2 percent of Africa's entire population estimate.[1] This phenomenal growth, which still continues into the future,[2] has been linked to factors such as the liberalization of telecommunications markets in African States, the widespread proliferation of mobile telecommunication technologies, and the increasing availability of broadband capacity.[3] However, the spread of ICTs and Internet penetration in Africa has also raised concerns over the need to promote cybersecurity governance and cyber stability in the continent. This need prompted the African Union to establish a regional cybersecurity treaty known as the African Union (AU) Convention on Cyber Security and Personal Data Protection, in June, 2014.[4] The Convention imposes obligations on Member States to establish legal, policy and regulatory measures to promote cybersecurity governance and control cybercrime. This paper analyzes the nature and scope of the cybersecurity governance obligations under the Convention, and also examines how the adoption of the Convention can promote cyber stability in the African region, as well as the challenges impeding the application of the Convention as a framework for promoting regional cyber stability in Africa.

---

1 Miniwatts Marketing Group. (2017) *Internet Usage Statistics for Africa* [online]. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

2 The GSMA (Global System for Mobile Communications Association) reports that *"over the next five years, an additional 168 million people will be connected by mobile services across Africa, reaching 725 million unique subscribers by 2020"*. See GSMA. (2016) *The Mobile Economy Africa 2016.* London: GSMA, p. 2.

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

4 See *The African Union Convention on Cyber Security and Personal Data Protection,* 27 June, 2014 (EX.CL/846 (XXV)).

The paper identifies the slow pace of ratification by Member States and the absence of effective regional coordination as some of the major reasons why the Convention has not been effectively applied as a framework for promoting regional cyber stability. Accordingly, the paper makes a case for the establishment of a regional monitoring mechanism within the AU framework to improve the regional harmonization of cybersecurity governance frameworks, and harness the application of the Convention as a framework for promoting regional cyber stability.

The paper comprises seven sections. The first section, which includes this introduction, will provide a brief overview of the concepts of cybersecurity and cyber stability. The second section discusses the development of the AU Convention on Cybersecurity. The third section discusses the nature and scope of the cybersecurity governance obligations under the Convention. The fourth section examines the legal status of the Convention in the domestic legal order of AU Member States. The fifth section examines the prospects of applying the Convention as a framework for promoting regional cyber stability in the African region, while the sixth section examines the challenges impeding the application of the Convention as a framework for promoting regional cyber stability. This is then followed by recommendations and the conclusion.

1.1 DEFINING CYBERSECURITY AND CYBER STABILITY

Cybersecurity 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]

Cybersecurity governance measures include technical, organizational, policy, and legal aspects.[6] The technical aspects of cybersecurity 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 cybersecurity, such as the establishment of law

[5] See ITU High Level Experts Group (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU, p. 27. See Orji, U. J. (2012) *Cybersecurity Law and Regulation*, Nijmegen: Wolf Legal Publishers, pp. 10–16.

[6] *Id*. at pp. 17–42.

enforcement organizations as well as the development of institutional capacities including the establishment of Computer Emergency Response Teams (CERTs) to provide critical services such as prevention and early warning, detection and management of cybersecurity incidents. The policy and legal aspects of cybersecurity governance deal with policy and legal measures that aim to promote cybersecurity. Legal measures are usually considered as probably the most relevant aspect of cybercrime control.[7] Such measures include the establishment of laws which prohibit 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 legal measures to facilitate cross-border cooperation on cybersecurity, including the prevention, investigation and prosecution of prohibited acts.

On the other hand, the concept of "cyber stability" has been defined as

> *"a geostrategic condition whereby users of the cyber domain enjoy the greatest possible benefits to political, civic, social, and economic life, while preventing and managing conduct that may undermine those benefits at the national, regional, and international levels"*.[8]

It has been observed that this definition creates a basis from which to identify when stability is the goal and also to discern what is potentially relevant, useful, and strategic information about activity in the cyber domain from what is not.[9] However, cyber stability is also regarded an emerging concept that has not yet been developed as an analytic category.[10] Basically, the concept of cyber stability aims to promote the exercise of State responsibilities to address the security challenges of the information society. This particularly requires States to establish appropriate legal, policy and regulatory measures to protect cyber users and cyber infrastructure within their jurisdiction, and also ensure that cyber activities which are conducted within their jurisdiction do not cause harm to other individuals or infrastructure in another jurisdiction. Thus, the concept of cyber stability requires that States will establish cybersecurity

---

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

[8] See Rudnick, L. et al. (2015) *Towards Cyber Stability: A User-Centered Tool for Policy Makers*. Geneva: United Nations Institute for Disarmament Research, p. 7.

[9] *Id.*

[10] *Id.*

governance measures including criminal laws such as cybercrime laws and regulations for the purpose of deterring persons within their jurisdiction from engaging in malicious cyber activities that will cause harm to other individuals or infrastructure in another jurisdiction. Apparently, the need to promote cyber stability arises from the increasing the interconnectedness of national information communication networks in different countries which has ushered in an age of network interdependence where the security of each country's network is also dependent on the actions of State and non-State actors around the world. Therefore, the concept of cyber stability requires States to maintain governance responsibility over cyber activities on their territory, and thus it enshrines elements of the international principles of trans-boundary harm and State responsibility. These principles have been recognized in different contexts in the Corfu Channel Case, where the International Court of Justice (ICJ) held that a State may not

> *"allow knowingly its territory to be used for acts contrary to the rights of other States"*,[11]

and in the Trail Smelter Case, where it was held that

> *"no State has a right to use or permit the use of its territory in such a manner as to cause injury […] in or to the territory of another or the properties or persons therein"*.[12]

2. THE AFRICAN UNION AND THE DEVELOPMENT OF THE CONVENTION CYBERSECURITY

The African Union (AU) is an intergovernmental regional body that unites sovereign States within the entire African continent.[13] The AU was established in 2001 to replace the Organization of African Unity[14] and its headquarters is located in Addis Ababa, Ethiopia. Currently, the AU comprises 55 sovereign African States.[15] The aims of the AU include *inter alia* to *"accelerate the political and socio-economic integration"* of the African

[11] See *The Corfu Channel Case (United Kingdom v. Albania)* (1949) ICJ Reports 4, at paragraph 22.

[12] See *The Trail Smelter Arbitration Case (United States of America v. Canada)* (1938) 3 R.I.A.A. 1905. *See* Editorial, (1941) The Trail Smelter Arbitral Decision. *American Journal of International Law*, 35, p. 684.

[13] See The African Union (AU) [online] Available from: http://www.au.int/en/ [Accessed 6 June 2018].

continent;[16] to promote economic development and *"the integration of African economies"*,[17] and to

> *"coordinate and harmonize the policies between the existing and future regional economic communities for the gradual attainment of the objectives of the Union"*.[18]

These mandates which are enshrined in the Constitutive Act of the AU create broad legal basis for the AU and its institutions to establish regional policy and regulatory regimes on issues that affect Africa's economic integration and development, such as telecommunications/ICTs and cybersecurity governance.[19] However, the AU did not commence the development of concrete regulatory initiatives cybersecurity until after 2008.[20] A major factor that might have impeded the development of regional cybersecurity initiatives can be traced to the low penetration of ICTs in Africa prior to the widespread availability of wireless technologies within the first decade of the 21st century. One of the AU's first 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).[21] The Report emphasized the need for the establishment of a harmonized regional policy

---

[14] The AU was originally established as the Organization of African Unity (OAU) by the OAU Charter on 25 May, 1963 in Addis Abba, Ethiopia. However, on the September 1999, the Heads of States of the OAU issued a Declaration (The Sirte Declaration) which called for the establishment of an African Union to accelerate the process of integration within the African continent with a view to enhancing Africa's role in the global economy and also addressing Africa's social, economic and political problems. Subsequently, the AU was established on 26 May, 2001 in Addis Abba and launched on 9 July, 2002 in South Africa to replace the OAU. See African Union (2017) *African Union in a Nutshell.* [online] Available from: http://www.au.int/en/abut/nutshell [Accessed 6 June 2018].

[15] See African Union (2017) *Member States*. [online] African Union. Available from: http://www.au.int/en/member_states/country profiles [Accessed 6 June 2018].

[16] See Article 3(c) Constitutive Act of the AU. Togo: The Thirty-sixth Ordinary Session of the Assembly of Heads of State and Government. In English.

[17] See Article 3(j) *id.*

[18] See Article 3(i) *id.*

[19] See Orji, U. J. (2018) International Telecommunications Law and Policy. United Kingdom: Cambridge Scholars Publishing, p. 240.

[20] For example, in Europe issues relating to cybersecurity have been on the Council of Europe's agenda since 1976. See Council of Europe (1976) *Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*. Strasbourg. See Schjolberg, S. (2008) *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva*, p. 2. [online] Available from: http://www.cybercrime law.net/documents/cybercrime_history.pdf [Accessed 6 June 2018].

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

and regulatory framework on cybersecurity.[22] Subsequently, on 5 November, 2009, the AU Ministers in Charge of Communication and Information Technologies convened an Extraordinary Session in Johannesburg, South Africa, where they adopted a set of declarations known as the Oliver Tambo Declaration.[23] 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, cybersecurity, and personal data protection"*.[24]

The Declaration further recommended that AU Member States should adopt the proposed Convention by 2012.[25]

In 2011, the efforts of the AU and UNECA led to the development of the Draft Convention for the Establishment of a Credible Legal Framework for Cybersecurity in Africa.[26] The Draft Convention was meant to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. Later, in June, 2012, the AU Expert Group on Cybersecurity (comprising experts from Member States and Regional Economic Communities in Eastern, Southern and Northern Africa) met in Addis Ababa, Ethiopia, to consider the Draft Convention.[27] The Draft Convention was subsequently adopted in September, 2012, by the AU Expert Group on Cybersecurity.[28] This was also followed by its approval during the 22nd Ordinary Session of the AU Executive Council in January, 2013. After that, the Draft Convention was to be presented for legal validation by the AU Justice Ministers Conference

---

[22] See African Union (2008) n. 21, p. 75.

[23] See Extra-Ordinary Conference of African Union Ministers in Charge of Communication and Information Technologies (2009) *Oliver Tambo Declaration*. Johannesburg, South Africa: African Union.

[24] *Id.* p. 4.

[25] *Id.*

[26] 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.

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

[28] *See* United Nations Economic Commission for Africa (UNECA) Press Release, *Draft African Union Convention on Cybersecurity Comes to its Final Stage*. [online] Available from: http://www1.uneca.org/TabId/3018/Default. aspx?ArticleId=1931 [Accessed 6 June 2018].

in October, 2013,[29] after which it was also to be presented for adoption by the AU Summit in January, 2014 and then open for signatures and ratification by AU Member States. However, the Draft Convention could not be presented to the AU for adoption in January, 2014, as a result of technical delays,[30] and also due to opposition from civil society groups and the academia.[31] There were also concerns that the Convention was drafted without a wide consultation of relevant stakeholders in Member States,[32] and lacked critical cybersecurity governance mechanisms to facilitate effective legal harmonization and international cooperation.[33] A revised version of the Draft Convention was later adopted on 27 June, 2014, by the AU Heads of State and Government during the 23rd Ordinary Session of the AU Assembly in Malabo.[34]

The Convention is known as the AU Convention on Cyber Security and Personal Data Protection[35] and basically aims to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. The 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

---

[29] See ECA Press Release (2012) ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity. [online] Available from: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislations-on-Cybersecurity.aspx [Accessed 6 June 2018].

[30] See Rosewarne, C. and Odunfa, A. (2014) *The 2014 Nigerian Cyber Threat Barometer Report.* South Africa and Nigeria: Wolfpack Information Risk and Digital Jewels, p. 40.

[31] See Van Zyl, G. (2014) Adoption of 'flawed' AU Cybersecurity Convention Postponed. *IT Web Africa*. [online] Available from: http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed [Accessed 6 June 2018].

[32] See *Open Forum to discuss the proposed legal framework for cybersecurity in Africa*, (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4 [Accessed 6 June 2018].

[33] See Orji, U. J. (2012) 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*, vol. 17, no. 4, pp. 128–130.

[34] For a history of the development of AU Convention on Cybersecurity and Personal Data Protection, see Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, Issue 5, pp. 129–135; Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In Maybaum, M. *et al* (eds.) *Architectures in Cyberspace – 7th International Conference on Cyber Conflict*. Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence, pp. 105–118; Orji, U. J. (2012) 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 ofComputer, Media and Telecommunications Law*, 17 (4), pp. 128–130.

[35] See *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (EX.CL/846(XXV)) (hereafter, *AU Convention on Cybersecurity and Personal Data Protection*).

Communities (RECs).[36] With respect to cybersecurity governance and cybercrime control, the Convention recognizes that:

> *"the current state of cybercrime constitutes a real threat to the security of computer networks and the development of the information society in Africa"*[37]

and that this state of affairs underscores the need

> *"to define broad guidelines of the strategy for the repression of cybercrime in Member States of the AU, taking into account their existing commitments at the sub-regional, regional and international levels".*[38]

Accordingly, the Convention adopts a *"technology neutral"*[39] language to establish substantive and procedural criminal law provisions which address cybersecurity governance and cybercrime control in AU Member States. Thus, aside from establishing substantive and procedural criminal law provisions on cybercrime, the Convention also imposes broad obligations on Member States to establish national cybersecurity policies as well as legal, regulatory and institutional frameworks for cybersecurity governance and cybercrime control. This approach apparently goes beyond that of the Council of Europe Convention on Cybercrime[40] which mainly requires Member States to criminalize cybercrimes by establishing substantive criminal law measures as well as procedural and international cooperation mechanisms for law enforcement.[41] The Convention will enter into force after it has been ratified by 15 AU Member States.[42]

---

[36] See Preamble, *AU Convention on Cybersecurity and Personal Data Protection*, 2014.

[37] *Id.*

[38] *Id.*

[39] The technology neutrality principle proposes that *"legislation should define the regulation to be achieved and should neither impose, nor discriminate in favour of the use of a particular type of technology to achieve those objectives"*. See European Commission (1999) *Towards a New Framework for Electronic Communications Infrastructure and Associated Services.* Brussels: European Commission, p. 539. See generally, Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) *Telecommunications Law and Regulation*. 3rd ed. New York: Oxford University Press, p. 53.

[40] See *The Council of Europe Convention on Cybercrime*, 23 November 2001 (41 I.L.M. 282).

[41] See Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, vol. 5, p. 132.

[42] See Article 36 *AU Convention on Cybersecurity and Personal Data Protection*.

3. MEMBER STATE OBLIGATIONS TO IMPLEMENT MEASURES THAT PROMOTE CYBER STABILITY

The Convention establishes obligations on Member States to implement measures that will promote cyber stability. In this regard, the Convention requires Member States to implement obligations that include: establishing a national cybersecurity framework; promoting a culture of cybersecurity; establishing national cybersecurity governance structures; protecting critical information infrastructure; establishing cybercrime offences and procedural measures; and, promoting international cooperation and legal harmonization. These obligations are discussed below.

3.1 OBLIGATIONS TO ESTABLISH A NATIONAL CYBERSECURITY FRAMEWORK

The Convention requires Member States to promote cyber stability by establishing appropriate cybersecurity governance frameworks. In this regard, Member States are required to establish a national cybersecurity framework that comprises a national cybersecurity policy and a national cybersecurity strategy.[43] A Member State's national cybersecurity policy is required to recognize the importance of national Critical Information Infrastructure (CII), and identify related risks using the all-hazards approach, while also outlining how the objectives of such policy are to be achieved.[44] The "all-hazards" approach to CII protection entails the protection of such infrastructure from all forms of threats, whether they originate from deliberate attacks, accidents or natural disasters.[45] In addition, the obligation to establish a national cybersecurity policy requires Member States to outline how their national cybersecurity policy will achieve the objectives of protecting national CII from identified risks.

With respect to the establishment of a national cybersecurity strategy, Article 24:2 of the Convention requires Member States to adopt strategies they deem "appropriate and adequate" when implementing their national cybersecurity policy, especially when undertaking initiatives such as legal reform and development, capacity building, public-private partnership,

---

[43] See Article 24 *AU Convention on Cybersecurity and Personal Data Protection*, 2014.

[44] See Article 24:1 *id*.

[45] See Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD, p. 5. See also Brommelhorster, J. et al. (2004) Critical Infrastructure Protection: Survey of World-wide Activities. *BSI KRITIS*, (4), p. 1.

international cooperation and cybersecurity awareness raising. In this regard, the Convention recognizes the sovereign right of each Member State to adopt any strategy that it deems fit or appropriate in order to effectively implement its national cybersecurity policy. The obligation under Article 24:2 of the Convention also requires that a Member State's national cybersecurity strategy should define the organizational structures for cybersecurity governance, set objectives and timeframes for the successful implementation of the national cybersecurity policy, and also establish the critical basis for the effective management of cybersecurity incidents and international cooperation in such matters.

To a large extent, the Convention's requirement that Member States should establish cybersecurity policies and strategies appears similar to Article 7 of the European Union (EU) Directive on Network and Information Security (2016)[46] which also requires Member States to adopt

> *"a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems […]".*[47]

3.2 OBLIGATIONS TO PROMOTE A CULTURE OF CYBERSECURITY

Article 26 of the Convention establishes obligations on Member States to promote a culture of cybersecurity amongst all stakeholders (such as governmental institutions, businesses and the civil society) that develop, operate, or use information systems and networks.[48] In this respect, Article 26:1 (a) of the Convention declares that

> *"the culture of cybersecurity should lay emphasis on security in the development of information systems and networks, and on the adoption of new ways of thinking and behaving when using*

[46] See Directive of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, *Official Journal of the European Union* (2016/1148) 19 July 2016) (hereafter *EU Directive on Network and Information Security*, 2016).

[47] See Article 7:1 EU Directive on Network and Information Security (2016).

[48] See Article 26:1(a) AU Convention on Cybersecurity and Personal Data Protection.

> *information systems as well as during communication or transactions across networks".*[49]

The need for the promotion of a culture of cybersecurity arises from the increasing interconnection of networks and the growing integration of networked ICTs to many of the essential aspects of daily life, including the provision of goods and services, research and development, innovation and entrepreneurship, and the free flow of information amongst individuals and organizations, governments, businesses and civil society.[50] This state of affairs implies that cybersecurity governance issues are not meant to be addressed only through the application of law enforcement or technological measures, but rather through holistic governance approaches that are widely supported by society.[51]

The obligation to promote a culture of cybersecurity under Article 26 of the Convention requires Member States to take the lead in developing a cybersecurity culture within their national territories by promoting public awareness and providing education and training on cybersecurity.[52] In this regard, Member States have obligations to

> *"adopt measures to develop capacity building with a view to offering training which covers all areas of cybersecurity to different stakeholders, and setting standards for the private sector".*[53]

This also includes the promotion of technical education for ICT professionals in both the public and private sectors through certifications and standardization trainings.[54] In addition, Member States are required to develop a public-private partnership model that will engage the participation of stakeholders such as industry groups, the civil society and the academia in promoting a culture of cybersecurity.[55]

---

[49] See Article 26:1(a) *AU Convention on Cybersecurity and Personal Data Protection.*

[50] See *United Nations Resolution on the Creation of a Global Culture of Cybersecurity,* 21 December 2009 (A/RES/64/211). See also *United Nations Resolution on the Creation of a Global Culture of Cybersecurity,* 23 December 2003 (A/RES/58/199).

[51] See ITU (2009) *National Cybersecurity/CIIP Self-Assessment Tool*. Geneva: ITU, p. 26. See also United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 20 December 2003 (A/RES/57/239).

[52] See Article 26:2 AU Convention on Cybersecurity and Personal Data Protection.

[53] See Article 26:4 *id.*

[54] *Id.*

[55] See Article 26:3 *id.*

3.4 OBLIGATIONS TO ESTABLISH NATIONAL CYBERSECURITY GOVERNANCE STRUCTURES

Article 25:2 of the Convention imposes obligations on Member States to establish appropriate structures or institutions as well as regulatory powers that are necessary for cybersecurity governance. Article 27:1(a) of the Convention also requires Member States

> *"to adopt the necessary measures to establish an appropriate institutional mechanism responsible for cybersecurity governance".*[56]

to a large extent, the provisions of Articles 25:2 and 27:1(a) of the Convention have similar implications with Article 8(1) of the EU Directive on Network and Information Security (2016), which requires Member States to

> *"designate one or more national competent authorities on the security of network and information systems".*[57]

Under the Convention, the obligations to establish national cybersecurity governance structures requires the establishment of appropriate national institutions with responsibilities to tackle cybercrimes and respond to cybersecurity incidents, and also facilitate international cooperation in the management of such incidents.[58] Thus, within the context of those obligations, it is implied that every Member State should establish institutions such as a national cybersecurity agency and a national Computer Emergency Response Team (CERT).[59] The Convention also requires that national cybersecurity governance structures should be established within a national framework that can respond to challenges and issues affecting all aspects of cybersecurity at the national level.[60] In order to ensure the effective functioning of national cybersecurity structures, the Convention requires Members States to take necessary measures to establish clear accountability on cybersecurity issues at all levels of government by defining the roles and responsibilities of institutions

---

[56] See Article 27:1(a) *AU Convention on Cybersecurity and Personal Data Protection.*
[57] See Article 8:1 EU Directive on Network and Information Security (2016).
[58] See Article 27:2 AU Convention on Cybersecurity and Personal Data Protection.
[59] See Article 28:3 *id.*
[60] See Article 27:1(c) *id.*

in clear and precise terms[61] and also expressing a clear public and transparent commitment to the promotion of cybersecurity, including encouraging the participation of the private sector in governmental initiatives to promote cybersecurity.[62]

3.5 OBLIGATIONS TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

The Convention establishes obligations on Member States to protect CII. In this respect, Article 25:4 of the Convention requires Member States to adopt necessary legislative and regulatory measures to identify those sectors that are "sensitive" to their national security and economic wellbeing, and also to classify the ICT systems that are designed to function in those sectors as elements of CII. Although, the Convention does not define the meaning of CII, it however classifies CII in relation to the concept of *"Critical Cyber/ICT Infrastructure"*.[63] Under Article 1 of the Convention the concept of Critical Cyber/ICT Infrastructure is defined as

> *"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".*[64]

The CII protection obligations under Article 25:4 of the Convention requires Member States to establish severe sanctions for cybercrimes and other criminal activities that affect ICT systems in critical sectors and also establish measures to improve the security and management of such systems.[65] Article 30:1(d) of the Convention also creates a CII protection obligation which requires Member States to

> *"establish necessary criminal law 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".*[66]

The Convention does not provide a definition of *"critical national defence infrastructure"*, however, within the context the term would apparently refer

---

[61] See Article 27:1(b) (i) *AU Convention on Cybersecurity and Personal Data Protection.*
[62] See Article 27:1(b) (ii) *id.*
[63] See Article 1 *id.*
[64] *Id.*
[65] See Article 25:4 *id.*
[66] See Article 30:1(d) *id.*

to CII (critical cyber/ICT infrastructure) which are used to provide national defence services, such as computer systems that are used for national security or military operations.

The Convention does not explicitly classify the sectors that should be regarded as "sensitive" to the national security and economic wellbeing of Member States. Apparently, the absence of such explicit classification could be due to the fact that sectors which are designated as "sensitive" vary in different countries.[67] However, the common trend in establishing such classification is that where the prolonged disruption of a sector or infrastructure would affect the wellbeing of a State by causing severe economic dislocation or national security challenges, then such sector or infrastructure is generally regarded as being "sensitive" to the national security and economic wellbeing of the State and therefore classified as a "critical sector" or "critical infrastructure".[68] Such sectors include (but are not limited to) banking and financial services, governmental services, telecommunications services and ICT infrastructure providers, emergency and rescue services, energy and electricity services, health services, transportation services including traffic management services, and water supply and distribution services.[69] Generally, most of the sectors that are classified as "critical sectors" rely heavily on elements of ICT systems such as computer technologies and digital networks to function effectively. Consequently, those elements of ICT systems in critical sectors are classified as CII. Therefore, the CII concept is generally used to designate core ICT elements including interconnected and interdependent information network systems that are vital to the functioning of critical sectors and essential services in modern societies.

The essence of establishing CII protection obligations in the African context arise from the increasing penetration of ICTs in Africa[70] which has given rise to their growing integration in sectors that can be classified

[67] See generally, Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[68] See the United States President's Commission on Critical Infrastructure Protection (PCCIP). (1997) *Critical Foundations: Protecting America's Infrastructure*. Washington DC: PCCIP, Appendix B, Glossary B-2.

[69] See Dunn, M. (2005) A Comparative Analysis of Cybersecurity Initiatives Worldwide. *World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity*. Geneva: ITU, p. 14. See Annex II EU Directive on Network and Information Security (2016).

[70] See GSMA (2016) *The Mobile Economy Africa 2016*. London: GSMA, pp. 2, 8 & 19. See also, Miniwatts Marketing Group (2017) *Internet Usage Statistics for Africa*. [online] Miniwatts Marketing Group. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

as critical sectors. This increasing integration of ICTs in critical sectors is also seen a means of facilitating Africa's economic development and regional integration.[71] However, while African States have not achieved a high level of digitalization that is comparable to developed countries, the rise of digitalization in Africa has increased the reliance of critical sectors on ICT elements as well as interconnected and interdependent information network systems, to the extent that the disruption of such infrastructure by accidents or malicious acts could also cause the disruption of economic and social activities as well as public services, and thereby trigger national security concerns.[72] Therefore, African States are also vulnerable to cybersecurity threats which affect the elements of critical sectors that rely on information infrastructure usually classified as CII. This appears to underscore the reason why Article 25:4 of the Convention aims to enhance the protection of CII in Africa by imposing obligations on AU Member States to establish legal and policy measures for their identification and protection.

3.6 OBLIGATIONS TO ESTABLISH CYBERCRIME OFFENCES AND PROCEDURAL MEASURES

Article 25:1 of the Convention imposes obligations on Member States to criminalize substantive criminal acts that affect the confidentiality, integrity, availability and survival of ICT systems, and the data processed by such systems. This implies that Member States are required to establish offences that criminalize acts such as unauthorized access to a computer system, unauthorized interference with a computer system or data, and unauthorized interception of data processed by a computer system. In addition, Article 25:1 of the Convention requires Member States to criminalize substantive criminal acts that affect ICT network infrastructure. This entails the establishment of offences that criminalize attacks against CII. The Convention also requires Member States to explicitly criminalize cybercrime offences including: attacks on computer systems;[73] unauthorized access to computer systems;[74] acts that hinder

[71] See GSMA (2016), n. 70, p. 2. *See also* GSMA (2013) *Sub-Saharan Africa Mobile Economy Report 2013.* London: A.T. Kearney, p. 4.

[72] See Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment.* Florida, United States: Solutions Consulting, p. 8.

[73] See Article 29:1 AU Convention on Cybersecurity and Personal Data Protection.

[74] See Article 29:1(a) *id.*

the functioning of a computer;[75] unauthorized modification of computer data;[76] unauthorized interception of computer data;[77] computer data forgery;[78] computer fraud;[79] child pornography offences;[80] and preparatory offences relating to the misuse of computing devices, such as the unlawful production, sale, importation, possession, or making available of computer equipment, program, or any device or data that is *"designed or specifically adapted"* for the purpose of committing any cybercrime offence.[81] To some extent, the Convention's requirement that Member States should explicitly criminalize the above cybercrime offences appears similar to some of the obligations under the European Union Directive on Attacks against Information Systems (2013).[82] For example, the Directive requires Member States to criminalize illegal access to information systems,[83] illegal interference with information systems,[84] illegal data interference,[85] and illegal data interception.[86]

Article 25:1 of the Convention also imposes obligations on Member States to establish effective procedural mechanisms for the prosecution of cybercrime offences. Such procedural mechanisms are basically meant to enhance the legal capabilities of law enforcement authorities to investigate and prosecute cybercrime offences, and they usually include measures to facilitate the search, seizure, or preservation of digital evidence, or the interception of electronic communications. While establishing substantive and procedural legal measures to tackle cybercrimes, Member States are also required to take into consideration the choice of language that is used in international best practices.[87] This implies that Member States are to consider the choice of language that is used in international

[75] See Article 29:1(d) *AU Convention on Cybersecurity and Personal Data Protection.*

[76] See Article 29:1(e) & (f) *id.*

[77] See Article 29:2(a) *id.*

[78] See Article 29:2(b) *id.*

[79] See Article 29:2(d) *id.*

[80] See Article 29:3(1) *id.*

[81] See Article 29:2(b) *id.*

[82] See Directive of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems (2013/40/EU) replacing Council Framework Decision 2005/222/JHA. *Official Journal of the European Union,* 14. August 2013 (hereafter, EU Directive on Attacks against Information Systems, 2013).

[83] See Article 3 EU Directive on Attacks against Information Systems (2013).

[84] See Article 4 *id.*

[85] See Article 5 *id.*

[86] See Article 6 *id.*

[87] See Article 25:1 AU Convention on Cybersecurity and Personal Data Protection.

instruments and model laws on cybercrime such as the Council of Europe Convention on Cybercrime and the ITU Toolkit for Cybercrime Legislation.[88] Apparently, this obligation aims to encourage Member States to draft substantive and procedural legal measures on cybercrime in a technology neutral language in order to promote the international harmonization of national cybercrime laws and procedural measures.

In addition, Article 25:3 of the Convention requires Member States to ensure that the establishment and implementation of legal measures for cybersecurity governance does not infringe the constitutional rights of citizens, such as the right to freedom of expression, the right to privacy, the right to fair hearing, and other fundamental rights that are protected under national or international law, including those established under the African Charter on Human and People's Rights.[89] This requirement appears similar to some degree with the approach that is adopted by the Council of Europe Convention on Cybercrime. Thus, the Council of Europe Convention on Cybercrime requires Member States to ensure that their procedural instruments for the investigation and prosecution of cybercrime do not violate fundamental human rights.[90]

3.7 OBLIGATIONS TO PROMOTE INTERNATIONAL COOPERATION AND LEGAL HARMONIZATION

The Convention establishes a framework to facilitate international cooperation on cybersecurity and cybercrime control within the AU. In this regard, Member States are required to

> *"encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)".*[91]

Article 28:4 of the Convention also requires Member States to

---

[88] See ITU and American Bar Association - Privacy and Computer Crime Committee (2010) *ITU Toolkit for Cybercrime Legislation*. Geneva: ITU.

[89] See *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58) which entered into force on 21 October 1986.

[90] See Article 15:2 Council of Europe Convention on Cybercrime.

[91] See Article 28:3 Convention on Cybersecurity and Personal Data Protection.

> *"make use of existing channels for international cooperation with a view to responding to cyber threats and improving cybersecurity and stimulating dialogue between stakeholders".*[92]

Such channels for international cooperation may be based on international or intergovernmental or regional arrangements, or private and public partnerships.[93]

In order to facilitate the effective harmonization of legal rules and international cooperation amongst Member States, Article 28:1 of the Convention establishes obligations on Member States to

> *"ensure that the legislative measures and/or regulations adopted to fight against cybercrime will strengthen the possibility of regional harmonization […] and respect the principle of double criminal liability".*[94]

Article 28:2 of the Convention also provides that Member States that do not have mutual assistance agreements on cybercrime

> *"shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability, while promoting the exchange of information as well as the efficient sharing of data between the organizations of [Member States] on a bilateral and mutual basis".*[95]

This implies that Member States that lack mutual legal assistance agreements on cybercrime have obligations to engage in such agreements in accordance with the principles of double criminality (dual criminality).[96]

---

[92] See Article 28:4 *AU Convention on Cybersecurity and Personal Data Protection.*

[93] *Id.*

[94] See Article 28:1 *id.*

[95] See Article 28:2 *id.*

[96] "Double criminality" or "dual criminality" exists where a conduct in issue has been criminalized in the laws of both the State requesting for assistance or extradition and the State to whom such request for assistance or extradition is being made to. 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]. (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU, p. 14. *See also* Garner, B. A. (ed.) (2004). *The Black's Law Dictionary*. 8th ed., St Paul MN, United States: West Publishing Co, p. 537.

4. THE STATUS OF THE AU CYBERSECURITY CONVENTION IN THE DOMESTIC LEGAL ORDERS

Having discussed the Convention's Member State obligations that aim to promote cyber stability, this section will discuss the legal status of the Convention in the domestic legal systems of Member States. Article 35 of the AU Cybersecurity Convention provides that the Convention

> *"shall be open to all Member States of the Union, for signature, ratification or accession, in conformity with their respective constitutional procedures".*[97]

The Convention will enter into force after it has been ratified by 15 AU Member States.[98] According to a report by the AU, as of May 2018, only 10 AU Member States (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) had signed the Convention, while two Member States (Mauritius and Senegal) had ratified the Convention.[99] The AU report also showed that the signatures and ratifications were done in 2015, 2016, 2017 and 2018 with none in 2014 when the Convention was adopted.[100] This slow pace of Member States towards signing and ratifying the Convention would hinder the timely achievement of its objectives such as the harmonization of cybersecurity laws in Member States. More importantly, the slow pace of ratifications also indicates that it will probably take some more years before the Convention can be ratified by the required 15 Member States in order for it to have legal force within the AU. This state of affairs practically impedes the sense of urgency that should normally characterize cybersecurity governance responses and also has the effect of slowing down the urgency of implementing the Convention's obligations.

However, it is also recognized that one of the major challenges to the effective implementation of international and regional legal instruments has been how to balance national sovereignty concerns

---

[97] See Article 35 AU Convention on Cybersecurity and Personal Data Protection.

[98] See Article 36 *id.*

[99] See African Union. (2018) *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.* [online] African Union. Available from: https//au.int/sites/default/files/treaties/29560-slafrican_union_convention_on_cyber_security_and_personal_data_protection.pdf [Accessed 6 June 2018].

[100] *Id.*

by Member States and the obligations under such legal instruments in order to ensure that they are recognized and domestically implemented by Member States. The AU comprises English speaking (Anglophone), French speaking (Francophone) and Portuguese speaking (Lusophone) Member States that operate different legal systems with respect to the domestic reception of international or regional legal instruments. The Anglophone States that are Members of the AU operate a dualist legal tradition. Under the dualist legal tradition, national law and international law are considered as two distinct categories of legal systems. Hence, regional legal instruments, such as the AU Cybersecurity Convention, cannot be directly applied within the national legal system of a dualist State, unless they have been domesticated by an Act of the parliament. For example, in Nigeria which is an AU Member State that operates a dualist legal tradition, Section 12(1) of the 1999 Constitution provides that

> *"No treaty between the Federation and any other country shall have the force of law except to the extent to which any such treaty has been enacted into law by the National Assembly".*[101]

A similar legal requirement exists in the Constitutions of other Anglophone Member States within the AU.[102]

On the other hand, Francophone States that are Members of the AU operate a monist legal tradition. Under this tradition, international law and national law are regarded as the manifestations of a single conception of law since both laws are meant to apply to the conduct of the same subjects.[103] The monist legal tradition is regarded as having its root in national law theories which see all law as the product of reason.[104] Thus, it

[101] See Section 12:1 *Constitution of the Federal Republic of Nigeria* (1999).

[102] See for *e.g.*, Section 79:1 *Constitution of the Gambia* (1997); Section 75:1 *Constitution of Ghana* (1992); Article 40:4(1) *Constitution of Sierra Leone* (1991), and; Section 57 *Constitution of Liberia* (1986).

[103] See Oji, E. A. (2011) Application of Customary International Law in Nigerian Courts. *Nigeria Institute of Advanced Legal Studies Law and Development Journal*, 1(1), p. 156.

[104] See Oppong, R. F. (2008) Making Regional Economic Laws Enforceable in National Legal Systems: Constitutional and Judicial Challenges. In Bosi, A. and Breytenbech, W. et al (eds.) *Monitoring Regional Integration in Southern Africa Year Book*. Stellenbosch: Trade Law Center for Southern Africa, pp. 10–11.

> *"envisions international law to automatically be part of national legal systems and suggests that no conflict can arise between international and national law because they derive from the same source"*.[105]

Accordingly, the monist legal tradition allows international law or community law to become part of a State's national law without the need for an enactment to domesticate such international law within a State's legal system, provided that such law is reciprocally enforced by other State parties. Therefore, an AU Member State that operates a monist legal tradition would allow a regional legal instrument such as the AU Cybersecurity Convention to become part of its national law without the need for the domestication of the Convention within that State's legal system, provided however, that the Convention is reciprocally enforced by other Member States. For example, in the Republic of Benin which is an AU Member State that operates a monist legal tradition, Article 147 of the Constitution provides that treaties or agreements lawfully ratified shall have upon their publication an authority superior to that of laws, without prejudice for each agreement or treaty in its application by the other party.[106] A similar legal requirement exists in other Francophone States within the AU.[107] The Lusophone States within the AU also practice a monist legal tradition and establish similar requirements for the enforcement of regional legal instruments such as the AU Cybersecurity Convention.[108]

5. PROSPECTS OF APPLYING THE CONVENTION AS A FRAMEWORK FOR REGIONAL CYBER STABILITY

The AU Cybersecurity Convention holds several prospects towards promoting regional cyber stability in Africa. Such prospects arise from

---

[105] See Oppong, R. F. (2008) n. 104, p. 11.

[106] See Section 147 *Constitution of the Republic of Benin* (1990).

[107] See for e.g., Article 98 of the *Constitution of Senegal* (2001) which provides that treaties or agreements duly ratified shall, upon their publication, have an authority superior to that of the laws, subject to its application by the other party.

[108] See for e.g., Article 11:2 of the *Constitution of Cape Verde* (1992) which provides that *"international treaties and agreements, validly approved or ratified, shall be in force in the Cape Verdian legal order after their official publication and their entry into force in the international legal order, and for the time that they are internationally binding on the State of Cape Verde"*. See also Article 11:4 of the *Constitution of Cape Verde* which provides that rules and principles of general or common international law and of conventional international law, validly approved or ratified, shall prevail, after their entry into force in the international and domestic legal orders over all legislative and domestic normative acts of an infra--constitutional value.

the fact that the establishment of the Convention increases policy and regulatory awareness on cybersecurity governance, while also improving the harmonization of national cybersecurity regimes in AU Member States. Other prospects of the Convention in this regard include that it imposes a range of positive obligations on AU Member States to establish national cybersecurity regimes, and also increases the possibility of imposing AU sanctions on non-compliant Member States. These prospects are discussed below.

5.1 INCREASED CYBERSECURITY AWARENESS

One of the major advantages of establishing regional legal instruments for cybersecurity governance is that they enhance the cybersecurity awareness of regional organizations and their Member States.[109] As such, there are prospects that the establishment of the AU Cybersecurity Convention would help to promote cyber stability by increasing regional and national awareness on cybercrime and cybersecurity governance in Africa. Such awareness can also help to facilitate the establishment of cybersecurity laws and policies and other governance frameworks, such as CERTs in AU Member States that are yet to establish such frameworks. For example, as of June, 2018, about 40 States out of the 55 States of the African continent had established laws on cybersecurity, while about 20 States had established national cybersecurity policies, and, on the other hand, 18 States had national CERT frameworks.[110]

5.2 HARMONIZATION OF NATIONAL CYBERSECURITY REGIMES

Another advantage of establishing regional legal instruments for cybersecurity governance is that such instruments provide a model framework of minimum standards that will guide Member States in the development of their national cybersecurity regimes. In this regard,

---

[109] See Orji, U. J. (2016) Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses. In Samuel, C. and Sharma, M. (eds.) *Securing Cyberspace: International and Asian Perspectives.* New Delhi: Institute for Defence Studies and Analyses & Pentagon Press, p. 211.

[110] See UNCTAD. (2018) *Cybercrime Laws.* [online] Available from: http://www.unctad.org/en/Docs/Cyberlaw/CC.xlsx [Accessed on 6 June 2018]. See ITU. (2018) *Cybersecurity Country Profiles.* [online] Available from: https//www.itu/en/ITU-D/Cybersecurity/Documents/Country_Profiles/ [Accessed 6 June 2018]. See also African Union and Symantec Corporation. (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation, pp. 53–56.

harmonization refers to the process of creating common standards within Member States that belong to a common regional or international intergovernmental body with a view to promoting uniformity in national laws and policies. Harmonization helps to coordinate different national legal and regulatory systems by eliminating or minimizing major differences in national laws and policies, and thereby creating minimum standards in a manner that makes them similar with each other.[111] Within the context of cybersecurity governance, the harmonization of national cybersecurity regimes through regional instruments contributes to a large extent in minimizing national differences in such regimes and also helps in promoting regional cybersecurity cooperation. Thus, to a large extent, the AU Cybersecurity Convention's establishment of minimum standards that are meant to guide Member States in the development of their national cybersecurity regimes also has prospects to promote regional cyber stability through legal harmonization and cybersecurity cooperation within the AU.

5.3 IMPOSITION OF POSITIVE OBLIGATIONS ON MEMBER STATES

Apparently, the most significant implication that arises from the adoption of the AU Cybersecurity Convention by Member States is that the Convention imposes positive obligations on them to promote cyber stability by establishing legal, policy and regulatory frameworks on cybersecurity governance and cybercrime control. As such, every AU Member State that is a party to the Convention has positive obligations to establish national cybersecurity laws, as well as policy and regulatory frameworks that enshrine the standards under the Convention. Thus, under international law, the general principle of *pacta sunt servanda* which is expressed in Article 26 of the Vienna Convention on the Law of Treaties declares that

> *"every treaty in force is binding upon the parties to it and must be performed by them in good faith."*[112]

The Vienna Convention further declares that

---

[111] See Shuma, T. (2015) Revisiting Legal Harmonization under the Southern African Development Community Treaty: The Need to Amend the Treaty. *Law, Democracy and Development*, 19, pp. 135–136. See also Walter, J. K. (1974) Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, 23 (3), p. 501.

[112] See Article 26, *Vienna Convention on the Law of Treaties*, 23 May 1969.

> *"a party may not invoke the provisions of its internal law as justification for its failure to perform a treaty"*.[113]

Consequently, it appears that, once the AU Cybersecurity Convention has entered into force, the positive obligations under the Convention can provide a basis for holding a Member State accountable, where the latter's failure to fulfill the obligations to establish relevant cybersecurity governance frameworks has encouraged the perpetration of cybercrime which results in the violation of human rights, such as those rights guaranteed under African international human rights instruments, including the African Charter on Human and Peoples' Rights,[114] the African Charter on Rights and Welfare of the Child,[115] and the Protocol on the Rights of Women in Africa.[116] In this regard, another Member State, or an individual, or a non-governmental organization that has an Observer status before the African Commission on Human and Peoples' Rights, can directly institute an action before the African Court on Human and Peoples' Rights for a determination of a Member State's liability for the non-fulfillment of its positive obligations under the AU Cybersecurity Convention.[117]

A Member State's failure to fulfill the obligations under the AU Cybersecurity Convention can also provide a valid basis for bringing a Communication before the African Commission on Human and Peoples' Rights, where the non-fulfillment of those obligations has resulted in the violation of any of the rights guaranteed under the African Charter on Human and Peoples' Rights.[118] In this respect, an individual may bring a Communication before the Commission to determine a Member State's liability, where the failure of such Member State to fulfill the obligations under the Convention (such as the establishment of legal and regulatory frameworks for cybersecurity governance) has passively encouraged the perpetration of cybercrimes that resulted in the violation of any

---

[113] See Article 27 *id.*

[114] See *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58).

[115] See *African Charter on the Rights and Welfare of the Child*, 1990 (OAU Doc. CAB/LEG/24.9/49).

[116] See *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa*, 11 July 2003.

[117] See Articles 5:1 & 5:3 *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, 10 June 1998.

[118] See Articles 45, 47 and 56 *African Charter on Human and Peoples' Rights* (1982).

of the human rights under the African Charter.[119] The possibility of holding an AU Member State accountable for its failure to fulfill the obligations under the African Charter has already been illustrated in several decisions of the African Commission on Human and Peoples' Rights (ACHPR).[120] For example, in *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria*[121], a Communication which was brought before the ACHPR alleged that the Nigerian government had been directly involved in oil production through the Nigerian National Petroleum Company (NNPC) alongside other multinational oil companies, and that oil production caused environmental degradation and severe health problems amongst the Ogoni people of the Niger Delta. The ACHPR found the Nigerian government liable for not fulfilling its positive obligations under the African Charter as a result of its failure to take measures to prevent environmental pollution and promote sustainable development use of natural resources in Ogoni land.[122] Thus, the ACHPR, while finding Nigeria liable for the violation of the right to health and the right to a generally satisfactory environment under Articles 16 and 24 of the African Charter, held that

> *"the State is obliged to protect right holders against other subjects by legislation and provision of effective remedies […] [and that] protection generally entails the creation and maintenance of an atmosphere or framework by an effective interplay of laws and regulations so that individuals will be able to freely realize their rights and freedoms"*.[123]

The ACHPR also held that a State is required to fulfill the rights and freedoms it freely undertook under the various human right regimes.[124]

The possibility of holding a State accountable for the non-fulfillment of its treaty obligations has also been illustrated outside Africa

[119] See Articles 55 and 56 *id.* See also, Hansungule, M. African Courts and the African Commission on Human and Peoples' Rights. In Bosi, A. and Diescho, J. (2009) *Human Rights in Africa: Legal Perspective on their Protection and Promotion*. Namibia: Macmillan Education, p. 259.

[120] See *Free Legal Assistances Group and Others v. Zaire*, ACHPR/COMM, No.25/89, 47/90, 56/91, 100/93 (1995), and; *International Penn & Others (on behalf of Saro-Wiwa) v. Nigeria*, ACHPR/COMM, 137/94, 139/94, 154/96, 161/97 (1998).

[121] See *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria*, Communication No. 155/96, ACHPR/COMM/A044/1 (2002).

[122] See Coomans, F. (2003) The Ogoni Case before the African Commission on Human and Peoples' Rights', *International and Comparative Law Quarterly*, 52, pp. 749-760.

[123] See *SERA and CESR v. Nigeria*, at paragraphs 46-47.

[124] *Id.* at paragraph 47.

by the decisions of the European Court of Human Rights in the cases of *K.U. v. Finland*[125] and *I. v. Finland*.[126] In both cases, the Court found the State of Finland liable for not taking adequate measures to fulfill the positive obligations that are attached to the right to a private life under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) due to Finland's failure to timely establish adequate cybercrime and data protection frameworks.

Also, even where an AU Member State has not adopted or ratified the AU Cybersecurity Convention, there are still prospects that such Member State can be held accountable for failing to establish adequate cybersecurity governance frameworks that will ensure the protection of the human rights guaranteed under its national laws, or under Africa's human right treaties. This is because the guarantee of human rights in national laws or international treaties imposes obligations on States to ensure their protection,[127] and also gives rise to citizens' expectation that such rights will be protected by the State. Therefore, the mere fact that an AU Member State has guaranteed human rights in its national laws or as a State party to any of the AU's human right treaties would trigger obligations to protect its citizens from malicious cyber acts that can infringe on those human rights. For example, malicious cyber acts such as hacking and denial of service of attacks can infringe the exercise of several human rights including the right to privacy,[128] the right to receive information and express ideas,[129] the right to freedom of association,[130] and the right to education.[131] As such, there exists a legitimate expectation by citizens that their fundamental human rights will be protected by the State against malicious cyber acts, which can impede the exercise of those rights. Consequently, if an AU Member State that has not signed or ratified the AU Cybersecurity Convention has also failed to establish adequate measures to tackle cybercrimes that can infringe on the exercise of the human rights

[125] Judgment of 2 December 2008, ECHR No. 2872/02.

[126] Judgment of 17 July 2008, ECHR No. 20511/03.

[127] See *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights v. Nigeria*, at paragraphs 46–47.

[128] See Article 10 *African Charter on the Rights and Welfare of the Child* (1990).

[129] See Article 9 *African Charter on Human and Peoples' Rights* (1982). See Article 17 *African Charter on the Rights and Welfare of the Child* (1990).

[130] See Article 10 *African Charter on Human and Peoples' Rights* (1982). See Article 8 *African Charter on the Rights and Welfare of the Child* (1990).

[131] See Article 17 *African Charter on Human and Peoples' Rights* (1982). See Article 11 *African Charter on the Rights and Welfare of the Child* (1990).

guaranteed under its national laws or under African human right instruments, then such Member State would be failing in its obligation to protect those rights.

5.4 THE POSSIBILITY OF AU SANCTIONS ON NON-COMPLIANT MEMBER STATES

Another significant implication of the AU Cybersecurity Convention with respect to the promotion of cyber stability is that it would enhance the possibility of applying AU sanction mechanisms against Member States that fail to fulfill their obligations under the Convention when it enters into force. Thus, AU Member States are generally bound to comply with the "decisions and policies" of the AU including those made by the AU Executive Council and the AU Assembly of Heads of State and Government. In this respect, Article 23:2 of the Constitutive Act of the AU provides that

> *"Any Member State that fails to comply with the decisions and policies of the Union may be subjected to other sanctions, such as the denial of transport and communications links with other Member States and other measures of a political and economic nature to be determined by the Assembly".*[132]

The AU Cybersecurity Convention clearly constitutes a decision and policy of the AU.[133] As such, once the Convention has entered into force, Article 23:2 of the AU Constitutive Act would provide a legal basis for the AU to administer sanctions against Member States that fail to implement their obligations under the Convention. However, despite the existence of sanction mechanisms within the AU's governance framework, the AU has rarely applied sanctions for the purpose of promoting the national implementation of its legal instruments, or for the purpose of facilitating the transposition of such instruments in order to promote legal harmonization amongst Member States.[134] Although, the AU has imposed sanctions on Member States in cases

[132] See Article 23:2 *Constitutive Act of the African Union*, 11 July 2000 (hereafter, Constitutive Act of the AU).

[133] See African Union. *The African Union Convention on Cyber Security and Personal Data Protection,* 27 June, 2014 (EX.CL/846 (XXV).

[134] See Magliveras, K. D. (2011) The Sanctioning System of the African Union: Part Success, Part Failure?, *The African Union: The First Ten Years*. 11–13 October 2011. Addis Ababa: Institute of Security Studies, pp. 1–33.

of the unconstitutional overthrow of governments[135] and non-payment of membership contributions,[136] however, it appears that sanctions have not been imposed on the authority of Article 23:2 of the AU Constitutive Act.[137]

6. CHALLENGES IMPEDING THE CONVENTION AS A FRAMEWORK FOR REGIONAL CYBER STABILITY

There are several challenges that impede the application of the obligations under the AU Cybersecurity Convention for the purpose of promoting regional cyber stability. These challenges include the absence of capacity in terms of expert personnel that will facilitate the development and implementation of national policy and regulatory frameworks for cybersecurity governance, and the administration of national cybersecurity agencies and CERTs.[138] There are also peculiar challenges arising from the absence of requisite institutional capacities in terms of cybersecurity governance and cybercrime law enforcement. For example, law enforcement authorities in many African States still lack capacities to detect, investigate and prosecute cybercrime.[139] Although there have been various initiatives to build capacities in law enforcement authorities in some States, it however, appears that such initiatives to a large extent have not yet achieved the intended results. Weak institutional capacity is reflected in terms of lack of up to date technological tools to enhance law enforcement and lack of awareness amongst law enforcement officials.[140] Another indicator of weak institutional capacities is the absence of functional national CERTs and national cybersecurity agencies and to coordinate responses to cybersecurity threats in most African States. [141]

The challenge of weak institutional capacities can also be traced to the poor funding of cybersecurity governance initiatives.[142] Poor funding

---

[135] See Mkhize, S. (2014) *Assessing the Efficacy of the AU Sanctions Policies with Regard to Unconstitutional Changes in Government: The Examples of Guinea and Madagascar*. M.A. University of South Africa, pp. 67–118.

[136] See Magliveras K. D. (2011), *id.* pp. 1–33.

[137] *Id.* pp. 8–9.

[138] See African Union and Symantec Corporation (2006) *Cyber Crime & Cyber Security Trends in Africa.* United States: Symantec Corporation, pp. 60, 61, 63, 66, 70, and 83.

[139] *Id.* pp. 70, 83, 134.

[140] See n. 138, p. 10.

[141] See Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment*. United States: Solutions Consulting, p. 37.

[142] See African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa.* United States: Symantec Corporation, pp. 70, 76, 88, 89, and 92. See Serianu Limited (2016) *Africa Cybersecurity Report 2016*. Kenya: Serianu Limited, p. 46.

of cybersecurity initiatives has been responsible for the absence of expert personnel that would facilitate the development and implementation of national policy and regulatory frameworks for cybersecurity governance and also assist law enforcement authorities in the prevention, investigation or prosecution of cybercrime. In addition, poor funding has limited research and development initiatives that would promote regional cybersecurity governance within the AU. To some extent, the poor funding of cybersecurity initiatives by African governments has been caused by the fact that cybersecurity is not really considered as a national security priority in many African States. This is also not unconnected with the fact many African States face physical national security challenges such as terrorism which policy makers usually consider more pervasive than cybercrime and other cybersecurity challenges.[143]

Another major challenge that has hindered the application of the Convention's obligations as a framework for promoting regional cyber stability is the slow pace that has characterized both the signing and ratification of the Convention by Member States, and the development of national policy and regulatory frameworks for cybersecurity governance in many Member States. To some extent, the challenge of slow responses appears to characterize the development of ICT regulatory initiatives in Africa.[144] The slow pace of responses can be traced to factors including lack of awareness amongst policy makers and legislators in Member States,[145] which may have resulted from factors such as the lack of a broad consultation of key stakeholders that drive policy and legislative processes in Member States during the development of the Convention.[146] This is also compounded by lack of capacity in terms of expert personnel to drive

[143] See Shuaibu, M. and Bernsah, L.D. (2016) An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach. *Journal of Social and Management Sciences*, 2 (1), pp. 3, 4, 6. See Ploch, L. (2010) Countering Terrorism in East Africa: The U.S. Response. *Congressional Research Service*, R41473, p. 19. See Vanguard (2017) *Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama*. [online] Vanguard. Available from: https://www.vanguardngr.com/2017/02/fgcommittingsignificant-share-2017-budget-northeast-onyeama/ [Accessed 6 June 2018].

[144] See UNTCAD (2012) *Harmonizing Cyberlaw and Regulations: The Experience of the East African Community*. New York/Geneva: UNCTAD, pp. 8–9.

[145] See Seck, M. (2014) Tackling the Challenges of Cybersecurity in Africa. *United Nations Economic Commission for Africa Policy Brief*, NTIS/002/2014, p. 4. [online] Available from: https:///www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf [Accessed 6 June 2018]. See Serianu Limited (2016) *Africa Cybersecurity Report 2016*. Kenya: Serianu Limited, pp. 21–22. See Links F. (2018) Tackling Cyber Security/Crime in Namibia – Calling for a Human Rights Respecting Framework. *Democracy Report – Special Briefing Report*, 20, p. 4.

the development of national cybersecurity governance frameworks[147] which then results in much reliance on technical assistance from international organizations[148] and their consultants.[149] In practice, however, a country's request for such technical assistance from an international organization may not be timely, which further contributes in slowing down the pace of developing national policy and regulatory frameworks for cybersecurity governance in Member States that request assistance. National budget constraints also impede the timely development of national cybersecurity policy and regulatory frameworks in many Member States who are challenged by other development concerns which are considered priority areas that require increased government funding such as curbing the spread of HIV/AIDS, tackling widespread poverty, and promoting the sustainable exploitation of natural resources.[150]

The slow pace of responses can further be traced to the absence of a dedicated and effective regional institutional governance mechanism that would promote the ratification of the Convention by Member States and also monitor and facilitate the development of national cybersecurity governance frameworks. This state of affairs appears to be resulting in a poor regional coordination and harmonization of cybersecurity frameworks, while also limiting prospects for regional cybersecurity cooperation and the dissemination of best practices. In addition, the large size of the AU with its 55 Member States and their diverse national legal traditions, and how they receive and implement international treaties is also a major challenge to the effective application of the Convention

---

[146] See Open Forum to Discuss the Proposed Legal Framework for Cybersecurity in Africa. (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-on-the-draft-african-union-cyber-security-convention/#comment-4 [Accessed 6 June 2018].

[147] See Bertelsmann-Scott, T. (2013) Regional Cooperation in the Telecommunications Sector via CRASA. *PERISA Series*, p. 3.

[148] A study by the United Nations Office on Drugs and Crime (UNODC) indicates that all African States that responded to its questionnaire, requested technical assistance to build the capacities of law enforcement, prosecution and court authorities to prevent and combat cybercrime. See UNODC (2013) Comprehensive Study on Cybercrime. New York: United Nations, p. 178.

[149] See Calandro, E. S. *Regionalism and the Development of the Information Society: Policy Considerations from SADC*, p. 10. [online]. Available from http://www.cprsouth.org/wp-content/uploads/2015/08/CPRsouth2015_PP115FINAL_vReviewed.pdf [Accessed 6 June 2018].

[150] See Orji, U. J. (2018) *International Telecommunications Law and Policy*. United Kingdom: Cambridge Scholars Publishing, p. 369. See also, African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation, p. 60.

as a framework for promoting regional cyber stability and harmonizing cybersecurity governance measures in Member States.

7. RECOMMENDATIONS

Article 32 of the AU Cybersecurity Convention provides for the establishment of a monitoring and operational mechanism for the purpose of implementing the Convention. The responsibilities of the Convention's operational mechanism include:

> (a) promoting the adoption and implementation of measures to strengthen cybersecurity in electronic services and combating cybercrime and human right violations in cyberspace; and
> (b) advising African governments on measures to promote cybersecurity and combat cybercrime and human right violations in cyberspace at the national level.[151]

The Convention's regional monitoring mechanism has not yet being formally established. However, the above mandates under Article 32 of the Convention may be broadly interpreted to create a regional network agency that is similar to the European Information Security Agency (ENISA).[152] The ENISA was established in 2004 by the European Commission[153] 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 cybersecurity issues. Its responsibilities include providing advice and recommendations on cybersecurity and disseminating information on best practices.[154] Given that the slow pace which has characterized both the signing and ratification of the Convention by Member States and the development of national cybersecurity governance frameworks in many AU Member States can also be traced to the absence of a dedicated and effective regional institutional governance mechanism that would promote the ratification of the Convention by Member States and also monitor

[151] See Article 32 *AU Convention on Cybersecurity and Personal Data Protection*.

[152] See Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In: Maybaum, M. et al. (eds.) *Architectures in Cyberspace - 7th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE, p. 116.

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

[154] See ENISA (2018) Available from: http://www.enisa.europa.eu/ [Accessed 6 June 2018].

the development of national cybersecurity governance frameworks, it appears imperative for the AU to formally set up the regional monitoring mechanism established under Article 32 of the Convention. This is also necessary in order to improve the regional coordination and harmonization of cybersecurity governance frameworks, while also increasing prospects for regional cybersecurity cooperation and the dissemination of best practices. Such a measure would go a long way towards harnessing the application of the Convention as a framework for promoting regional cyber stability. In addition, it is imperative for African States to take other measures such as: promoting cybersecurity governance as a core regional security priority; improving the funding of cybersecurity capacity building initiatives to enhance the development of a pool of skilled personnel; promoting awareness amongst policy makers and legislators; and, improving funding for national cybersecurity initiatives including the operation of National CERTs/CSIRTS and law enforcement institutions.

8. CONCLUSION

Africa still lacks efficient capacities and resources for cybersecurity governance. This absence of capacities and resources remains a major factor that has contributed to creating an enabling environment for rising cybercrime trends in African States.[155] The adoption of the AU Cybersecurity Convention indicates Africa's awareness of cybersecurity concerns and also signals its interest in promoting cyber stability at least from a regional perspective. However, while there is no doubt that the AU Cybersecurity Convention seeks to promote regional cyber stability, the achievement of this objective is dependent on the timely implementation obligations that arise from the Convention, as well as on the ability of the AU to coordinate and monitor its implementation by Member States. In order to achieve such desired outcomes, the AU and its Member States may have to consider taking timely steps towards addressing the highlighted challenges that impede the application of the Convention as a framework for promoting regional cyber stability.

[155] See Flores, R. et al. (2017) *Cybercrime in West Africa: Poised for an Underground Market*. United States: Trend Micro and INTERPOL, p. 3. See also, Kharouni. L. (2013) *Africa: A New Safe Harbour for Cyber Criminals?* Trend Micro Research Paper. United States: Trend Micro Inc. pp. 1–26.

LIST OF REFERENCES

[1] *African (Banjul) Charter on Human and Peoples' Rights*, 27 June 1981 (OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58).

[2] *African Charter on the Rights and Welfare of the Child*, 29 November 1999 (OAU Doc. CAB/LEG/24.9/49)(1990).

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

[4] African Union. (2017) *African Union in a Nutshell*. [online] Available from: http://www.au.int/en/abut/nutshell [Accessed 6 June 2018].

[5] African Union. (2017) *Member States*. [online] Available from: http://www.au.onlinet/en/member_states/country profiles [Accessed 6 June 2018].

[6] African Union. (2018) *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.* [online] Available from: https//au.int/sites/default/files/treaties/29560slafrican_union_convention_on_cybe_security_and_personal_data_protection.pdf [Accessed 6 June 2018].

[7] African Union (AU). Available from: http://www.au.int/en/ [Accessed 6 June 2018].

[8] African Union and Symantec Corporation (2016) *Cyber Crime & Cyber Security Trends in Africa*. United States: Symantec Corporation.

[9] *African Union Convention on Cyber Security and Personal Data Protection*, 27 June 2014 (EX.CL/846 (XXV).

[10] Bertelsmann-Scott, T. (2013) Regional Cooperation in the Telecommunications Sector via CRASA. *PERISA Series*.

[11] Brommelhorster, J. et al. (2004) Critical Infrastructure Protection: Survey of World-wide Activities. *BSI KRITIS*, (4).

[12] Calandro, E.S. Regionalism and the Development of the Information Society: Policy Considerations from SADC. [online] Available from http://www.cprsouth.org/wp-content/uploads/2015/08/CPRsouth2015_PP11FINAL_vReviewed.pdf [Accessed 6 June 2018].

[13] *Constitution of Cape Verde* (1992).

[14] *Constitution of Ghana* (1992).

[15] *Constitution of Liberia* (1986).

[16] *Constitution of Senegal* (2001).

[17] *Constitution of Sierra Leone* (1991).

[18] *Constitution of the Federal Republic of Nigeria* (1999).

[19] *Constitution of the Gambia* (1997).

[20] *Constitution of the Republic of Benin* (1990).

[21] *Constitutive Act of the African Union*, 11 July 2000.

[22] Coomans, F. (2003) The Ogoni Case before the African Commission on Human and Peoples' Rights, *International and Comparative Law Quarterly*, vol. 52.

[23] Council of Europe (1976) *Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*. Strasbourg.

[24] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks against Information Systems and replacing Council Framework Decision 2005/222/JHA, *Official Journal of the European Union.*

[25] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, *Official Journal of the European Union.*

[26] Dunn, M. (2005) A Comparative Analysis of Cybersecurity Initiatives Worldwide. *World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity*. Geneva: ITU.

[27] Economic Commission for Africa (2012) *Declaration of Addis Ababa on the Harmonization of Cyber Legislation in Africa*. Addis Ababa: Economic Commission for Africa.

[28] Editorial (1941) The Trail Smelter Arbitral Decision. *American Journal of International Law*.

[29] European Commission (1999) *Towards a New Framework for Electronic Communications Infrastructure and Associated Services.* Brussels: European Commission.

[30] Flores, R. et al. (2017) *Cybercrime in West Africa: Poised for an Underground Market*. United States: Trend Micro and INTERPOL.

[31] *Free Legal Assistances Group and Others v. Zaire*, ACHPR/COMM, No. 25/89, 47/90, 56/91, 100/93 (1995).

[32] Garner, B. A. (ed.) (2004). *The Black's Law Dictionary*. 8th ed., St Paul MN, United States: West Publishing Co.

[33] Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[34] Gordon, K. and Dion, M. (2008) *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*. Paris: OECD.

[35] GSMA (2013) *Sub-Saharan Africa Mobile Economy Report 2013.* London: A.T. Kearney.

[36] GSMA (2013) *The Mobile Economy Report 2013*. London: A.T. Kearney.

[37] GSMA (2016) *The Mobile Economy Africa 2016*. London: GSMA.

[38] Hansungule, M. African Courts and the African Commission on Human and Peoples' Rights. In: Bosi, A. and Diescho, J. (2009) *Human Rights in Africa: Legal Perspective on their Protection and Promotion*. Namibia: Macmillan Education.

[39] *I. v. Finland* (2008), Judgment of 17 July 2008 (No. 20511/03, ECHR).

[40] *International Penn & Others (on behalf of Saro-Wiwa) v. Nigeria (*1998), ACHPR/COMM, 137/94, 139/94, 154/96, 161/97 .

[41] ITU (2009) *National Cybersecurity/CIIP Self-Assessment Tool*. Geneva: ITU.

[42] ITU (2018) *Cybersecurity Country Profiles* [online] Available from: https//www.itu/en/ITU -D/Cybersecurity/Documents/Country_Profiles/ [Accessed 6 June 2018].

[43] ITU High Level Experts Group (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU.

[44] ITU High Level Experts Group [HLEG] (2008) *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*. Geneva: ITU.

[45] *ITU Toolkit for Cybercrime Legislation*. Geneva: ITU.

[46] *K.U. v. Finland* (2008), Judgment of 2 December 2008 (No. 2872/02ECHR).

[47] Kharouni. L. (2013) Africa: A New Safe Harbour for Cyber Criminals? *Trend Micro Research Paper*. United States: Trend Micro Inc.

[48] Links F, (2018) Tackling Cyber Security/Crime in Namibia – Calling for a Human Rights Respecting Framework. *Democracy Report – Special Briefing Report*.

[49] Magliveras, K. D. (2011) The Sanctioning System of the African Union: Part Success, Part Failure?, *The African Union: The First Ten Years*. Addis Ababa: Institute of Security Studies, 11–13 October 2011.

[50] Marco, G. (2009) *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU.

[51] Miniwatts Marketing Group (2017), *Internet Usage Statistics for Africa*. [online] Miniwatts Marketing Group. Available from: http://www.internetworldstats.com/stats1.htm [Accessed 6 June 2018].

[52] Mkhize, S. (2014) *Assessing the Efficacy of the AU Sanctions Policies with Regard to Unconstitutional Changes in Government: The Examples of Guinea and Madagascar.* M.A. University of South Africa.

[53] Oji, E. A. (2011) Application of Customary International Law in Nigerian Courts. *Nigeria Institute of Advanced Legal Studies Law and Development Journal*, vol. 1, no. 1.

[54] *Oliver Tambo Declaration* (2009).

[55] *Open Forum to discuss the proposed legal framework for cybersecurity in Africa*, (26 July 2013) [online] Available from: http://daucc.wordpress.com/2013/07/26/event-panel-discussion-

on-the-draft-african-union-cyber-security-convention/#comment-4
[Accessed 6 June 2018].

[56] Oppong, R. F. (2008) Making Regional Economic Laws Enforceable in National Legal Systems: Constitutional and Judicial Challenges. In: Bosi, A. and Breytenbech, W. et al. (eds.) *Monitoring Regional Integration in Southern Africa Year Book*. Stellenbosch, South Africa: Trade Law Center for Southern Africa.

[57] Orji, U. J. (2012) 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*, vol. 17, no. 4.

[58] Orji, U. J. (2012) *Cybersecurity Law and Regulation*. Nijmegen, Nijmegen: Wolf Legal Publishers.

[59] Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. *Computer Law Review International*, vol. 5.

[60] Orji, U. J. (2015) Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In: Maybaum, M. et al. (eds.) *Architectures in Cyberspace – 7th International Conference on Cyber Conflict*. Tallinn: NATO CCD COE.

[61] Orji, U. J. (2016) Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses. In: Samuel, C. and Sharma, M. (eds.) *Securing Cyberspace: International and Asian Perspectives.* New Delhi, India: Institute for Defence Studies and Analyses & Pentagon Press.

[62] Orji, U. J. (2018) *International Telecommunications Law and Policy*. United Kingdom: Cambridge Scholars Publishing.

[63] Ploch, L. (2010) Countering Terrorism in East Africa: The U.S. Response. *Congressional Research Service*, R41473.

[64] *Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa*, 11 July 2003.

[65] *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, 10 June 1998.

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

[67] Rosewarne, C. and Odunfa, A., (2014) *The 2014 Nigerian Cyber Threat Barometer Report.* South Africa and Nigeria: Wolfpack Information Risk and Digital Jewels.

[68] Rudnick, L. et al. (2015) *Towards Cyber Stability: A User-Centered Tool for Policy Makers*. Geneva: United Nations Institute for Disarmament Research.

[69] Schjolberg, S. (2008) *The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva* (2008). [online] Available from: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf [Accessed 6 June 2018].

[70] Seck, M. (2014) Tackling the Challenges of Cybersecurity in Africa. *United Nations Economic Commission for Africa Policy Brief*, NTIS/002/2014.

[71] Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) *Telecommunications Law and Regulation*. 3rd ed. New York: Oxford University Press.

[72] Shuaibu, M. and Bernsah, L.D. (2016) An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach. *Journal of Social and Management Sciences*, vol. 2, no. 1.

[73] Shuma, T. (2015) Revisiting Legal Harmonization under the Southern African Development Community Treaty: The Need to Amend the Treaty. *Law, Democracy and Development*, vol. 19.

[74] *Social and Economic Rights Action Center (SERAC) and the Center for Social and Economic Rights (CESR) v. Nigeria* (2002), Communication No. 155/96, ACHPR/COMM/A044/1.

[75] Solutions Consulting (2018) *West Africa Cybersecurity Indexing and Readiness Assessment.* Florida, United States: Solutions Consulting.

[76] *The Corfu Channel Case (United Kingdom v. Albania),* (1949), Merits, ICJ Reports.

[77] *The Council of Europe Convention on Cybercrime* (2001), 41 I.L.M. 282.

[78] *The Trail Smelter Arbitration Case (United States of America v. Canada)*, (1938) 3 R.I.A.A.

[79] UNCTAD 2018) *Cybercrime Laws.* [online] Available from: http://www.unctad.org/en/Docs/Cyberlaw/CC.xlsx [Accessed 6 June 2018].

[80] UNECA Press Release, *ICT Ministers call for harmonized policies and cyber legislations on Cybersecurity*. [online] Available from: http://www1.uneca.org/ArticleDetail/tabid/3018/ArticleId/1934/ICT-Ministers-call-for-harmonized-policies-and-cyberlegislationson Cybersecurity.aspx [Accessed 6 June 2018].

[81] United Nations Economic Commission for Africa (UNECA) Press Release, *Draft African Union Convention on Cybersecurity Comes to its Final Stage*. [online] Available from: http://www1.uneca.org/TabId/3018/Default.aspx?ArticleId=1931 [Accessed 6 June 2018].

[82] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 20 December 2003, (A/RES/57/239).

[83] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 21 December 2009 (A/RES/64/211).

[84] United Nations Resolution on the Creation of a Global Culture of Cybersecurity, 23 December 2003 (A/RES/58/199).

[85] United States President's Commission on Critical Infrastructure Protection (PCCIP). (1997) *Critical Foundations: Protecting America's Infrastructure*. Washington DC: PCCIP, Appendix B, Glossary B-2.

[86] UNODC (2013) *Comprehensive Study on Cybercrime*. New York: United Nations.

[87] UNTCAD (2012) *Harmonizing Cyberlaw and Regulations: The Experience of the East African Community*. New York/Geneva: UNCTAD.

[88] Van Zyl, G. (2014) Adoption of 'flawed' AU Cybersecurity Convention Postponed. *IT Web Africa*, 21 January. [online] Available from: http://www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed [Accessed 6 June 2018].

[89] Vanguard (25 February 2017) *Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama.* [online] Vanguard. Available from: https://www.vanguardngr.com/2017/02/fg-committing-significant-share-2017-budget-northeast-onyeama/ [Accessed 6 June 2018].

[90] *Vienna Convention on the Law of Treaties*, 23 May 1969.

[91] Walter, J. K. (1974) Comparative Law: A Theoretical Framework. *International and Comparative Law Quarterly*, vol. 23, no. 3.