Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa

Uchenna Jerome Orji, Ph.D.[*]
Assistant Professor
School of Law
American University of Nigeria

Abstract

Measures to address the security challenges of the information society have given rise to the concept of cybersecurity governance. One major aspect of cybersecurity governance is the establishment of legal measures to criminalize and deter malicious acts that affect the integrity, confidentiality, availability and security of digital data and computer systems. Accordingly, several States and intergovernmental organizations across the world have established legal frameworks to promote cybersecurity governance. This is also the case in Africa. The African Union has adopted a Convention on Cyber Security and Personal Data Protection, while other African regional intergovernmental organizations such as the Economic Community of West African States, the Common Market for Eastern and Southern Africa and the Southern African Development Community have established legal and policy frameworks for cybersecurity governance. In addition, many African States have developed legal and policy frameworks to promote cybersecurity, while some others in the process of developing such frameworks. However, most of Africa's responses to cybersecurity governance have been focused on the establishment of criminal law measures. Yet while the establishment of criminal law measures is regarded as a critical component of cybersecurity governance, the isolated existence of such measures may not produce desirable outcomes in terms of minimizing cybersecurity vulnerabilities in Africa's information society. This paper seeks to make a case for the development of other critical components of cybersecurity governance, including technical and organizational measures and user education. It suggests that 'stand-alone' criminal law measures will not be able to reduce the rising trends of cyber-criminality in Africa, and that the timely development of other critical components of cybersecurity governance is imperative especially due to the peculiar challenge of weak law enforcement capacities and justice delivery systems in many African States.

Keywords

Africa, Cybercrime, Cybersecurity Governance Measures, Law, Policy

[*] Direct correspondence to Uchenna Jerome Orji, Ph.D., Assistant Professor, School of Law, American University of Nigeria; e-mail: jeromuch@yahoo.com; uchenna.orji@aun.edu.ng.

[*] http://dx.doi.org/10.36889/IJCJ.2021.002.
[*] Received 15 Nov 2020; Revised 19 March 2021; Accepted 13 April 2021; Available online 26 April 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 60-98

INTRODUCTION

During the 20th century advances in information and communications technologies brought about the convergence of telecommunications and computer technologies. This signified the beginning of an era known as the information age. A very distinctive feature of the information age is the continuous integration of computers and digital communication technologies in virtually all aspects of life and critical services that support modern societies and the tendency towards “connecting everything to everything”.[1] This has given rise to the emergence of the information society. However, with the emergence of the information society, the security of computer systems, digital data, digital communication technologies and networks now have an overwhelming influence on almost all aspects of life in modern societies. Malicious acts that target computer systems and their networks now have the potential of affecting individuals, countries and the global economy in ways previously unimagined. In particular, the most critical challenges of the information society have been the security of computer systems and digital data and the prevention of the malicious misuse of information communications technologies by criminals, terrorist groups, or State actors. Measures to address these security challenges of the information society have given rise to the concept of cybersecurity governance.

One major aspect of cybersecurity governance is the establishment of legal measures to criminalize and deter malicious acts that affect the integrity, confidentiality, availability and security of digital data and computer systems. Accordingly, several States and intergovernmental organizations across the world have established legal and policy frameworks to promote cybersecurity governance. In Africa, Internet penetration has also raised concerns on the need to strengthen cybersecurity and prevent Africa from becoming a “safe harbour” for cybercrime.[2] There are also concerns over the negative impact of cybercrime on African economies. For example, a survey conducted on Nigeria which has the largest Internet User population in Africa estimates that the country annually loses around

[1] M. Dunn, A Comparative Analysis of Cybersecurity Initiatives Worldwide, World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, Geneva, ITU: June 2005, p.5.

[2] L. Kharouni, ‘Africa: A New Safe Harbour for Cyber criminals?”, Trend Micro Research Paper, Trend Micro Inc: USA, 2013, pp.1-26.

13 Billon US Dollars to cybercrime including loss of potential foreign investments.[3] South Africa is also reported to annually lose over 5.7 Billion Rand due to cybercrime,[4] while Norton reports that 70 percent of South Africans have fallen victim to cybercrime compared with a global average of 50 percent.[5] It is estimated that cyber-attacks cost African businesses around 1.048 billon US Dollars a year.[6] To address cybersecurity governance concerns and promote the control of cybercrime, the African Union (AU) adopted a Convention on Cyber Security and Personal Data Protection, while African regional intergovernmental organizations such as the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have all established legal frameworks for cybersecurity governance. In addition, many African States have developed legal and policy frameworks for cybersecurity governance, while some States are in the process of developing such frameworks. However, most of Africa’s responses to cybersecurity governance have focused on the establishment of criminal law measures. While there is no doubt that the establishment of criminal law measures is an essential component of cybersecurity governance, the isolated existence of such measures may not produce desirable outcomes in terms of minimizing cybersecurity vulnerabilities in Africa’s information society.

This paper makes a case for the development of other critical components of cybersecurity governance including technical and organizational measures and user education. It suggests that ‘stand-alone’ criminal law measures will not reduce rising trends of cyber-criminality in Africa and that the timely development of other critical components of cybersecurity governance is imperative especially due to the peculiar challenge of weak law enforcement capacities and justice delivery

[3] G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, p.11, available at < https://pinigeria.org/download/download/cybercost.pdf> last accessed on 18 March, 2021.

[4] T. Mastile, ‘South Africa Loses R.5.7 Billion Annually to Cybercrime’, CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime> last accessed on 18 March, 2021.

[5] T. Jackson, ‘Can Africa Fight Cybercrime and Preserve Human Rights?’, BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

[6] Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa’s Cyber Security Poverty Line (Kenya: Serianu Limited, 2017), p.3.

systems in many African States.

The paper is divided into six sections. The first section which includes this introduction examines the concept of cybersecurity and the major components of cybersecurity governance. The second section looks at Africa's cybersecurity threat landscape. The third section presents an overview of African responses to cybersecurity governance. The fourth section examines current challenges to cybersecurity governance in Africa. The fifth section makes proposals for the development of other critical aspects for cybersecurity governance aside from criminal law measures. The conclusion then follows.

Cybersecurity

Cybersecurity is an information age terminology that was derived by merging the prefix – 'cyber' with the concept of 'security'. The term is defined as "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assets".[7][8] Cybersecurity also refers to the following:

(1) "a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security;

(2) the degree of protection resulting from the application of these activities and measures;

(3) the associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality".[9]

Cybersecurity is primarily concerned with protecting the cyberspace and information communications technologies from all forms of cyber threats. Within

[7] ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU 2008, p.27.

[8] U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012, pp.10-16.

[9] M. Dunn, A Comparative Analysis of Cybersecurity Initiatives Worldwide, World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, Geneva, ITU: June 2005, p.4.

the context, “cyber threats” refer to malicious acts that are perpetrated in the electronic environment known as the ‘cyberspace’ and other species of malicious acts that target information communication technologies. These have been classified into the following forms of threats: threats to individual users such as viruses or identity theft, as well as annoyances such as spam, spyware or pop-ups; threats to businesses, governments or other organizations, for instance, through the exploitation of vulnerabilities in their data storage, industrial espionage or denial of service etc; threats to critical public infrastructure such as electronic communication networks, financial systems, emergency services, navigation systems, electrical power grids, air traffic control, and water control systems etc.[10)]

Cybersecurity Governance

The concept of governance[11)] basically refers to the organized control or direction of activities, States, societies, individuals and organizations to achieve desired objectives. To a large extent, the definition of the concept of governance would vary in meaning depending on the context in which it is used. For example, “governance” has been defined as a government's “ability to make and enforce rules and to deliver services”.[12)] Governance has also been defined as referring to structures and processes designed to ensure accountability, transparency, responsiveness, rule of law, stability, and also represent the norms, values and rules through which public affairs are managed in a responsive and transparent manner.[13)] Another definition refers to governance as “the conscious management of regime structures, with a view to enhancing the public realm”.[14)] Since 1990s, the term ‘governance’ has acquired the status of a generalized concept to classify the act of regulation and has been applied by institutions, States, policy-makers,

[10)] ITU, ‘Challenges to Building a Secure Information Society’, 2007 World Information Society Report: Beyond WSIS, ITU, Geneva, 2007, p. 83.

[11)] The word “governance” originates from the Latin word “gubernare,” which means “to steer. See M. M. Tamayao, What Is Governance?, available at <https://tamayaosbc.wordpress.com/2014/08/ 21/what-is-governance/> last accessed on 18 March, 2021.

[12)] F. Fukuyama, ‘What Is Governance?’, CGD Working Paper 314 (Washington, DC: Center for Global Development, January 2013), p.3.

[13)] International Bureau of Education, ‘Concept of Governance’, available at <http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance> last accessed on 18 March, 2021.

[14)] ‘Understanding the Concept of Governance’, available at <https://www.gdrc.org/u-gov/governance-understand.html> last accessed on 18 March, 2021.

researchers and other commentators to diverse aspects of human endeavour.[15] When placed within the cybersecurity context, the concept of governance would generally encompass the establishment, implementation and monitoring of a broad range of measures and activities technical and non-technical, including legal, policy and institutional measures intended to protect computers, computer networks, related hardware and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security. As such, cybersecurity governance concerns the establishment and effective implementation of technical and non–technical measures (including legal and policy measures, institutional measures, end user education and research and development) that aim to promote cybersecurity, as well as the monitoring of such measures to achieve desired objectives.

Cybercrime

Malicious acts which are prohibited by cybersecurity laws are commonly referred to as 'cybercrime' or 'computer crime'. These terms are often used interchangeably to refer to instances where computer technologies are the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. However, there is no universally accepted legal definition of cybercrime or computer crime[16] and cybersecurity laws generally tend to avoid such explicit definitions. For example, the African Union Convention on Cyber Security and Data Protection[17] and the Council of Europe Convention on Cybercrime[18] does not explicitly define the terms 'cybercrime' or 'computer crime'. However, the Council of Europe Convention on Cybercrime criminalize a range of acts in its Articles 2-10 on substantive criminal law in four different categories, namely:

[15] J. Graham, B. Amos and T. Plumptre, Governance Principles for Protected Areas in the 21st Century 5 (Ottawa: Institute of Governance, 2003) p. 2-7; D. Olowu, 'Environmental Governance Challenges in Kiribati: An Agenda for Legal and Policy Responses', Law, Environment and Development Journal (2007) Vol .3, Issue 3, p.259.

[16] U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012, pp.17-19.

[17] The African Union Convention on Cyber Security and Personal Data Protection EX.CL/846 (XXV) adopted by the 23rd Ordinary Session of the African Union Assembly, Malabo, 27 June, 2014.

[18] The Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

(1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences, and;
(4) offences related to infringement of copyright and related rights.

The above categories of offences under Convention are regarded as establishing a minimum universal standard of what can be classified as cybercrime or computer crime.[19]

Cybersecurity basically appears a broader concept than cybercrime. For example, while cybercrime control measures aim to criminalize and tackle intentional acts that impair the confidentiality, integrity and availability of computer data and systems. On the other hand, cybersecurity governance measures seek to address non-intentional cyber incidents including natural disasters and accidents that affect information communication technology (ICT) infrastructure, as well as intentional attacks against the confidentiality, integrity and availability of computer systems and data offences and any offences involving electronic evidence.[20]

Critical Components of Cybersecurity Governance

Cybersecurity governance encompasses multi-disciplinary components including but not limited to legal measures, technical measures, institutional/organizational measures, end user education and research and development. These components are discussed below.

Legal measures

This component covers all legal aspects of cybersecurity governance and it is usually regarded as probably the most relevant aspect especially in the control of cybercrime.[21] This aspect entails the establishment of adequate legal measures such as laws, regulations, and policies to criminalize instances where computer systems, digital technologies or critical information infrastructure are the target of

[19] S. Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva', (2008), pp. 8-9, available at <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf> last accessed on 18 March, 2021.

[20] UNODC, Comprehensive Study on Cybercrime (Draft – February 2013), United Nations, New York, 2013, p.228.

[21] G. Marco, Understanding Cybercrime: A Guide for Developing Countries, ITU, Geneva, 2009, p.84. See also G. Marco, 'The Slow Wake of a Global Approach against Cybercrime', Computer Law Review International, 2006, Issue 5, p. 141.

a malicious activity, or where computer systems or digital technologies are the instrument for facilitating a malicious activity. The establishment of legal measures for cybersecurity governance is usually best approached through the enactment of new laws that are drafted in a technology neutral[22] language. This approach enables legal regulation to keep up with new technological developments and emerging trends in the criminal misuse of information technologies. Legal aspects of cybersecurity governance also cover issues relating to procedures for investigating cybercrimes, the handling of evidence and prosecution of cybercrimes, and the development of international cooperation mechanisms for controlling cybercrime and responding to cybersecurity incidents.[23]

Technical measures

The technical aspects of cybersecurity governance cover the development and implementation of technical protection measures for computer systems and network infrastructure. Generally, computer systems or digital technologies that are well protected are hard to attack or penetrate. Technical protection measures are usually implemented based on a computer's security architecture through the use of tools such as fire walls, passwords or synchronized passwords, voice or fingerprint identification or retinal and biometric access protocols, antivirus software and real time intrusion detection software. Technical aspects of cybersecurity governance also include the development and implementation of active countermeasures to secure computers and digital technologies. An example is the use of software bombs by software developers to secure software. Software bombs are sometimes built into software by developers as a means of enforcing payment in the event of a dispute[24] or for the purpose of curtailing unauthorized access or distribution of such software. However, the use of such active countermeasures may be unlawful in some jurisdictions.[25]

[22] Technological neutrality is a regulatory principle that implies that legislation should define the objectives 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 C. Reed, 'The Law of Unintended Consequences ‒ Embedded Business Models in IT Regulation', Journal of Information Law and Technology, 2007 (2), p.2.

[23] U. J. Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?' in M. Maybaum, et al (eds.), Architectures in Cyberspace- 7th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, Estonia, pp.110-112.

[24] T.J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1), p.7.

Institutional/Organizational measures

This component of cybersecurity governance deals with the development of institutional capacities to promote cybersecurity. It includes the establishment of law enforcement organizations as well as the development of the capacities of such organizations to prevent and detect cybercrime or enforce cybersecurity laws. This aspect of cybersecurity governance also includes the establishment of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)[26] to manage cybersecurity incidents by providing prevention, early warning, detection, reaction and crisis management platforms. CERTs are usually responsible for a range of functions which include:

(1) monitoring cybersecurity threats and issuing early warnings of such threats;
(2) effectively responding to emergencies arising from threats against computer systems and critical information infrastructure and;
(3) providing security analysis of potential vulnerabilities against computer systems.[27]

A CERT may be established by a national government or a private organization or through public–private partnership arrangements.[28] However, the responsibilities of a national CERT are broader than that of a private organization, because a national CERT is usually responsible for coordinating national emergency responses to cyber threats and establishing related best practices within a State.[29]

End-user education

The individual operating a computer system is usually regarded as the weakest link in the cybersecurity chain.[30] Hence, end-user education is regarded as a vital

[25] Rubicon Computer Systems v. United Paints Limited (2000) 2 TCLR 453. See T. J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1), p.7. See also T. Sewart, 'Time to Drop the Bomb', *Computers & Law*, 2003 Vol.14 (4), p.22.

[26] The terms 'CERT' and 'CSIRT' are used interchangeably. See ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU: 2008, p.96.

[27] *Ibid*, pp. 96-97.

[28] *Ibid*, pp. 94-96.

[29] ITU Study Group Q.22/1, Report on Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts [Draft], Geneva, ITU-D, January 2008, p. 39/71.

[30] ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU: 2008, p.31.

component of cybersecurity governance. Computer users are usually the major target of criminals in the cyber environment. This is because, it is usually easier to attack private computers to obtain sensitive financial information rather than the well protected computer systems of a financial institution.[31] Also, cybercrimes such as phishing, spoofing and e-mail scams[32] are usually successful not because of the absence of technical cybersecurity measures, but rather due to a victim's lack of awareness.[33] Accordingly, it has been aptly observed that: "if users are aware that their financial institutions will never contact them by E-mail requesting passwords or bank accounts details they cannot fall victim to phishing or identity fraud attacks".[34]

User education in the cybersecurity context involves the education of end-users of computer systems and digital technologies on the risks they face in the information society so as to enable them manage such risks. User education can be undertaken through several avenues such as public enlightenment campaigns, lessons in schools, ICT centers, universities, and ICT equipment user guide provided by manufacturers or service providers. Organizations that can play strategic roles in promoting end-user education include network service providers, manufacturers of ICT equipment, financial institutions, non-governmental organizations, schools and CERTs.

Research and development

This component of cybersecurity governance deals with the promotion of research on cybersecurity issues. Relevant research topics in cybersecurity governance range from legal and policy issues to technical, social and national security issues. Cybersecurity governance has already become a major research issue in developed countries with a great deal of research being undertaken by States organs (including law enforcement and military institutions), private sector research institutes and the research institutes of universities and international organizations. For example, international organizations such as the NATO Cooperative Cyber Defense Center of Excellence, the International Telecommunication Union (ITU), and the Council of Europe have been very active in researching cybersecurity governance issues.

[31] G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009, p.86.

[32] One the most common forms of e-mail scams in the cyberspace is the Nigerian email Scam commonly known as Yahoo-Yahoo in Nigeria. This term derives its origin from Yahoo mail a popular free email service provider on the Internet.

[33] G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009, p.86.

[34] G. Marco, ibid, p.87.

AFRICA'S CYBERSECURITY THREAT LANDSCAPE

The increasing penetration of information communication technologies (ICTs) in Africa[35] has naturally given rise to their growing integration in critical national sectors.[36] For example, banking and financial services sectors in African States are increasingly integrating ICTs to enhance service delivery and improve consumer satisfaction.[37] Also, across several African States, critical sectors including transportation, energy, health, immigration services, education and manufacturing are increasingly deploying ICTs in their operations.[38] This increasing integration of ICTs in critical national sectors is also seen a means of facilitating Africa's economic development and regional integration.[39] 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 national sectors on information infrastructure to the extent that the disruption of such infrastructure by accidents or cyber-attacks will cause the disruption of economic and social activities and public services in a manner that could trigger serious national security concerns. For example, while mobile phone banking innovations and platforms has enhanced the penetration of financial services to unbanked individuals, while further increasing financial flows and ecommerce across African countries, there are also increased chances that such platforms and institutions that operate them can suffer cyber-attacks.[40] In South Africa alone, an average of over 19, 842 cyber –attacks are daily

[35] GSMA, The Mobile Economy Africa 2020 (GSMA: London, 2020) pp. 2, 8 &19. See also, Miniwatts Marketing Group, 'Internet Usage Statistics for Africa', (31 December, 2020), available at <http://www.internetworldstats.com/stats1.htm> last accessed on 18 March, 2021.

[36] S. R. Ponelis and M. A. Holmer, 'ICT in Africa: Building a Better Life for all', Information Technology for Development (2015)B. T. Mbatha, D.N. Ocholia and J.L. Roux, 'Diffusion of ICTs in Selected Government Departments in KwaZulu –Natal, South Africa', Information Development, (2011) , Vol. 27 (4), pp251-263.

[37] M. K. Luka and I. A. Frank, 'The Impacts of ICTs on Banks: A Case Study of the Nigerian Banking Industry', International Journal of Advanced Computer Science and Applications (2012), Vol. 3 (9), pp.145-150; M. Andrianaivo and Kangni Kpodar, 'ICT, Financial Inclusion, and Growth: Evidence from African Countries', *IMF Working Paper*, WP/11/73 (2011), pp.4-41

[38] P. Wallet, Information and Communication Technology (ICT) in Education in Sub-Saharan Africa: A Comparative Analysis of basic e-readiness in Schools (UNESCO Institute for Statistics: Canada, 2015), pp.5-25; R. Bahrini and A. Qaffas, 'Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries', Economies (March, 2019) Vol. 7 (21), pp.1-13.

[39] U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p.237.

reported on ecommerce platforms.[41] This is observed as a major factor that degrades consumer confidence in terms of the widespread adoption of ecommerce services in Africa.[42] Recent research also indicate that attacks on critical infrastructure are becoming "frequent" in Africa with banks particularly being the common targets and losing billions of dollars to theft and service disruption.[43] As such, there is no doubt that African States are also vulnerable to cybersecurity threats which affect elements of critical sectors that rely on information infrastructure.

In addition, the increasing spread of ICTs and Internet penetration within Africa around the first decade of the 21st century also brought about the migration of advance fee fraud scammers to Internet platforms, with some African countries being classified as major sources of Internet advance fee fraud email scams.[44] Aside from email fraud scams, there has also been a growing trend in perpetration of other sophisticated forms of cybercrime such as hacking, credit card scams, identity theft, web cloning, phishing, Business Email Compromise fraud, and tax scams.[45] A survey conducted by the INTERPOL amongst its member countries in West Africa (including Benin, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Liberia, Mauritania, Niger, Nigeria, Senegal, and Sierra Leone) revealed that cybercriminals in the West African region have gained a high level of expertise in committing crimes against individuals and businesses.[46] A report by Trend Micro report indicates the rise of an underground cybercrime economy in West Africa due to the constant increase in the volume of cybercrime-related complaints received by law enforcement agencies in the region.[47]

There are also concerns over the negative impact of cyber-attacks on African

[40] I. Gagliardone and N. Sambuli, 'Cyber Security and Cyber Resilience in East Africa', Global Commission on Internet Governance Paper Series, No. 15 (May, 2015), p.1.

[41] A. A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html> last accessed on 18 March, 2021.

[42] Ibid.

[43] N. Allen, 'Africa's Evolving Cyber Threats', African Center for Strategic Studies, (19 January, 2021), available at <https://africacenter.org/spotlight/africa-evloving-cyber-threats/> last accessed on 18 March, 2021.

[44] Internet Crime Complaint Center, 2010 Internet Crime Report (National White Collar Crime Center: United States, 2011) p.11; Internet Crime Complaint Center, 2013 Internet Crime Report (National White Collar Crime Center: United States, 2014) pp. 15 & 21.

[45] R. Flores, et al, Cybercrime in West Africa: Poised for an Underground Market (Trend Micro and INTERPOL, 2017) p.3.

[46] Ibid, pp.12-13.

[47] Ibid, p.4.

economies. For example, South Africa is also reported to annually lose over 5.7 Billion Rand due to cybercrime,[48] while Norton reports that 70 percent of South Africans have fallen victim to cybercrime compared with a global average of 50 percent.[49] A survey conducted on Nigeria which has the largest Internet User population in Africa estimates that the country annually loses around 13 Billon US Dollars to cybercrime including loss of potential foreign investments.[50] Another report published by the United States based Center for Strategic and International Studies (CSIS) on the global economic impact of cybercrime estimates that about 0.08 percent of Nigeria's gross domestic product (GDP) is lost to cybercrime.[51] In Ghana, the Cybercrime Unit of the Police Service Criminal Investigation Department reported that 230 million US Dollars was lost due to cybercrime cases between 2016 and August, 2018.[52] Ghana's Cybercrime Unit also estimates that the country annually loses an average of 166 million US Dollars to cybercrime.[53] The annual financial cost of cybercrime in Senegal is estimated at 27 million US Dollars;[54] while Kenya which is East Africa's central information technology hub is estimated to annually lose over 295 million US Dollars to cybercrime.[55] It has been generally estimated that cyber-attacks cost African businesses around 1.048 billon US Dollars a

[48] T. Mastile, 'South Africa Loses R.5.7 Billion Annually to Cybercrime', CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime> last accessed on 18 March, 2021.

[49] T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

[50] G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, p.11, available at < https://pinigeria.org/download/download/cybercost.pdf> last accessed on 18 March, 2021.

[51] Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime (Center for Strategic and International Studies: Washington, DC, June, 2014) pp.9 and 21.

[52] G. Akweiteh Allotey, 'Ghana Loses $230 Million to Cyber Criminals – CID', Citinews (4 October, 2018), available at <https://citinewsroom.com/2018/10/04/ghana-loses-230m-to-cyber-criminals-cid/> last accessed on 18 March, 2021.

[53] 'Cybercrime Impact and the Way Forward', Business & Financial Times Online (5 November, 2018), available at <https://www.thebftonline.com/2018/features/cybercrime-impact-and-the-way-forward/> last accessed on 18 March, 2021.

[54] L. S. and K. Signe, 'Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa', Brookings: Africa in Focus (30 May, 2018), available at <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/> last accessed on 18 March, 2021.

[55] Serianu Limited, Africa Cybersecurity Report 2018: Kenya (Kenya: Serianu Limited, 2018), p.12.

year.[56] A recent report by the INTERPOL also estimates that Africa lost about 3.5 billion US Dollars in 2017.[57] However, to a large extent there appears to be a dearth of empirical and verifiable data on the economic cost of cyber-attacks in African countries due to the under-reporting of cyber-attacks.[58] Notwithstanding this state of affairs, there is no doubt that African countries are suffering economic losses from cyber-attacks[59] which further limits the social and economic development prospects of the Internet within the African region.[60]

AN OVERVIEW OF AFRICAN RESPONSES TO CYBERSECURITY GOVERNANCE

African States and intergovernmental organizations have established frameworks to promote cybersecurity governance and also prevent Africa from becoming a “safe harbour” for cybercrime.[61] This section will undertake an overview of African regional and national responses to cybersecurity governance. In this regard, the section will review cybersecurity governance responses from African regional intergovernmental organizations such as the AU, the ECOWAS, the COMESA and the SADC, and also provide an overview of national responses in African States.

The AU Convention on Cyber Security

The African Union (AU) was originally founded as the Organization of African Unity on 25 May, 1963, and later assumed its current name and structure in 2002.[62]

[56] Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa’s Cyber Security Poverty Line (Kenya: Serianu Limited, 2017), p.3.

[57] INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.8.

[58] Ibid, p.67.

[59] Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (Solutions Consulting: Florida, United States, 2018). See Serianu Limited, Africa Cyber Security Report 2017: Demystifying Africa’s Cyber Security Poverty Line (Serianu Limited: Kenya, 2017) p.11; African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa (Symantec Corporation and African Union, November, 2016), p.7.

[60] Nigerian Communications Commission (NCC), Final Report on Effects of Cyber Crime on Foreign Direct Investment and National Development (NCC: Abuja, 2017). See U.J. Orji, ‘Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria’, Tilburg Law Review (2019) Vol. 24(1), pp.109 &122.

[61] L. Kharouni, ‘Africa: A New Safe Harbour for Cyber criminals?”, Trend Micro Research Paper, Trend Micro Inc: USA, 2013, pp.1-26.

[62] African Union, ‘African Union in a Nutshell’, available at <http://www.au.int/en/abut/nutshell>

The AU is the most prominent regional intergovernmental organization that unites African States and it comprises of 55 sovereign States.[63] The aims of the AU include to "accelerate the political and socio-economic integration" of the African continent[64] and to coordinate and harmonize the policies between the existing and future Regional Economic Communities.[65] In line with its mandate, the AU established a Cybersecurity Convention which was adopted by AU Heads of State and Government during the 23rd Ordinary Session of the AU Assembly in Malabo on 27 June, 2014. The Convention which is known as the AU Convention on Cyber Security and Personal Data Protection[66] aims to harmonize the laws of African States on electronic commerce, data protection, cybersecurity promotion and cybercrime control. The Convention will to enter into force after it has been ratified by 15 AU Member States.[67] However, according to a report by the AU, as of June 2020, only 14 AU Member States (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia) had signed the Convention, while eight Member States (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal) had ratified the Convention.[68] The AU report also shows that the signatures and ratifications were done in 2015, 2016, 2017, 2018, 2019 and 2020 with none in 2014 when the Convention was adopted.[69]

The Convention recognizes that cybercrime constitutes "a real threat to the security of computer networks and the development of the Information Society in Africa".[70] Under the Convention Member States are required to establish national legal, policy and institutional governance mechanisms to promote cybersecurity. This

last accessed on 18 March, 2021.

[63] African Union, 'Member States' <http://www.au.int/en/member_states/country profiles> last accessed on 18 March, 2021

[64] Article 3 (c) Constitutive Act of the African Union, adopted the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government, 11 July, 2000 (Lome, Togo).

[65] Article 3 (i) ibid.

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

[67] Article 36 AU Convention on Cyber Security.

[68] African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, (18/06/2020), available at <https//au.int/sites/default/files/treaties/29560-sl-African%20Union%Convention%20On%Cyber%20Security%20And%Personal%20Data%20Protection.pdf> last accessed on 18 March, 2021.

[69] Ibid.

[70] Preamble, AU Convention on Cyber Security.

includes the establishment of a National Cybersecurity Framework that comprises a National Cybersecurity Policy, a National Cybersecurity Strategy[71] and National Cybersecurity Governance Structures.[72] In addition, the Convention requires Member States to establish laws to criminalize offences such as attacks against computer systems[73] and data,[74] as well as online child pornography[75] and also establish procedural measures for the control of cybercrime.[76]

The Convention further establishes legal provisions to promote international cooperation on cybersecurity.[77] In particular, 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)"[78] and also make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) for the purpose of promoting cybersecurity and tackling cyber threats.[79] To a large extent, the Convention adopts a holistic cybersecurity governance approach that apparently goes beyond that of the Council of Europe Convention on Cybercrime which limits its focus to the criminalization of cybercrime and the establishment of procedural mechanisms for law enforcement and international cooperation.[80]

The ECOWAS Directive on Fighting Cybercrime

The ECOWAS was founded by the Treaty of Lagos on 28 May, 1975.[81] Its aims to promote regional cooperation and integration that will lead to the establishment of an economic union in West Africa and also foster economic stability

[71] Article 24 ibid.

[72] Article 25 ibid.

[73] Article 29:1 ibid.

[74] Article 29:2 ibid.

[75] Article 29:3(1) ibid.

[76] Articles 29:3(4), 31:3(a) ibid.

[77] Article 28 ibid.

[78] Article 28:3 AU Convention on Cyber Security.

[79] Article 28: 4 ibid.

[80] U. J. Orji, 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection', Computer Law Review International, October, 2014, Issue 5, pp.131-132.

[81] Treaty of ECOWAS (Revised, 24 July, 1993), 35 ILM 660, (1996) [Hereafter, ECOWAS Treaty].

and relations amongst Member States.[82] The ECOWAS Treaty requires Member States to ensure “the harmonization and co-ordination of national policies and the promotion of integration programmes” in areas including communications, technology and legal matters.[83] On the basis of the above mandates the ECOWAS Council of Ministers adopted Directive C/DIR.1/08/11 on Fighting Cybercrime at its Sixty Sixth Ordinary session at Abuja, in August, 2011.[84] The adoption of the Directive was underscored by the need to curb cybercrime within the ECOWAS region as some Member States were beginning to gain global notoriety as major sources of email scams commonly known as the West African Letter Scam.[85] Accordingly, the Directive requires Member States to criminalizes cybercrime[86] including unauthorized access to a computer system;[87] unauthorized interference with the operation of a computer system;[88] unauthorized modification of computer data;[89] unauthorized interception of computer data;[90] computer fraud; [91] unauthorized manipulation of personal data;[92] and online child pornography.[93] The Directive also establishes a framework to facilitate international cybersecurity cooperation.[94]

In order to facilitate the development and harmonization of national cybersecurity laws in Member States, the Directive establishes binding obligations on Members to implement its provisions. Accordingly, Article 35 of the Directive declares that: “Member States shall adopt the necessary legislative, regulatory and administrative measures in order to comply with this Directive not later than 1st January, 2014”.[95] However, some Member States have not complied with the obligations under the

[82] Article 3 ECOWAS Treaty.

[83] Articles 3(2) (a), 33 (2) and 57(1), Treaty of ECOWAS.

[84] ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

[85] U. J. Orji, ‘Curbing Advance Fee Fraud in Nigeria: An Analysis of the Regulatory Framework and Contemporary Challenges’, International Company and Commercial Law Review, Issue 12, November 2011, pp. 408-421. See also A. Atta-Asamoah, ‘Understanding the West African Cybercrime Process’, African Security Review, Vol. 18, No. 4, pp.106-114.

[86] Article 2 ECOWAS Directive on Cybercrime.

[87] Article 4 ibid.

[88] Article 6 ibid.

[89] Articles 7 and 9 ibid.

[90] Article 8 ibid.

[91] Articles 10 and 11 ibid.

[92] Article 12 ibid.

[93] Article 16 ibid.

[94] Article 33 (1) ibid.

[95] Article 35 (1) ibid.

Directive. As of March, 2021, some ECOWAS Members including Guinea–Bissau, Liberia, and Sierra Leone[96] were yet to establish national cybersecurity laws, although there were ongoing initiatives to develop laws in those States.

The COMESA Model Cybercrime Bill

The Common Market for Eastern and Southern Africa (COMESA) is a free trade union that was formed in December, 1994 and aims to achieve regional integration by reducing barriers to cross border trade amongst Member States.[97] In line with its objectives, the COMESA developed a Model Cybercrime Bill in October 2011,[98] with a view to providing a uniform framework that would serve as a guide for the development of cybersecurity laws in Member States. Thus, the Model Cybercrime Bill provides a guide for the criminalization of offences against computer systems and data such as unauthorized access, data interference; data interception; misuse of digital devices; digital forgery; digital fraud, and cyber extortion.[99] However, the Bill does not establish any binding obligations on Member States to criminalize cybercrimes. As of March, 2021, COMESA Member States including Eritrea, Libya, Comoros, Swaziland, Democratic Republic of Congo, and South Sudan did not have cybercrime laws.[100]

The SADC Model Law on Computer Crime and Cybercrime

The Southern Africa Development Community (SADC) was founded in 1980 to promote economic integration and cooperation amongst Member States.[101] In March, 2012, the SADC adopted a Model Law on Computer Crime and Cybercrime[102] to serve as a guide for the development of cybercrime laws in SADC Member States. However, the model law does not impose any binding obligations on Members to

[96] African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa, Symantec Corporation and African Union, November, 2016, pp.53-55.

[97] Articles 3 and 6, Treaty Establishing the Common Market for Eastern and Southern Africa (1994).

[98] Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

[99] Part VI COMESA Model Cybercrime Bill.

[100] African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa, Symantec Corporation and African Union, November, 2016, pp.53-55.

[101] See <http://www.sadc.int/> last accessed on 18 March, 2021.

[102] SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

establish cybercrime laws. As of March, 2021, SADC Members including Democratic Republic of Congo, Lesotho, Mozambique, and Swaziland did not have cybercrime laws.

National Responses to Cybersecurity Governance in Africa

Notwithstanding, the fact that only eight AU Member State have ratified the AU Convention on Cyber Security,[103] many Member States have already established national frameworks for cybersecurity governance. For example, as of March, 2020, 39 States out of the 55 AU Member States had established cybersecurity laws, while 21 States had established national cybersecurity policies, 23 States also had national CERT frameworks (see Table 1 below). However, aside from the establishment of cybersecurity laws and policies, there appears to be very slow or no efforts towards developing other critical aspects of cybersecurity governance such as technical and organizational measures and user education at the national levels in AU Member States.

[103] T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, (10 April, 2015), available at <http://www.bbc.com/news/business-32079748>; D. Finnan, 'Lack of Laws Governing Cybercrime Making Africa a Safe Haven for Cyber Criminals (Interview)', Radio France Internationale, (16 February 2015), available at <http://www.english.rfi.fr/africa/20150215-lack-laws-governing-cybercrime-making-africa-safe-haven-cybercriminals-interview> last accessed on 18 March, 2021.

Table 1. A Summary of National Responses to Cybersecurity Governance in Africa (March, 2021)

	Country	Cybersecurity Legislation	National Cybersecurity Policy	Computer Emergency Response Teams (CERTS)
1	Algeria	√	No information	No information
2	Angola	√	None	None
3	Benin	√	√	√
4	Botswana	√	√	√
5	Burkina Faso	√	√	√
6	Burundi	√	None	None
7	Cameroon	√	None	√
8	Cape Verde	√	√	No information
9	Central African Republic	None	None	None
10	Chad	None	None	None
11	Comoros	None	None	None
12	Côte d'Ivoire	√	√	√
13	Democratic Republic of the Congo	None	None	None
14	Djibouti	√	None	None
15	Egypt	√	√	√
16	Equatorial Guinea	None	None	None
17	Eritrea	None	None	None
18	Ethiopia	√	√	√
19	Gabon	√	√	None
20	Gambia	√	In progress	None
21	Ghana	√	√	√
22	Guinea	√	None	None
23	Guinea-Bissau	None	None	None
24	Kenya	√	√	√
25	Lesotho	None	None	None
26	Liberia	In progress	None	None
27	Libya	None	None	√

	Country	Cybersecurity Legislation	National Cybersecurity Policy	Computer Emergency Response Teams (CERTS)
28	Madagascar	√	None	None
28	Malawi	√	In progress	√
29	Mali	√	None	None
30	Mauritania	√	√	None
31	Mauritius	√	√	√
32	Morocco	√	√	√
33	Mozambique	None	In progress	√
34	Namibia	√	None	None
35	Niger	√	None	None
36	Nigeria	√	√	√
37	Arab Saharawi Democratic Republic	No information	No information	No information
38	Republic of the Congo	None	None	None
39	Rwanda	√	√	√
40	São Tomé and Príncipe	√	None	None
41	Senegal	√	√	√
42	Seychelles	√	None	None
43	Sierra Leone	None	None	None
44	Somalia	None	None	None
45	South Africa	√	√	√
46	South Sudan	None	None	None
47	Sudan	√	√	√
48	Swaziland	In progress	None	None
49	Tanzania	√	None	√
50	Togo	√	None	None
51	Tunisia	√	√	√
52	Uganda	√	√	√
53	Zambia	√	In progress	√
54	Zimbabwe	√	√	None
55				

CHALLENGES TO CYBERSECURITY GOVERNANCE IN AFRICA

Aside from the absence of legal and policy frameworks for cybersecurity governance in many African States as seen in the table above, there are also other peculiar challenges arising from the absence of requisite institutional capacities in terms of cybercrime law enforcement.[104] For example, law enforcement authorities in many African States still lack capacities that are necessary to detect, investigate and prosecute cybercrime.[105] In this regard, an INTERPOL report recently observed the lack of investment and limited capacities to prevent, detect, and investigate cyber-attacks in many African countries, which is further driving cyber criminality on the continent.[106] Although, there have been various initiatives to build capacities in law enforcement authorities in some States, however, it appears that such initiatives have not yet achieved the intended results.[107] In some countries, policy makers have expressed a lack of interest in funding training for cybersecurity skills that will enhance cybercrime control due to fears over the dual use of such skills. For example, in 2016, it was reported that policy makers in Cameroon were in the process of launching cybersecurity skill development programs, but however feared that after completing the training program, the trainees could use the skills acquired to commit cybercrime.[108] Weak institutional capacity is also reflected in terms of

[104] A. Fassassi and C. F. Akoussan, 'Cybercrime in Africa: Facts and Figures' , Sci Dev Net, (7 July,2016), available at <https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/> last accessed on 18 March, 2021; N. Kshetri, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies', in Cybercrime and Cybercrime in the Global South, Palgrave Macmillan, 2013, pp.152-170.

[105] African Union and Symantec Corporation (2016) Cyber Crime & Cyber Security Trends in Africa. United States: Symantec Corporation, pp.60, 61,63,66,70, and 83.

[106] INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.67.

[107] Ibid, pp.70, 83,134. See also.F.E. Eboibi, 'Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime Policy Implementation and Institutional Accountability', Commonwealth Law Bulletin, (2020), Vol. 46, Issue 1, pp.78-99; M. Lucchetti, Cybercrime Legislation in Africa: Regional and International Standards, African Union/Council of Europe Joint Programme on Cyber Security and Cybercrime for African Diplomats (12 April, 2018: Addis Ababa), p.3, available at <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-05.press_cybercrime_legislation _in_africa_12apr2018_matteo.l.pdf> last accessed on 18 March, 2021.

[108] N. K. Chimtom, 'Cameroon's Dilemma in Fighting Cybercrime', African Independent (16 April, 2016), available at <https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265> last

lack of up to date technological tools to enhance law enforcement and lack of awareness and expertise amongst law enforcement officials,[109] as well as the absence of requisite technical and infrastructural frameworks to promote cybersecurity.[110] Another indicator of weak institutional capacities is the absence of functional national CERTs to coordinate responses to cybersecurity threats in most African States.[111]

The challenge of weak institutional capacities can also be traced to the fact that most African States have not dedicated adequate financial resources to promoting cybersecurity governance initiatives.[112] Poor funding of cybersecurity initiatives is to a large extent responsible for the absence of highly skilled cybersecurity experts that will render cybersecurity governance services including assisting law enforcement authorities in the prevention, investigation or prosecution of cybercrime. [113] Another challenge that arises from poor funding is the limitation of research and development initiatives that would promote cybersecurity governance. To some extent, the poor government funding of cybersecurity initiatives is caused by the fact that cybersecurity is not really considered as a national security priority in many African States.[114] 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.[115]

accessed on 18 March, 2021. See also, N. Kshetri, ‘Cybercrime and Cybersecurity in Africa’, Journal of Global Information Technology Management (2019), Vol. 22, No.2, p.77

[109] *Ibid*, p.10.

[110] INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.67; S. Dlamini and C. Mbambo, ‘Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses’, Cogent Social Sciences, (2019) Vol. 5:1, p.17.

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

[112] Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa’s Cyber *Security* Poverty Line (Kenya: Serianu Limited, 2017), p.9; N. Kshetri, ‘Cybercrime and Cybersecurity in Africa’, Journal of Global Information Technology Management (2019), Vol. 22, No.2, p.78; N. N. Schia, ‘The Cyber Frontier and Digital Pitfalls in the Global South’, Third World Quarterly, (2018), Vol. 39, No. 5, pp.821-837.

[113] African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa, United States: Symantec Corporation, 2017, pp.70, 76, 88, 89, and 92. See also, Serianu Limited, Africa Cybersecurity Report 2016, Kenya: Serianu Limited, 2016, p.46; W. Mcanyana and C. Brindley, Insight into The Cyber Threat Landscape in South Africa (Accenture: South Africa, 2020), p.6.

[114] U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p. 369. See also, African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa (Symantec Corporation: United States, 2016), p. 60; U. J. Orji, ‘The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability’, Masaryk University Journal of Law and Technology (2018) Vol. 12 (2), pp.119

Another major challenge to cybersecurity governance in most African States arises from lack of awareness by the end-users of ICT applications and information society services.[116] Lack of awareness amongst a large segment of Africa's growing ICT user population has been a major contributory factor to the increasing rates of cybercrime on the continent.[117] Many end-users of ICT products and services in Africa are getting connected to the Internet for the first time and lack basic knowledge to protect themselves from cyber threats and which exposes them to cyber-attacks.[118] This also raises grave concerns about the negative impact of cybercrime on African economies. For example, South Africa is reported to have the third highest number of cybercrime victims globally,[119] while a survey by Norton indicates that 70 percent of South Africans have fallen victim to cybercrime which is higher than the global average of 50 percent.[120] In Nigeria which has the largest Internet user population in Africa, it is estimated that over 17,600 bank customers lost over 39 million US Dollars in 2018 to due to cybercrime.[121]

[115] M. Shuaibu and L.D. Bernsah, 'An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach', Journal of Social and Management Sciences, (2016) Vol.2 (1), pp. 3, 4, 6; L. Ploch, Countering Terrorism in East Africa: The U.S. Response. Congressional Research Service, (2010), R41473, p. 19. See Vanguard, Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama (2017), available at <https://www.vanguardngr.com/2017/02/fgcommittingsignificant-share-2017-budget-northeast-onyeama/> last accessed on 18 March, 2021; U.J. Orji, 'Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses', in C. Samuel and M. Sharma, (eds.) Securing Cyberspace: International and Asian Perspectives, New Delhi, India: Institute for Defence Studies and Analyses & Pentagon Press, 2016, p.213.

[116] M. Bada, B. Von Solms, and I. Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa', International Journal on Advances in Security (2019), Vol. No. 1 &2, pp.108-118.

[117] O. Regha, 'Aggressive Consumers Awareness Initiatives: A Proactive & Consistent Mechanism to Preventing E-fraud' in Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment, Central Bank of Nigeria: 2015, pp.10-13.

[118] The Cyber Diplomat, 'Cybercrime in West Africa — An Overview' (18 April, 2020), available at <https://medium.com/@cyberdiplomacy/cybercrime-in-west-africa-an-overview-e3af22ebdb9a>; A. A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html> last accessed on 18 March, 2021.

[119] See B. Koigi, 'South Africa has the third –highest number of Cybercrime Victims Globally, Report', Africa Tech, (4 July, 2020), available at <https://www.africabusiness communities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/> last accessed on 18 March, 2021.

[120] T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, (10 April, 2015), available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

[121] M. Ogbonnaya, 'Cybercrime in Nigeria Demands Public-Private Action', Institute for Security Studies-ISS Today, (19 October, 2020), available at <https://www.issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action> last accessed on 18 March, 2021.

Lack of awareness by the end-users also raises serious concerns that Africa could become a “safe harbour” for cybercrime.[122] This is because most African States already lack efficient law enforcement capacities to tackle cybercrime as well as effective criminal justice delivery systems.[123] Thus, aside from lack of capacities for cybercrime control amongst law enforcement authorities in most African States[124], there also appears to be a lack of skills for administering cybercrime cases in the judiciary.[125] In addition, it is possible that few cybercrime cases which are eventually brought before the Court would spend very long trial periods. For example, in some African States it could take up to an average of five years for a High Court to determine a criminal matter that is not related to cybercrime.[126] Consequently, it is probable that cybercrime cases which are inherently technical and require skilled expertise and the use of digital evidence during trial may even take more years for determination. Therefore, with the challenge of lack of awareness, it is foreseeable that the impact of cybercrime on African economies will continue to rise with their increasing dependence on ICTs and the availability of broadband capacity, and criminal law enforcement mechanisms will not be able to provide enough deterrence to cybercrime.

[122] L. Kharouni, ‘Africa: A New Safe Harbour for Cyber criminals?’, Trend Micro Research Paper, USA, Trend Micro Inc, 2013, pp.1-26.

[123] C. M. Fombad, ‘The Context of Justice in Africa: Emerging Trends and Prospects’, in Evelyn Edroma (ed), Rethinking the Role of Law and Justice in Africa’s Development: An Edited Volume of Discussion Papers, United Nations Development Programme: Addis Ababa, Ethiopia, June, 2013, pp.16 and 17. See also, M. Shaw and T. Reitano, ‘The Evolution of Organized Crime and Illicit Trafficking in Africa, and its Implications for Citizen and State Security’, in Evelyn Edroma (ed), ibid, p.38.

[124] K. A. Barfi, et al, ‘Internet Users and Cybercrime in Ghana: Evidence from Senior School in Brong Ahafo Region’, Library Philosophy and Practice (e-Journal), 2018, 1715. See M. Sarrab, et al, ‘Challenges of Computer Crime Investigation in North Africa’s Countries’, The International Arab Conference of Information Technology, 2013, pp1-6.

[125] I. A. Yusuf, ‘Nobody has been prosecuted for Cybercrime in Nigeria’, The Nation, 16 April, 2017, available at <http://thenationlineng.net/nobody-prosecuted-cybercrime-nigeria/> last accessed on 18 March, 2021. See also, ‘Cybercrime in Africa: Facts and Figures’ (07/07/2016), available at <https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html> last accessed on 18 March, 2021.

[126] J. Agbonika and A. Musa, ‘Delay in the Administration of Criminal Justice in Nigeria: Issues from a Nigerian Viewpoint’, Journal of Law, Policy and Globalization, 2014, Vol.26, pp.126 -138. See also, Hon. Justice D. Mann, Curbing Delays in the Administration of Justice: Case Management in the Magistrate Courts. [A paper presented at the orientation for newly appointed Magistrates at National Judicial Institute, Abuja, 24 July, 2017], available at <http://www.nji.gov.ng/images/Workshop_Papers/2017/Orientation_Newly_Appointed_Magistrates/s2.pdf>; T. Soniyi, ‘CJN Decries in Criminal Trials’, Thisday, 18 April, 2016, available at <https://www.thisdaylive.com/index.php/2016/04/18/cjn-decries-delay-in-criminal-trials/amp/> last accessed on 18 March, 2021.

PROPOSALS FOR THE DEVELOPMENT OF OTHER ASPECTS OF CYBERSECURITY GOVERNANCE ASIDE FROM CRIMINAL LAW MEASURES

As seen in table 1 above, cybersecurity governance responses in Africa have been focused mainly on the development of criminal law measures. For example, with respect to African countries within the SADC it has been observed that their cybersecurity governance responses have been focused cybercrime offences and criminalizing online behavior.[127] With respect to African countries within the ECOWAS, it has been observed that financial constraints have also impeded the timely implementation of comprehensive governance measures 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 diseases, tackling widespread poverty, and promoting the sustainable exploitation of natural resources.[128] As such, there exists a lack of requisite capacities in terms of cybersecurity governance in many African countries[129] with more focus on the development of criminal law measures, and without an adequate development of other critical governance measures such as organizational measures,[130] user education[131] and international cooperation.[132] This section will make proposals on the development of those critical governance measures beyond criminal law measures.

[127] E. Calandro, and N. Berglund, ‘Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC Case’ (2020), pp.10-11, available at <https://www.researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf> last accessed on 18 March, 2021.

[128] U.J Orji, ‘An Inquiry into the Legal Status of ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States’ Computer Law & Security Review, 2019, Vol. 35 (6), p.14.

[129] U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p. 369. See also, African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa (Symantec Corporation: United States, 2016), p. 60; U. J. Orji, ‘The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability’, Masaryk University Journal of Law and Technology (2018) Vol. 12 (2), pp.119

[130] N. Waag –Cowling, ‘Living below the Cyber Poverty Line: Strategic Challenges for Africa’ Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/> last accessed on 18 March, 2021.

[131] R. Butler and M. Butler, ‘It Will Take Education, Not Just Legislation, To Take Cybercrime’, The Conversation, (10 March, 2016), available at <https://www.theconversation.com/it-will-take-education-not-just-legislation-to-tackle-cybercrime-56030> last accessed on 18 March, 2021.

[132] E. Tamarkin, ‘The AU’s Cybercrime Response: A Positive Start, but Substantial Challenges Ahead’, ISS Policy Brief (January, 2015), Issue 73, p.3.

Building Institutional Capacities

It is imperative for African States to focus on building technical and human capacities in various institutions that are responsible for cybersecurity governance including CERTs and law enforcement authorities. In particular, CERTs and law enforcement authorities should be adequately funded and equipped and their personnel regularly trained and updated on emerging trends in cybercrime and cybersecurity governance.[133] Institutional capacity building for cybersecurity governance should also include the establishment of cybercrime units in law enforcement authorities. In addition, African States will have to ensure that judicial officers and prosecutors undergo constant training to keep up with developments in cybersecurity law and the handling of electronic evidence, as well as other related issues in the judicial administration of cybercrime cases.

Building Capacities for End-User Education

End-user education should be effectively integrated into national cybersecurity governance frameworks in African States. One way of building capacities for the implementation of end-user education is by imposing legal requirements on the manufacturers of ICT products, electronic service providers (such as financial institutions) and communications service providers to integrate end-user education components in their products and services. For example, banks that provide electronic/online banking services could be required to develop mandatory cybersecurity awareness programmes to educate consumers on the secure usage of such services. Failure to fulfill such obligations by service providers should give rise to civil and regulatory liabilities.[134]

[133] N. Waag ‒Cowling, 'Living below the Cyber Poverty Line: Strategic Challenges for Africa', Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/> last accessed on 18 March, 2021.

[134] For example in the United States, banks have been held liable for failing to create an electronic banking environment that will ensure consumer protection. See Ognibene v. Citibank (446 NYS 2d 845 (CIV.Ct.1981).In that case, a rogue standing near a bank's ATM terminal memorized the personal identification number (PIN) of a cardholder who was using the machine. The rogue pretended to be servicing the ATM terminal and used an adjacent telephone to conduct a fictitious telephone conversation with his employees, after which he asked the cardholder to let him have the use of his card to ensure the terminal was in order. After withdrawing the money by keying in the number, the rogue returned the cardholder saying all was well. The cardholder contested the banks right to debit his account with the amount withdrawn by the rogue, claiming that the bank had failed to introduce a

Another way of building capacities for end-user education is through the establishment of policies that will encourage institutions such as universities, non-governmental organizations, and other stake holders to promote end-user awareness on cybersecurity. Such policies could also create incentives for institutions that are engaged in research and development initiatives to enhance end-user awareness on cybersecurity. Imposing a form of social corporate responsibility obligation on mass media organizations to promote cybersecurity awareness will also help in creating a culture of cybersecurity amongst end-users in African States.

Building Capacities to Enhance the Implementation of Technical Solutions to Cybersecurity

African States may have to consider establishing legal obligations that will require the manufacturers/vendors and providers of ICT products and services to integrate the implementation of technical protection measures in such products and services before making them available to end-users. Capacities for technical protection can also enhanced by establishing obligations on network service providers and end-users to report cybersecurity incidents to the appropriate authorities such as CERTs. For example, in Nigeria, the Cybercrimes Act imposes obligations on persons or institutions that operate a computer network to report cyber threats to the national CERT Coordination Center so that the National CERT can take the necessary measures to address such issues.[135] In addition, the Central Bank of Nigeria's Risk-based Cybersecurity Framework and Guidelines for Deposit money banks and Payment Service Providers imposes a similar reporting obligation banks and electronic payment service providers by requiring them "to report all cyber-incidents whether successful or not immediately after such incident was identified to the Director of Banking Supervision of the CBN".[136] The implementation of such obligations aims to facilitate timely national responses to cybersecurity incidents that may affect data held on the computer systems and networks of organizations including banks and financial institutions that provide electronic banking and payment services, and also helps to timely mitigate the effect and spread of cybersecurity threats.

safe method for the use of a card. The Court held that the bank had been negligent in not taking measures to combat fraud and that the bank ought to have provided the cardholder with sufficient information to handle such dangers.

[135] Section 21(1) Cybercrimes (Prohibition and Prevention, etc) Act, 2015.

[136] Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 25 June, 2018, at paragraph 7.6, p.10.

Establishment of Computer Emergency Response Teams (CERTs)

It is imperative for African States to timely establish well equipped and functional national CERTs to enhance the protection of their national critical information infrastructure and their capabilities to respond to cybersecurity threats in a timely and coordinated manner. As seen in the table above, only 23 African States had national CERT frameworks. However, there are also indications that CERTs are not actually functioning in some African States that have formally established CERT frameworks as some of the established CERTs appear to be inactive or offline[137] and therefore not providing critical computer emergency response services that qualify them as CERTs. This implies that many African States still do not have the requisite national capacity to effectively provide emergency responses to cybersecurity threats, even though they may have established CERTs. Therefore, there is need to ensure that established CERTs are fully functional so that they can efficiently provide services in their States.

Building Capacities for the Regional Cooperation on Cybersecurity

Cybersecurity issues are inherently transnational due to the ubiquitous nature of electronic communications networks. This state of affairs underscores the need for regional and international cooperation on cybersecurity governance. In order to enhance such cooperation in the African context, it will be necessary for the African Union to establish an institutional framework for cybersecurity governance that is similar to the European Information Security Agency (ENSIA)[138] to coordinate regional cybersecurity efforts and responses to cybersecurity incidents. Also the establishment of such regional institutional framework can enhance global cybersecurity cooperation and further serve as a forum for the dissemination of information and national best practices amongst African States. A legal basis may be found for the establishment of a network security agency within the African Union framework under Article 32 of the African Union Convention on Cybersecurity which provides for an operational mechanism for the Convention.[139] Some of the functions of the

[137] G. van Zyl, ‘Africa Lacks Computer Emergency Response Team Readiness’, IT Web Africa, 27 May, 2014, available at <http://www.itwebafrica.com/m/news/zw2Wo44AaJQDo>; Africa Cert <africacert.org/African-csirts> last accessed on 18 March, 2021.

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

Convention's operational mechanism include:

(1) Promoting the adoption and implementation of measures to strengthen cyber security in electronic services and combating cybercrime and human rights violations in cyberspace;

(2) Advising African governments on measures to promote cybersecurity and combat cybercrime; and;

(3) Analyzing the criminal behaviors of cyberspace users within Africa and transmitting such information to competent national authorities. [140]

The above mandates may be broadly interpreted to create a regional network agency which is similar to the ENISA which was established in 2004 by the European Commission to promote cybersecurity and critical information infrastructure protection.[141] 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 standards for best practices.[142] A regional network agency that is established under article 32 of the Convention may also function as a regional CERT where its mandate is enlarged to function as such.[143]

Promoting Private Sector Participation

The private sector has an enormous role to play in promoting cybersecurity governance in African States. Following market liberalization in several economic sectors in Africa, the private sector now controls significant segments of networked critical sectors in African States. Such critical sectors include banking and financial services, broadcasting services and telecommunications.[144] This state of affairs makes the private sector a critical stakeholder in promoting cybersecurity and protecting

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

[140] Article 32 African Union Convention on Cyber Security and Personal Data Protection

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

[142] See <http://www.enisa.europa.eu/>.

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

[144] M.D.J. Williams, et al, Africa's ICT Infrastructure: Building on the Mobile Revolution, World Bank: Washington DC, 2011, pp.9, 11, 15 -16.

critical information infrastructure. Therefore, it is imperative for national cybersecurity governance frameworks to recognize the strategic position of the private sector in promoting cybersecurity.[145] One way of achieving this, is for cybersecurity laws and policies to create clear frameworks for cooperation between government agencies and private sector organizations through arrangements for the sharing of information and critical resources that can enhance responses to cyber incidents that affect national critical infrastructure sectors or through other public-private partnership arrangements. Public-private partnerships are also usually very important in setting cybersecurity standards on issues including software accreditation, public key infrastructure (PKI) regulation and end-user education. Public-private partnership arrangements can also be used to fund the operation of national CERTs.

CONCLUDING REMARKS

African States still lack efficient capacities and resources for cybersecurity governance. This absence of capacities and resources remains a major contributory factor that has been responsible for creating an enabling environment for the rising trend of cybercrime in African States. Although, most African States have established criminal law measures to promote cybersecurity governance, however standing alone, such measures would produce very little impact in terms of minimizing cybersecurity vulnerabilities. Therefore, only criminal law measures would never be able enough to deter cybercrime or minimize exposure to cybersecurity threats in Africa’s information society. This state of affairs requires that the governments of African States should actively go beyond the establishment of criminal law measures in their cybersecurity governance responses in order to effectively cover other critical aspects of cybersecurity governance including technical and organizational measures and user education. This is also imperative given the peculiar challenges that impede effectiveness of cybercrime law enforcement measures in Africa. In concluding, it is important to point out that there can be no silver bullet for addressing Africa’s cybersecurity challenges, however there is a higher probability that the timely implementation of holistic approaches to cybersecurity governance would reduce vulnerabilities in Africa’s information society.

[145] ITU-D Secretariat, ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, Geneva, ITU, January, 2008, p.19.

References

A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html>.

A. Allotey, 'Ghana Loses $230 Million to Cyber Criminals – CID', Citinews (4 October, 2018), available at <https://citinewsroom.com/2018/10/04/ghana-loses-230m-to-cyber-criminals-cid/>.

A. Atta-Asamoah, 'Understanding the West African Cybercrime Process', African Security Review, Vol. 18, No. 4.

A. Barfi, et al, 'Internet Users and Cybercrime in Ghana: Evidence from Senior School in Brong Ahafo Region', Library Philosophy and Practice (e-Journal), 2018, 1715.

A. Fassassi and C. F. Akoussan, 'Cybercrime in Africa: Facts and Figures', Sci Dev Net, (7 July, 2016), available at <https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/>.

A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html>.

A. Yusuf, 'Nobody has been prosecuted for Cybercrime in Nigeria', The Nation, 16 April, 2017, available at <http://thenationlineng.net/nobody-prosecuted-cybercrime-nigeria/>.

Africa Cert <africacert.org/African-csirts>.

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

African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa, United States: Symantec Corporation, 2016.

African Union Convention on Cyber Security and Personal Data Protection.

African Union, 'African Union in a Nutshell', available at <http://www.au.int/en/abut/nutshell>.

African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, (18/06/2020), available at <https//au.int/sites/default/files/treaties/29560-sl-African%20Union%Convention%20On%Cyber%20Security%20And%Personal%20Data%20 Protection.pdf>.

B. Koigi, 'South Africa has the third –highest number of Cybercrime Victims Globally, Report', Africa Tech, (4 July, 2020), available at <https://www.africabusiness communities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/>.

B. T. Mbatha, D.N. Ocholia and J.L. Roux, 'Diffusion of ICTs in Selected Government Departments in KwaZulu –Natal, South Africa', Information Development, (2011) , Vol. 27 (4).

'Cybercrime Impact and the Way Forward', Business & Financial Times Online (5 November, 2018), available at <https://www.thebftonline.com/2018/features/cybercrime-impact-and-the-way-forward/>.

'Cybercrime in Africa: Facts and Figures' (07/07/2016), available at <https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html>.

C. Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation', Journal of Information Law and Technology, 2007 (2).

Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime (Center for Strategic and International Studies: Washington, DC, June, 2014).

Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 25 June, 2018.

COMESA Model Cybercrime Bill, Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

Constitutive Act of the African Union, adopted the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government, 11 July, 2000 (Lome, Togo).

Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

D. Finnan, 'Lack of Laws Governing Cybercrime Making Africa a Safe Haven for Cyber Criminals (Interview)', Radio France Internationale, (16 February 2015), available at <http://www.english.rfi.fr/africa/20150215-lack-laws-governing-cybercrime-making-africa-safe-haven-cybercriminals-interview>.

D. Olowu, 'Environmental Governance Challenges in Kiribati: An Agenda for Legal and Policy Responses', Law, Environment and Development Journal (2007) Vol. 3, Issue 3.

E. Calandro, and N. Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC Case' (2020), available at <https://www.researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro _Berglund_Unpacking-Cyber-Capacity-Building-1.pdf>.

E. Tamarkin, 'The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead', ISS Policy Brief (January, 2015), Issue 73.

EC Regulation No 460/2004 establishing the European Network and Information Security Agency.

ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

F. Fukuyama, 'What Is Governance?', CGD Working Paper 314 (Washington, DC: Center for Global Development, January 2013).

F.E. Eboibi, 'Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime Policy Implementation and Institutional Accountability', Commonwealth Law Bulletin, (2020), Vol. 46, Issue 1.

G. Marco, 'The Slow Wake of a Global Approach against Cybercrime', Computer Law Review International, 2006, Issue 5.

G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009.

G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, available at <https://pinigeria.org/download/download/cybercost.pdf>.

G. van Zyl, 'Africa Lacks Computer Emergency Response Team Readiness', IT Web Africa, 27 May, 2014, available at <http://www.itwebafrica.com/m/news/zw2Wo44AaJQDo>.

GSMA, The Mobile Economy Africa 2020 (GSMA: London, 2020).

Hon. Justice D. Mann, Curbing Delays in the Administration of Justice: Case Management in the Magistrate Courts. [A paper presented at the orientation for newly appointed Magistrates at National Judicial Institute, Abuja, 24 July, 2017], available at <http://www.nji.gov.ng/images/Workshop_Papers/2017/Orientation_Newly_Appointed_Magistrates/s2.pdf>.

I. Gagliardone and N. Sambuli, 'Cyber Security and Cyber Resilience in East Africa', Global Commission on Internet Governance Paper Series, No. 15 (May, 2015).

International Bureau of Education, 'Concept of Governance', available at <http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance>.

Internet Crime Complaint Center, 2010 Internet Crime Report (National White Collar Crime Center: United States, 2011).

Internet Crime Complaint Center, 2013 Internet Crime Report (National White Collar Crime Center: United States, 2014).

INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020).

ITU High Level Experts Group [HLEG] ITU Global Cyber-SecurityAgenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU 2008.

ITU Study Group Q.22/1, Report on Best Practices For A National Approach

To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts [Draft], Geneva, ITU-D, January 2008.

ITU, 'Challenges to Building a Secure Information Society', 2007 World Information Society Report: Beyond WSIS, ITU, Geneva, 2007.

ITU-D Secretariat, ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, Geneva, ITU, January, 2008.

J. Agbonika and A. Musa, 'Delay in the Administration of Criminal Justice in Nigeria: Issues from a Nigerian Viewpoint', Journal of Law, Policy and Globalization, 2014, Vol.26.

J. Graham, B. Amos and T. Plumptre, Governance Principles for Protected Areas in the 21st Century 5 (Ottawa: Institute of Governance, 2003).

L. Kharouni, 'Africa: A New Safe Harbour for Cyber criminals?', Trend Micro Research Paper, USA, Trend Micro Inc, 2013.

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

L. S. and K. Signe, 'Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa', Brookings: Africa in Focus (30 May, 2018), available at <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/>.

M. Bada, B. Von Solms, and I. Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa', International Journal on Advances in Security (2019), Vol. No. 1 &2.

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

M. Fombad, 'The Context of Justice in Africa: Emerging Trends and Prospects', in Evelyn Edroma (ed), Rethinking the Role of Law and Justice in Africa's Development: An Edited Volume of Discussion Papers, United Nations Development Programme: Addis Ababa, Ethiopia, June, 2013.

M. K. Luka and I. A. Frank, 'The Impacts of ICTs on Banks: A Case Study of the Nigerian Banking Industry', International Journal of Advanced Computer Science and Applications (2012), Vol. 3 (9).

M. Andrianaivo and Kangni Kpodar, 'ICT, Financial Inclusion, and Growth: Evidence from African Countries', IMF Working Paper, WP/11/73 (2011).

M. Lucchetti, Cybercrime Legislation in Africa: Regional and International Standards, African Union/Council of Europe Joint Programme on Cyber Security and Cybercrime for African Diplomats (12 April, 2018: Addis Ababa), available at <https://au.int/sites/default/files/

newsevents/workingdocuments/34122-wd-05.press_cybercrime_legislation_in_africa_12apr2018_matteo.l.pdf>.

M. M. Tamayao, What Is Governance?, available at <https://tamayaosbc.wordpress.com/2014/08/ 21/what-is-governance/>.

M. Ogbonnaya, 'Cybercrime in Nigeria Demands Public-Private Action', Institute for Security Studies-ISS Today, (19 October, 2020), available at <https://www.issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action>.

M. Sarrab, et al, 'Challenges of Computer Crime Investigation in North Africa's Countries', The International Arab Conference of Information Technology, 2013.

M. Shuaibu and L.D. Bernsah, 'An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach', Journal of Social and Management Sciences, (2016) Vol.2 (1).

M.D.J. Williams, et al, Africa's ICT Infrastructure: Building on the Mobile Revolution, World Bank: Washington DC, 2011.

Miniwatts Marketing Group, 'Internet Usage Statistics for Africa', (31 December, 2020), available at <http://www.internetworldstats.com/stats1.htm>.

N. Allen, 'Africa's Evolving Cyber Threats', African Center for Strategic Studies, (19 January, 2021), available at <https://africacenter.org/spotlight/africa-evloving-cyber-threats/>.

N. K. Chimtom, 'Cameroon's Dilemma in Fighting Cybercrime', African Independent (16 April, 2016), available at <https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265>.

N. Kshetri, 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management (2019), Vol. 22, No.2.

N. Kshetri, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies', in Cybercrime and Cybercrime in the Global South, Palgrave Macmillan, 2013.

N. N. Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', Third World Quarterly, (2018), Vol. 39, No. 5.

N. Waag –Cowling, 'Living below the Cyber Poverty Line: Strategic Challenges for Africa' Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/>.

Nigerian Communications Commission (NCC), Final Report on Effects of Cyber Crime on Foreign Direct Investment and National Development (NCC: Abuja, 2017).

Nigerian Cybercrimes (Prohibition and Prevention, etc) Act, 2015.

O. Regha, 'Aggressive Consumers Awareness Initiatives: A Proactive &

Consistent Mechanism to Preventing E-fraud' in *Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment*, Central Bank of Nigeria: 2015. *Ognibene v. Citibank* (446 NYS 2d 845 (CIV.Ct.1981).

P. Wallet, Information and Communication Technology (ICT) in Education in Sub-Saharan Africa: A Comparative Analysis of basic e-readiness in Schools (UNESCO Institute for Statistics: Canada, 2015).

R. Bahrini and A. Qaffas, 'Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries', Economies (March, 2019) Vol. 7 (21).

R. Butler and M. Butler, 'It Will Take Education, Not Just Legislation, To Take Cybercrime', The Conversation, (10 March, 2016), available at <https://www.theconversation.com/it-will-take-education-not-just-legislation-to-tackle-cybercrime-56030>.

R. Flores, et al, Cybercrime in West Africa: Poised for an Underground Market (Trend Micro and INTERPOL, 2017).

R. Ponelis and M. A. Holmer, 'ICT in Africa: Building a Better Life for all', Information Technology for Development (2015).

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

Rubicon Computer Systems v. United Paints Limited (2000) 2 TCLR 453.

S. Dlamini and C. Mbambo, 'Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses', Cogent Social Sciences, (2019) Vol. 5:1.

S. Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva', (2008), available at <http://www.cybercrime law.net/documents/ cybercrime_ history.pdf>.

SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

Serianu Limited, Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line (Serianu Limited: Kenya, 2017).

Serianu Limited, Africa Cybersecurity Report 2016, Kenya: Serianu Limited, 2016.

Serianu Limited, Africa Cybersecurity Report 2018: Kenya (Kenya: Serianu Limited, 2018).

Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (United States: Solutions Consulting, 2018).

Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (Solutions Consulting: Florida, United States).

T. J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1).

T. Jackson, ‘Can Africa Fight Cybercrime and Preserve Human Rights?’, BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748>.

T. Mastile, ‘South Africa Loses R.5.7 Billion Annually to Cybercrime’, CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime>.

T. Sewart, ‘Time to Drop the Bomb’, *Computers & Law,* 2003 *Vol.*14 (4).

T. Soniyi, ‘CJN Decries in Criminal Trials’, *Thisday*, 18 April, 2016, available at <https://www.thisdaylive.com/index.php/2016/04/18/cjn-decries-delay-in-criminal-trials/amp/>.

T.J. McIntyre, ‘Computer Crime in Ireland: A Critical Assessment of the Substantive Law’, *Irish Criminal Law Journal*, 2005, Vol. 15 (1).

The Cyber Diplomat, ‘Cybercrime in West Africa — An Overview’ (18 April, 2020), available at <https://medium.com/@cyberdiplomacy/cybercrime-in-west-africa-an-overview-e3af22ebdb9a>.

Treaty Establishing the Common Market for Eastern and Southern Africa (1994).

U. J. Orji, ‘Curbing Advance Fee Fraud in Nigeria: An Analysis of the Regulatory Framework and Contemporary Challenges’, International Company and Commercial Law Review, Issue 12, November 2011.

U. J. Orji, ‘Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection’, Computer Law Review International, October, 2014, Issue 5.

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

U. J. Orji, ‘Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria’, Tilburg Law Review (2019) Vol. 24(1).

U. J. Orji, ‘The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability’, Masaryk University Journal of Law and Technology (2018) Vol. 12 (2).

U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012.

U. J. Orji, ‘An Inquiry into the Legal Status of ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States’ Computer Law & Security Review, 2019, Vol. 35 (6).

U. J. Orji, International Telecommunications Law and Policy (Cambridge

Scholars Publishing: United Kingdom, 2018).

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

‘Understanding the Concept of Governance’, available at <https://www.gdrc.org/u-gov/governance-understand.html>.

UNODC, Comprehensive Study on Cybercrime (Draft – February 2013), United Nations, New York, 2013.

Vanguard, Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama (2017), available at <https://www.vanguardn gr.com/2017/02/ fgcommittingsignificant-share-2017-budget-northeast-onyeama/>.

W. Mcanyana and C. Brindley, Insight into The Cyber Threat Landscape in South Africa (Accenture: South Africa, 2020).