Jurisdictional Challenges of Transnational Cybercrimes in the African Region

Flora Alohan Onomrerhinor*

ABSTRACT

Transnational cybercrimes are cybercrimes occurring across several jurisdictions. The advancement of technology has brought about an increase in the sophistication, severity and comprehensiveness of incidents of cybercrimes such that cybercrimes can now be effortlessly transnational. Existing literature reveals that inadequacy of cybercrime specific legislation in some states, inadequacy of procedural powers and inadequacy of enforceable mutual legal assistance provisions constitute jurisdictional challenges to transnational cybercrimes (TNCCs). This paper appraises the adequacy of legal responses to jurisdictional challenges of TNCCs in the African region and finds that in spite of the emphasis on the need for the enactment and harmonisation of cybercrime legislations, the problem of safe haven persist. It also finds that the various legal responses by states that have enacted cybercrime legislation in the region, have shown states consistently applying traditional territorially based rules to online activities by enacting laws that do not adequately address the borderless nature of the Internet. It concludes that purely domestic legal responses to cybercrimes, no matter how advanced, are inadequate as fragmented approach cannot effectively eradicate the problem created by the presence of safe havens. It proposes a holistic approach by way of a regional instrument patterned after the Council of Europe's Convention on Cybercrime with provisions for effective and adequate international cooperation

1. INTRODUCTION

Cybercrime refers to any crime committed on the computer network especially with the use of the Internet. It covers a vast array of criminal activities such as financial crimes, identity theft, Internet defamation and privacy infringement, hacking, creation and dissemination of malicious codes, child pornography and child grooming, people trafficking, copyright infringement and money

* LLB, LLM, PhD, BL, Senior Lecturer, Department of Jurisprudence and International Law, Faculty of Law, University of Benin, Benin City, Edo State, Nigeria, PMB 1154, E-mail flora.alohan@uniben.edu, GSM +234 703 442 8226, +234 818 946 9617

laundering. The prosecution of cybercrime within a state's territory can be challenging due to the opportunities presented by the Internet and computer networks. It is even more so where the elements of the crime occur across different jurisdictions.[1]

` Cybercrime is a global phenomenon. In today's world, a lot depends on the Internet and computer networks and cybercriminals take advantage of the over dependence on the Internet to commit cybercrimes.[2] A significant feature of cybercrime is that the elements of the crime can occur across several jurisdictions. Technological advancements have brought about increase in the severity and sophistication of incidents of cybercrimes such that they can now be effortlessly transnational.[3]

The use of and reliance on information technology has become more and more pervasive in the society especially in the Covid and Post Covid African societies.[4] Unfortunately, the targeting and exploitation of computer systems have also become increasingly common. Offences involving computers have grown rapidly in number and sophistication and cybercrime and electronic evidence represent transnational challenges.[5] The African continent is the fastest growing region of the world in terms of internet penetration and the use of mobile based financial services that have become an increasingly attractive areas for cybercriminals.[6]

Our present era has been referred to as the 'age of the Internet.'[7] Unfortunately, access to information which is now unprecedented can be negatively used to gain unauthorized access to information or steal profitable data.[8] The ease with which information can be shared on the Internet renders it vulnerable and makes it a target for criminal activities as immense damage can be done by an individual sitting half way across the world.[9] The

1 Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015) 4

2 M Gercke, 'Understanding Cybercrime: Phenomena, Challenges and Legal Responses' ITU, 2012 <wwwitu.int-D/cyb/cybersecurity/legislation.html> 'accessed 26 December 2018.'

3 Clough, *Principles of Cybercrime* (n 1) 3.

4 Jennigay Coetzer, 'Africa's Lack of Data Protection and Cybercrime Laws has Created Deep Vulnerabilities: But is Change on the Way?' <https://www.law.com/international-edition/2020/05/27/africas-lack-of-data-protection-and-cybercrime-laws-has-created-deep-vulnerabilities-but-is-change-on-the-way/?slreturn=2020> 'accessed 17 October 2021.'

5 Council of Europe, 'Second African Forum on Cybercrime 2021' <www.https://coe.int/en/web/cybercrime> 'accessed 15 October 2021.'

6 Nir Kshetri, 'Cybercrime and Cyber security in Africa' (2019) 22(2) Journal of Global Information Technology Management 77, 77-78

7 Adrian Bannon, 'Cybercrime Investigation and Prosecution- Should Ireland Ratify the Cybercrime Convention?' (2007) 3 Galway Student Law Review 116, 119

8 ibid

9 ibid

relationship between cybercrime and opportunity is captured by the maxi, crime follows opportunity, as virtually every advancement in technology has been accompanied by a corresponding niche to be exploited for criminal purposes: The magic of digital cameras and the sharing of photographs is exploited by child pornographers; the convenience of electronic banking and online sales is exploited by fraudsters; Electronic communications and social networking have been used to stalk and harass and the ease with which digital media may be shared has led to an explosion in copyright infringement. [10]

The well know dimension and common problems surrounding normal use of Internet such as Ransome ware, Denial of service or (DDoS) Phishing, money Laundering from crimes are highly present in Africa. Cybercrime in Africa has rendered the use of the Internet particularly for e-commerce purposes a highly risky venture. As in other world region, organised crime groups in Africa use the Internet for criminal ends, leveraging on digital tools to contact and solicit victims. The Interpol supported operations Sarraounia saw the rescue of 232 victims of human trafficking in Niger, 46 of which were minors.[11] The operation revealed that 180 male victims had been recruited online with messages that promised decent work.[12] The African region is a growing global transit hub for the trafficking of drugs and a range of illicit commodities with narcotics, pharmaceuticals, stolen motor vehicles and other goods sold and bought on line.[13]

At the 2nd African Forum on Cybercrime held on the 28th -29 of June 2021, it was stated that cybercrime is one of the most pressing challenges impacting economic activity in Africa.[14] The cybercrime and cyber enabled crime trends reported in Africa are malware incidence, online fraud, the use of virtual currency to finance criminal activities as well as threats related to online child safety. A major concern is the growing link between cybercrime, terrorist funding and cyber terrorism. In the face of this reality, some countries have responded to the challenges of transnational cybercrimes by enacting legislations to address online conducts. Others have entered agreement

10 Clough, *Principles of Cybercrime* (n 1) 4

11 Interpol, 'Niger: Police Rescue 232 Victims of Human Trafficking, 26 February 2020 <www.interpol.int/en/News-and-Event/News/2020/Niger-police-rescue.../> 'accessed 21 October 2021.'

12 Council of Europe, 'Second African Forum on Cybercrime' (n 5)

13 ibid

14 In 2017, Africa's GDP was 3.3 trillion dollars and the cost of cybercrime for the same year amounted to 3.5 billion dollars.

for mutual legal assistance on the subject. In the main however, the various cybercrime legislations enacted by different countries in the region have shown states consistently applying traditional territorially based rules to online conducts and refusing to acknowledge the borderless nature of the Internet.

This paper appraises the adequacy of present legal responses to jurisdictional challenges of transnational cybercrimes in the African region. It is divided into five parts. This part, the introduction, is the first part. The second discusses the concept of jurisdiction in international law. The third identifies jurisdictional challenges or issues of TNCCs. The fourth examines domestic and regional responses to cybercrimes in the African region for the purpose of determining their adequacy in resolving jurisdictional issues of TNCCs, while the sixth and final part contains the recommendations and conclusion.

2. MEANING OF JURISDICTION

A state's Jurisdiction can be said to be the state's legitimate assertion of authority to affect legal interests.[15] It refers to a state's authority under international law to regulate the conduct of persons, natural and legal, and to regulate property in accordance with its municipal law.[16] Jurisdiction has also been described as the power of a State in international law to regulate or otherwise impact upon people, property and circumstances.[17]

Put simply, jurisdiction to prescribe refers to a state's authority to criminalize given conducts. It includes a state's jurisdiction to enforce its authority, inter alia, to arrest and detain, to prosecute, try and sentence, and to punish persons for the commission of acts or offences so criminalized.[18]

There are five bases ordinarily relied on by States to assert jurisdictions over crimes. They include: the territorial principle, where jurisdiction is exercised by reference to the place where the offence is committed; the

15 M Z Öner, 'The Principle of 'Universal Jurisdiction' in International Criminal Law' (2016) 7(12) Law and Justice Review 177, 178; Q Trinh 'The Principle of Universal Jurisdiction' (2010) Australian Red Cross 5. See also M P Scharf, 'The ICC's Jurisdiction over the National of Non Party States: A Critique of the US Position' (2001) 64(1) Law and Contemporary Problems 67, 71

16 Öner, 'The Principle of 'Universal Jurisdiction' (n 15) 177

17 Malcom N Shaw *International Law* (Cambridge University Press 2016) 469

18 C K Randall 'Universal Jurisdiction under International Law' (1988) 66 Texas Law Review 785, 785; I Brownlie, *Principles of Public International Law* (Oxford University Press 1998) 301; R O'Keefe, 'Universal Jurisdiction: Clarifying the Basic Concept' (2004) 2 Journal of International Criminal Justice 735, 736-737 and Trinh (n 5) 6

nationality principle, where jurisdiction is assumed on the basis of the nationality or national character of the person committing the offence; the protective principle, where jurisdiction is exercised by virtue of the national interest injured by the offence; the universality principle, where jurisdiction is assumed on the basis of the custody of the person committing the offence and the passive personality principle where jurisdiction is assumed on the basis of the nationality or national character of the person injured by the offence. These criminal jurisdictions can rest on territorial or extraterritorial basis. In all cases of extraterritorial jurisdiction, the prosecuting state must establish a connection with either the criminal conduct, the offender, the victim or the affected interest.[19] It is only in the case of universal jurisdiction that no such link is required.[20]

Universal jurisdiction is the right of a state to define and prescribe punishment for certain offences recognized by the community of nations as of universal concern regardless of whether or not the prosecuting state can establish a connection with the perpetrator, the victim or the location of the offense.[21] The exercise of universal jurisdiction is not without some difficulties. The exercise of jurisdiction under this principle by a state without any form of connection with the requisite criminal conduct, location or victim ordinarily amounts to a violation or an infringement on the sovereignty of a state with a closer or more direct connection with the offense.[22] Other concerns that have been expressed are issues of legitimacy, practicality and political ramification. Some even fear that stronger nations could use universal jurisdiction as an excuse to invade weaker ones.[23] In spite of these concerns, universal jurisdiction is increasingly being recognized in the international community. Universal jurisdiction has been used in the prosecution of crimes of genocide, war crimes, crimes against humanity, torture, terrorism, and for a long time piracy.[24]

19 Amos Enabulele and Bright Bazuaye, *Teachings on Basic Topics in Public International law* (1st edn, Ambik Press 2014) 233 According to Enabulele and Bazuaye such necessary connection have the effect of tampering the truly extraterritorial character of such criminal conduct. See Enabulele and Bazuaye, *Teachings on Basic Topics in Public International law*, 244.

20 Öner, 'The Principle of 'Universal Jurisdiction' (n 5) 174

21 ibid

22 ibid

23 ibid

24 B Bazuaye and A Fenemigho, 'Universal Jurisdiction Fault Lines and the Immunity of State Officials Salutary Warning Before Perdition' (2018) 26(4) African Journal of International Comparative Law 548.

3. ISSUES OF JURISDICTION OF TNCCS

According to Weber, the jurisdictional problems in the prosecution of cybercrime manifest itself in three ways: lack of criminal statutes, lack of procedural powers and lack of enforceable mutual assistance provisions with foreign states.[25] While it may no longer be accurate to say that there is a complete absence of legal and technical facilities for the prosecution of cybercrimes, it is true that the inadequacy of existing facilities for the investigation and prosecution of cybercrime, especially transnational cybercrimes, constitutes a challenge.

3.1 Absence of, or Inadequacy of Cybercrime Specific Legislation in Some States.

More recently at the 2nd African Forum on Cybercrime held on the 28th -29 of June 2021, it was stated that the major challenges to the effective prosecution of cybercrime in the region can be found in policy and legislation; the majority of which stem from the lack of common understanding on cybercrime among criminal justice authorities, insufficient cybercrime legislation harmonization, lack of or no common definition on cybercrime, insufficient standardization which results in identification, collection and use of e-evidence and admissibility issues.[26]

According to Clough, no other type of crime can become transnational so effortlessly like cybercrime.[27] This is because even where the offender and the victim are in the same jurisdiction, evidence of the offence may have passed through or be stored in other jurisdictions. As a result of this, it is thus important that there be some degree of harmonization between countries in order to effectively regulate cybercrimes. This is because harmonization will help to eliminate safe havens and increase cooperation among states.[28]

Significantly, a lot has been done in the African region since the United Nations' General Assembly's Resolution 55/63 of 4th December 2000 which called on states to ensure that their laws and practice eliminate safe havens

25 Amelia M Weber, 'The Council of Europe's Convention on Cybercrime' (2003) 18 Berkeley Technology Law Journal 425
26 Council of Europe, 'Second African Forum' (n 5).
27 Clough, *Principles of Cybercrime* (n 1) 4.
28 ibid

for those who criminally misuse information technologies. As at 2016, 22 countries have enacted cybercrime legislation and the number is increasing by the day. A good number of states in the African region have enacted cybercrime specific legislation in the last decade, while others are updating existing ones.[29] However, just as Clough also noted, although desirable harmonization presents considerable challenges when seeking to address complex issues like substantive and procedural laws, mutual assistance and extradition. This is because different states have different perspectives which have been shaped by their legal tradition as well as their cultural and historical factors.[30]

While it is true that a significant number of states in the region have enacted cybercrime specific laws, there are still some that are yet to do so.[31] States that are without adequate cybercrime laws constitute safe havens for cybercriminal. Clough sums up the challenge of harmonization better when he stated that the global reach or international dimension of interconnected network 'presents enormous challenge to law enforcement and harmonization'.[32]

The presence of safe havens (countries with inadequate cybercrime legislations) thus continues to present a major challenge in the fight against cybercrime. It remains one of the foremost jurisdictional issues constituting a challenge to the effective prosecution of transnational cybercrime. Even though cybercrimes have become a phenomenon of global concern, there are still countries without specific legislations for cybercrime. Out of 57 countries in the Africa region, less than half have criminal statutes prohibiting cybercrimes.[33] In a survey carried out by the council of Europe on the current state of cybercrime legislation in Africa, in 2016, a cursory overview of the 54 countries of Africa in terms of specific criminal law provisions on cybercrime and electronic evidence

29 Mauritius is currently updating it laws on the subject

30 Clough, *Principles of Cybercrime* (n 1) 4

31 According to a November 2016 report of the African Union Commission (AUC) and the cybersecurity firm Symantec, out of the 54 countries of Africa, 30 lacked specific legal provisions to fight cybercrime and deal with electronic evidence. Law enforcement officials in some countries do not take major actions against hackers attacking international websites. See Nir Kshetri, 'Cybercrime and Cyber Security in Africa' (2019) 22 Journal of Global Information Technology Management 77, 78. Zimbabwe introduced its Cyber Security and Data Protection Bill in May 2020. See Jennigay Coetzer, 'Africa's Lack of Data Protection and Cybercrime Laws has Created Deep Vulnerabilities: but is Change on the Way?' <https://www.law.com/international-edition/2020/05/27/africas-lack-of-data-protection-and-cybercrime-laws-has-created-deep-vulnerabilities-but-is-change-on-the-way/?slreturn=2020> 'accessed 17 October 2021.'

32 ibid

33 E F G Ajayi, 'Challenges to Enforcement of Cyber-crimes Laws and Policy' (2016) 6 Journal of Internet and Information Systems 1, 2

revealed that as at April 2016, only 11 States[34] seemed to have basic substantive and procedural law provisions in place, a further 12 States[35] seemed to have substantive and procedural law provisions partially in place while the majority of African States did not have specific legal provisions on cybercrime and electronic evidence in force. Draft laws or amendments to existing legislation reportedly had been prepared in at least 15 States[36] and in some instances, bills had been presented to national parliaments, in others the fate of draft laws were uncertain.[37] States without cybercrime specific legislations act as safe havens for cybercriminals and reduces the effectiveness of cybercrime legislations in countries with advanced cybercrime legislations. At the time of the report, 17 states[38] constituted safe haven for cybercrime as they had no statute prohibiting cybercriminal conducts.

Admittedly, some countries have enacted cybercrime legislation in the last five years since the report was given in 2016. At the 2nd African Forum on cybercrime held recently in June 2021, it was reported that 41 countries in the African region now have substantive criminal law provisions partly or largely in place to deal with cybercrime and 16 countries have procedural legislation in place to secure evidence necessary for effective prosecution of cybercrime.[39] However, while it is true that some countries that once constituted safe havens have now enacted cybercrime specific legislation, the problem of safe haven is far from over.[40] It is therefore true that in spite of the increased awareness of the threat presented by cybercrime, states that are yet to enact statutes that specifically criminalize cybercrime constitute safe havens and present jurisdictional challenges to the prosecution of transnational cybercrimes in the African region. At the same time, the speed of development coupled with

34 Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia

35 Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe

36 Burkina Faso, Djibouti, Ethiopia, Guinea, Kenya, Lesotho, Mali, Morocco, Namibia, Niger, South Africa, Swaziland, Togo, Tunisia, and Zimbabwe

37 Council of Europe (n 5).

38 Algeria, Equatorial Guinea, Gabon, Guinea, Guinea Bissau, Angola, Burundi, Cape Verde, Central Africa Republic (CAR), Comoros, Democratic Republic of Congo, Dibouti, Eygpt, Eritea.

39 Mauritius is currently updating it laws on the subject

40 As at March 2018, countries such as Libya, Mali, Guinea Bissau, Sierre leone, Togo, Eritea, Gabon, Demoncratic Republic of Congo, Angola, Namibia, Swaziland, Lesotho, Central Africa Republic, Somalia and Comoros still constituted safe havens. See Matteo Lucchetti, 'Cybercrime Legislation in Africa: Regional and International Standard' (GLACY+ - Global Action on Cybercrime Extended) 12 April 2018 <https://au.1nt>newsevents> 'accessed 17 October 2021.'

its sophistication along with the increasing advance in technology continues to challenge the adequacy of present legal responses to cybercrime in States where such legislations exist.

Closely associated with inadequacy of present cybercrime specific legislation, is the issue of coverage. According to World Internet Users and Population Statistics of 2016, over 3 billion people have access to the Internet.[41] The effect of this is that the Internet provides an unprecedented pool of potential offenders and victims which allows offences to be committed on a scale that could not have been committed otherwise. Coupled with this is the fact that modern computer systems now available in the markets are powerful and can be used to extend criminal activities. In most cases, cybercriminals infect computers with malicious software that allows them to take control. They can use botnets to gather information about targets or for high level attacks. The size of a botnet can vary from a few computers to more than a million computers. The increase in the numbers of compromised computers also increases the danger that can result as well as the scale of the resulting consequences. This aspect of cybercrime makes purely domestic legal responses to it, even where they are available and up to date, inadequate.

In addition, modern computer networks challenge the use of territorial jurisdiction in the prosecution of criminal offences. Individuals can now communicate with people living overseas as if they were next door neighbors and offenders are taking advantage of this development to commit crime and cause harm anywhere there is Internet connection. In a study conducted by the United Nations Office on Crime and Drugs in 2013, over half of the responding countries stated that between 50 and 100 per cent of cybercrime acts that are encountered by their police involved a transnational element.[42] This international dimension of the internet or interconnected networks does not only provide a world of opportunity to offenders, it also present enormous challenges to law enforcement and harmonization. The possibility of an international element has been added to almost all cybercrimes. Some criminals may deliberately weave communications through multiple countries in order to avoid being traced.[43]

41 This figure has no doubt increased in the past 5 years.

42 United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime: Draft – February 2013' <unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/ CYBERCRIME_STUDY_210213.pdf> 'accessed 18 May 2019.'

43 Chris Uwaje, 'Nigeria and the Challenges of Cyber Crime –Part 4' <http://www.techtrendsngcom/nigeria-and-the-challenge-of-cyber-crime-part-/> 'accessed 6 February 2015.'

3.2 Inadequate procedural powers

Another problem associated with the prosecution of TNCCs is that of inadequacy of procedural powers. States often lack resource and procedural tools necessary to conduct computer crime investigations.[44] In a November 2016 report of the African Union Commission and the Cyber security firm Symantec, about 30 countries in the African region lack procedural provisions to deal with electronic evidence in the fight against cybercrime.[45]

The complex technical and legal issues raised by computer-related crime require that each jurisdiction have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications.[46] The complexities of these technologies, and their constant and rapid change mean that investigating and prosecuting offices must designate investigators and prosecutors to work these cases on a full time basis, immersing themselves in computer-related investigations and prosecutions.[47] Recently, Mauritius reported a steep increase in the number of cybercrime offences as a result of the technical challenges that its prosecution presented to the police force, other law enforcement agencies and for the magistrate and prosecutors. This challenge was only surmounted by the training initiative of the Council of Europe GLACY + project[48]

Giving the quickly evolving nature of computer technology, countries must continue to increase their computer forensic capabilities which are essential in computer crime investigations and because of the speed at which communication technologies and computer evolve; prompting rapid evolution in criminal tradecraft, experts must receive regular and frequent training in the investigation and prosecution of high-tech cases.[49] In the absence of such training and facilities, law enforcement agents are unable to effectively prosecute cases of TNCC and this constitute jurisdictional challenge.

44 Weber, The Council of Europe's Convention' (n 26) 425.
45 Kshetri, 'Cybercrime and Cyber Security in Africa' (n 6) 78
46 Weber, 'The Council of Europe's Convention' (n 26) 425.
47 ibid
48 Global Action on Cybercrime Extended Project.
49 Weber, 'The Council of Europe's Convention' (n 26) at 426

3.3 Inadequate enforceable mutual assistance provisions.

Inadequate enforceable mutual assistance provision with foreign States is also a problem that constitute a jurisdictional issue for TNCCs. Even when both the host and victim states have adequate criminal statutes and investigative powers, prosecution is frustrated in the absences of enforceable cooperation.[50]

International cooperation between criminal justice authorities is needed for several potential reasons; data is volatile and likely to be found outside the jurisdiction of the prosecuting state; supplementary forensic skill might be necessary as international cooperation is a two way street. A comprehensive and coherent international standard on cybercrime and electronic evidence is a requirement for effective prosecution of transnational cybercrime in the African region.[51] The absence of this presents jurisdictional challenges,

Commenting on this challenge, Uwaje stated that 'inadequate regimes of international legal assistance and extradition can shield cybercriminals from law enforcement.'[52] As France's President Jacques Chirac once stated at a G8 Cybercrime Conference in Paris, "what we need is the rule of law at an international level, a universal legal framework equal to the world wide reach of the Internet." [53]The above jurisdictional issues are particularly evident in the context of TNCCs.

4. LEGAL RESPONSES TO TRANSNATIONAL CYBERCRIME IN THE AFRICAN REGION

4.1 Domestic Legal Response

As already noted, 41 countries in the African region now have substantive criminal law provisions partly or largely in place to deal with cybercrime and 16 countries have procedural legislation in place to secure evidence necessary for effective prosecution of cybercrime. This section examines some of this legislations in selected countries in other to determine their adequacy in

50 ibid 427
51 Council of Europe, 'Second African Forum on Cybercrime' (n 5)
52 Uwaje, 'Nigeria and the Challenges of Cyber Crime' (n 44).
53 Jacques Chirac cited in S S Murphy, *United States Practice in International law* (Cambridge University Press 2002) 347

resolving jurisdictional issues of transnational cybercrimes in the region. The choice of countries is done to reflect states with both substantive and procedural laws as well as states with only substantive legislations. Additionally states selection also reflects the level of advancement of legislations as some states have painstaking updated their cybercrime laws to reflect modern realities in the field while others are yet to do so.

4.1.1 Cameroon

Cameroon is one of the countries with cybercrime specific legislation in the region. The Cyber security Law and the Electronic Communications Law both relates to cyber security and cyber-criminality in Cameroun. These laws govern the security framework of electronic communications networks and information systems.[54] The Section 1 of the Cyber security and Cyber criminality Law defines and punishes offences related to the use of information and communication technologies,[55] while Electronic Communications Law harmonizes the substantive criminal law element of offences connected with provisions in the area of cybercrime. It also ensures that there is a domestic procedural law necessary for the investigation and prosecution of offences related to or committed by means of a computer system.[56] Part IV of the Electronic Communication Law makes provision for international cooperation and mutual judicial assistance. It comprises of chapters 1 and 2. Chapter 1 which is section 90 contains the provision for international cooperation. The said section provides:

> (1) In the discharge of their duties, Cameroonian Certification Authorities may, under the control of the Agency, conclude conventions with foreign Certification Authorities.
>
> (2) The conditions for concluding the conventions referred to in Subsection 1 above shall be laid down by regulation[57]

From the above it is evident that such cooperation is premised on

54 AfrICT 'Full Text in English: Cybersecurity and Cyber criminality Law in Cameroun' <www.africt.com/2013/11/camerou n-law-0n-cybersecurity-and-cybercriminality.html> 'accessed 3 July 2017.'

55 Cyber security and Cyber criminality Law, Law No. 2010/012 of 2010, s 1

56 P N Asongwe, 'E- Government and the Cameroon Cybersecurity Legislation 2010: Opportunities and Challenges' (2012) 12 African Journal of Information and Communication 158, 159

57 Cyberseurity and Cybercriminality Law 2010, s 90.

the existence of mutual legal assistance agreement with foreign States. Section 91(4) erases any doubt by stating categorically that request for mutual judicial assistances are subject to international conventions. The effectiveness of the above will thus require the existence of partnership with foreign States. However, according to the International Telecommunications Union (ITU), 'Cameroun does not have officially recognized partnerships to facilitate sharing of cyber security assets across borders or with other states'.[58] Thus, combating cybercrime in Cameroon is still a challenge owing to a number of factors. For one thing, Cameroon still has little partnership with foreign countries in relations to mutual legal assistance in relation to cybercrime. Perhaps this was one of the deficiencies sought to be cured by the promulgation of the Electronic Communication Law, but unfortunately, the Electronic Communication Law does not seem to have achieved much success in this regards. This is majorly due to the fact that the provision on international cooperation relies on the existence of cybercrime laws in other countries and as a result, the non-existence of cybercrime specific laws in neighbouring countries challenges the effectiveness of the Electronic Communications Law.[59]

While the presence of cybercrime specific laws in neighbouring countries will improve the effectiveness of the above law, it should be noted that reliance on Mutual Legal Assistance Treaty (MLAT) alone which is the heart of the provisions of section 90 to 94 of the Electronic Communication Law is not without its drawbacks, such MLATs place too much emphasis on extradition which requires the double criminality principle, a two edged sword, to function and more than that, TNCCs are more global in nature and cannot be restricted by territorial boundaries.

Therefore, in spite of the existence of a cybercrime specific legislation in Cameroon, jurisdiction will continue to constitute a challenge in the prosecution of TNCCs because the provisions of sections 90 to 94 in Part IV of the Electronic Communications Law are inadequate as the majority of the surrounding neighbouring countries are without cybercrime specific legislations.

Most importantly, Asongwe have observed and rightly so, that while the 'country is taking measures to combat computer-based crimes,[60] it

58 ITU 'Cyberwellness Profile Cameroon' <www.itu.int>country_profiles> 'accessed 3 July 2017.'

59 Asongwe, 'E- Government and the Cameroon, (n 57) 161.

60 As evident in the review of the above cybersecurity and electronic communication legislation in 2015

acknowledges that national laws alone are not sufficient to address the global nature of cybercrime because online crimes are inherently international'.[61]

4.1.2 Kenya

Another state that have enacted cybercrime specific legislation in the African region is Kenya. Its most recent law regulating cybercrime is the Computer Misuse and Cybercrimes Act, 2018.[62] The Act provides for offences relating to computer systems and establishes the national computer and cybercrimes coordination committee. It contains provisions protecting confidentiality, integrity and availability of computer systems, programs and data. It also provides for timely and effective prevention, detection, investigation, prosecution and punishment of computer and cybercrimes. Significantly, it provides for international cooperation in dealing with computer and cybercrimes matter.[63] It criminalizes conducts such as illegal access, data and system interference, child pornography and other computer related fraud.[64] The Act is aimed at improving investigation in cybercrimes by making provisions for procedural law tools and securing electronic evidence for effective national and international cooperation.[65]

Its provision for international cooperation is contained in part V (section 57- 65). Particularly, section 57(1) to (4) provides as follows:

> 57 (1) this part shall apply in addition to the Mutual Legal Assistance Act, 2011 and the Extradition (Contiguous and Foreign Countries) Act.
> (2) The Central Authority may make a request for mutual legal assistance in any criminal matter to a requested State for the purposes of –
> (a) Undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or data;
> (b) Collecting evidence of an offence in electronic form; or

61 ibid 162.

62 John Walubengo and Mercy Mutemi, 'Treatment of Kenya's internet intermediaries under the Computer Misuse and Cybercrimes Act 2018' ((2018) 21 AJIC 1, 5

63 Mahesh Acharya and Neema Oriko, 'Kenya: Kenya's computer Misuse and Cybercrimes Act, 2018: Suspended Provisions Now Effective' <https://www.mondaq.com>security> 'accessed 18 October 2021.' Also see Mohamed Daghar, 'Cybercrime: Is Kenya the New Playground for Cyber Criminals?' (04 February, 2020), <https//www.enactafrica.org/research> 'accessed 18 October 2021.'

64 K Shitemi, 'Cabinet Approves the Computer and Cybercrime Bill 2016' <www.ifree.co.ke/2014/cbinent-approves-computer-cybercrime-bill-2016/> 'accessed 5 July 2017.'

65 ibid

> (c) Obtaining expeditious preservation and disclosure of traffic data, real-time collection of data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act.
> (3) A requesting State may make a request for mutual legal assistance to the Central Authority in any criminal matter for the purposes provided in subsection (2).
> (4) Where a request has been received under subsection (3), the Central Authority may subject to the provisions of the Mutual Legal Assistance Act 2011, the Extradition (Contiguous and Foreign Countries) Act, this Act and any other relevant law-
> (a) Grant the legal assistance requested; or
> (b) Refuse to grant the legal assistance requested.

From the above, international cooperation is evident in the fact that the Central authority may make request for mutual legal assistance in any criminal matter to a requested state for the purposes of undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or data; collecting evidence of an offence in an electronic form or obtaining expeditious preservation and disclosure of traffic data, real time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provision under the act. In the same vein, subsection 3 provides that a requesting state may make a request for mutual legal assistance to the Kenyan central authority in any criminal matter for the same purposes.

However, the above cooperation is subject to the provision of the Mutual Legal Assistance Act, 2011 and the Extradition (Contiguous and Foreign Countries) Act. Section 7 of the Mutual Legal Assistance Act 2011 provides that the 'Court may request the temporary transfer of a person in custody for purposes of identification or for obtaining testimony or other assistance subject to such conditions as that State and the Court may agree.' One of such conditions is stated in part 2 (section 3) and 3 (section 11) of the Extradition (Contiguous and Foreign Countries) Act 2018. The said sections provides thus:

> 3(1) Where an agreement has been made with any country other than a designated Commonwealth country within the meaning of the

Extradition (Commonwealth Countries) Act (Cap. 77), with respect to the surrender to that country of any fugitive criminal, the Minister may, by order published in the Gazette, declare that this Part of this Act shall apply in the case of that country subject to such conditions, exceptions and qualifications as may be specified in the order, and this Part shall apply accordingly.

(2)An order made under this section shall recite or embody the terms of the agreement and shall not remain in force for any longer period than the agreement.

(3)Every order made under this section shall be laid before the National Assembly.

11(1) Where the Minister is satisfied that reciprocal provision has been or will be made by or under the law of any contiguous country other than a designated Commonwealth country within the meaning of the Extradition (Commonwealth Countries) Act (Cap. 77), for the backing of warrants issued in Kenya and their execution in that country and that it is appropriate to do so, he may, by order published in the Gazette, declare that this Part of this Act shall apply in the case of that country subject to such conditions, exceptions and qualifications as may be specified in the order, and this Part shall apply accordingly.

(2)Every order made under this section shall be laid before the National Assembly

As seen above, a major condition for cooperate with Kenya is reciprocity. Therefore, as significant as this provision is with respect to TNCCs, a major challenge to its effectiveness is the willingness or lack thereof of other states to accept or reciprocate by adopting similar arrangements. In the absence of similar practice by other states, combating TNCCs originating from other states in Kenya will continue to be challenged by jurisdictional issues.

4.1.3 Mauritius

Mauritius is one of the states in the region that has both substantive and procedural

laws in place to combat cybercrime in the African region. A significant legal response to cybercrime in Mauritius is the Computer Misuse and Cybercrime Act.[66] The Act criminalizes unauthorized access to, or modification of computer held data or software.[67] It created specific offences to deal with hacking, creation and dissemination of malicious codes and related criminal activities that have plagued computer users for years. [68]

Part IV of the Act labelled miscellaneous deals with criminal prosecutions, jurisdiction, extradition, forfeiture and consequential amendments. For our purpose the provisions on jurisdiction and extraditions contained in sections 19 and 20 respectively are of interest, as they are the only provisions of significant consideration in relation to international cooperation on TNCC.

Section 19(2) provides that the country's domestic court shall have jurisdiction to try any act constituting an offence under the Act committed outside Mauritius where the said act is committed on board a Mauritian ship or on board an aircraft registered in Mauritius. Section 20 provides that any offence under sections 3, 4, 5, 6, 7 and 10 of the Act are extraditable. That is, they are crimes for which extradition may be granted or obtained under the Extradition Act. On the face of it, this would seem to be a significant attempt at international cooperation in fighting transnational cybercrime. However its inadequacy is evident on a close inspection of Article 3 of the Mauritius Bilateral Extradition Treaties.

The said Article 3 listed crimes for which extradition shall be granted but stipulates clearly that it would only do so reciprocally and provided that such acts for which the fugitive is to be extradited is punishable by the law of the both high contracting parties. Here too we see the requirement of double criminality with it attendant advantages and difficulties. More than that, the requirement of reciprocity also has it challenges in the context of TNCC. What this means is that States without reciprocal arrangement with Mauritius will constitute a safe haven where cybercriminal can effectively act to undermine the effectiveness of this Act.

66 WIPO, 'The Computer Misuse and Cybercrime Act. No. 22 of 2003' available at www.wipo.int>edocs>lwxdocs>laws 'accessed 11 December 2017.'

67 Computer Misuse and Cybercrime Act, 2003 s 3-9

68 A Mootoo, 'Mauritius Computer Misuse Act' <http://hostintruder.wordpress.com2008/05/30/mauritius-computer-misuse-act/> 'accessed 11 December 2017.'

4.1.4 Nigeria

The Nigerian legal response to cybercrime is the Cybercrimes (Prohibition, Prevention, etc) Act 2015 (Act). This Act creates legal procedure for the investigation, prosecution and enforcement of its provisions. Essentially, it makes provision for international legal cooperation, National Forensic Laboratory and the creation of regulatory mandate over cybercrimes and cyber security in the office of the Attorney General of the Federation.

The provision on jurisdiction can be found in part vii of the Act. Section 52(2) and (4) provides for international cooperation by the Attorney General of the Federation of Nigeria and other foreign countries for the purpose of investigation aimed at detecting, preventing, responding and prosecuting cybercrime irrespective of whether or not there exists bilateral and multilateral agreement between Nigeria and the requested or requesting state.

As noted by Abdullahi, Muhammad and Aminu, the efficacy of these provisions depend on the will of such foreign states as well as their law enforcement agents to punish or assist in the punishment of such crimes.[69] Thus, where one state's law criminalizes cybercrime sought to be punished and the other state does not, cooperation in relation to such cybercrime may not be possible. Furthermore, where there is no extradition treaty between Nigeria and the other foreign state, cybercriminals cannot be extradited to Nigeria (or from Nigeria to such other foreign state wishing to prosecute) and this will act as a shield, thus limiting the effect of section 51 of the Act which stipulates that 'offences under the Act shall be extraditable under the extradition Act' since a state has no obligation in international law to turn over a criminal to the requesting party without any agreement to that effect.

4.1.5 South Africa

In its bid to combat cybercrime, the government of South Africa has enacted and implemented various pieces of legislation that touch on cybercrime. Most

69 I Abdullahi I, 'Cybercrimes (Prohibition , Prevention, ETC) Act 2015: Issues and Challenges in Nigeria' Being a paper written on behalf of the Faculty of Law, Usman Danfodiyo University, Sokoto at the 49th Annual Conference of the Nigerian Association of Law Teachers, held at Nasarawa State University, Keffi, on May 21 – 24, 2016, 1-17, 2.

notably is the Electronic Communication and Transaction Act 25 of 2002. This Act and its subsequent amendment contain no provision for international mutual cooperation. The South African State's legal frame work for international cooperation can be found in section 39 of its Constitution which states that when interpreting the Bill of Rights a court, tribunal or forum must take cognizance of international law and may consider foreign law. It is significant to note that South Africa is a signatory to the Council of Europe Convention on Cybercrime which addresses crimes committed over electronic media and require signatories to adopt substantive and Procedural laws for cybercrime. South Africa is also a member of Southern Africa Development Community (SADC). The SADC Model law on Computer Crime and Cybercrime provides for the harmonization of SADC region Country policies toward s cybercrime by primarily identifying cybercrime offences.[70]

4.1.6 Zambia

The Computer Misuse and Crimes Act 2004 was the first singular attempt to criminalize cybercrime in Zambia. It was enacted to address inadequacies in the computer/cybercrime law which at the time was mainly the Penal Code.[71] The act criminalizes unauthorized access to computer program or data; access with intent to commit or facilitate the commission of an offence, unauthorized modification of computer program or data, unauthorised use or interception of computer service, unauthorised obstruction of the use of computer, unauthorised disclosure of access code and causing computer to cease functioning among others.[72]

The Electronic Communications and Transactions Act 2009 repealed the Computer Misuse Crimes Act. Part XV of the Act defined cybercrime

70 Government of South Africa 'South Africa: Cybercrime Policies/ Strategies' <http://www.coe.int/en/web/octopus/country-wiki-/asset-publisher/> 'accessed 12 December 2017.'

71 These inadequacies became glaringly obvious with the hacking of the Zambian State House's website which resulted in publishing on the internet of the then president's caricature which act could not be prosecuted under the Zambian Penal Code and the incidents of fraud which became prevalent in the banking/financial institutions. See D N Kapumba, 'The Computer Misuse and Crimes Act 2004: Its Effectiveness in Combating Cyber Crime in Zambia' <www.dspace.unza.zm:8080/xmlui/handle/123456789/2895?show=full> 'accessed 11 May 2018.'

72 G Mukelabai G (2008) 'Cybersecurity in Zambia' being a paper presented at the ITU Regional Security Forum for Eastern and Southern African States, held in Chisamba, Zambia on the 25th to 28th of August, 2008 <http://www.itu.int> 'accessed 11 May 2018.'

and criminalizes categories of cybercrimes. It however made no provision for international mutual cooperation for TNCCs taking place or originating from or outside the Zambian shores. Perhaps this was because of the existence of the Extradition Act and the Mutual Legal Assistance in Criminal Matters Act 1998.[73]

The principal statute which regulates the extradition and surrender of suspects in Zambia is the Extradition Act.[74] The extradition Act necessarily requires that the conduct for which extradition is sought be criminal both in Zambia and the requesting State.[75] The provision of the Extradition Act is supplemented by the Mutual Legal Assistance in Criminal Matters Act.[76] This piece of legislation is meant to provide for the implementation of treaties of Mutual Legal Assistance on criminal matters. Under the Act, legal assistance in criminal matters is rendered by Zambia to the countries listed in the Order made by the Minister under Section 5. Although the Mutual Legal Assistance in Criminal Matters Act may supplement the provisions and procedures under the Extradition Act, section 4 of the Mutual Legal Assistance in Criminal Matters Act provides that nothing in the Act should be taken to authorise the extradition or arrest or detention with a view to extradition of any person. What this means is that, for the purpose of extradition and surrender, the principal instrument remains the Extradition Act.[77] The short coming of the Extradition Act like most extradition arrangements discussed earlier in this paper is the double criminality requirement which in the context of cybercrime act as a two edged sword.

The Mutual Legal Assistance in Criminal Matters Act makes provision for the implementation of treaties for mutual legal assistance in criminal matters between Zambia and states with which Zambia has such mutual assistance arrangement. However, this act is limited to States with which Zambia has such arrangement as evident in Section two of the Act where 'foreign state' is defined as a state that is a party to same treaty as Zambia and treaty is said to be 'a convention or other agreement that is in force and to which Zambia

73 Laws of Zambia, 1998 c 98.

74 Laws of Zambia, 1998 c 94

75 The countries with which Zambia can cooperate with for extradition purposes are broadly divided into commonwealth countries and foreign countries and there is the explicit assumption that the extradition arrangement will convey reciprocal obligations and benefits. See Extradition Act 1998, s 3 and s 45.

76 Laws of Zambia, 1998 c 98.

77 C Murungu and Japhet Biegon, *Prosecuting International Crimes in Africa* (Pretoria University Law Press 2011) 300

is a party, the purpose of which is to provide for mutual legal assistance in criminal matters' and offence in the said section is said to be an offence within the meaning of the relevant treaty. What this means is that there will only be cooperation where the transnational crime in question arises from or relates to States parties to treaties to which Zambia is a signatory. What is more, the treaty in question must provide for mutual cooperation in criminal matters for this act to be given effect. This mutual legal assistance arrangement as with most MLATs does not adequately resolve jurisdictional issues related to TNCCs.

4.1.7 Botswana

According to the recent statistics on the current cybercrime legislation on the African Region (the global action of cybercrime) a joint programme of the African Union Commission and the Council of Europe on cyber security and cybercrime, Botswana is one of the states in the region with both substantive and procedural law on cybercrime. Its most recent legislation on cybercrime is the Cybercrime and Computer Related Crimes Act. The Act criminalizes unauthorized access, unauthorized interference, unlawful interception of data, unlawful possession of devices or data, unauthorized disclose, cyber extortion, cyber fraud, cyber harassment, cyber stalking among others.[78] Its provision on procedural powers include provisions relating to preservation, disclosure of preserved data, production order, access, search and seizure, real time collection of content or traffic data, deletion order, acting without an order, limited use of disclosed data and information and non-compliance with order or notice.[79] The provisions for international cooperation can be found in section 33 which stipulates that cybercrimes and computer related crimes are extraditable offences. Section 33 states that an offence under the Act shall be considered to be an extraditable crime for which extradition may be granted or obtained under the Extradition Act.

Essentially, international cooperation under this Act relies majorly on extradition. A common requirement of most extradition arrangement is the dual or double criminality which requires that the requisite conduct be criminalized

78 Cybercrime and Computer Related Crimes Act 2018 Part II s 4-23.
79 Cybercrime and Computer Related Crimes Act 2018 Part III, s 24-32.

in both the requesting and requested jurisdictions.[80] In the context of TNCCs, the presence of safe havens make it difficult to meet this requirement.

While the above is just a sample and in no particular order, of some countries in Africa with cybercrime laws,[81] the enforcement of cybercrime laws have largely been hampered due to inadequate legislations in some states of the region and the ineffectiveness of same where they era available. It is also apparent that no matter how advanced, beautiful or sophisticated any domestic legal response may be, it will not sufficiently combat transnational cybercrime

4.2 The African Union Convention on Cybercrime and Cyber security and Personal Data Protection

The African Union Convention on Cyber security and Personal Data Protection, also known as the Malabo Convention, is the only document available at the regional level in the African region.[82] It was adopted on the 27th of June 2014 at the 23rd Session of the Summit of the African Union in Equatorial Guinea.[83] The Convention seeks to harmonize and strengthen African Cyber legislations on electronic commerce organization, personal data protection, cyber security promotion and cybercrime control. It also sets broad guidelines for incrimination and repression of cybercrime.[84] It defines the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa.[85]

The Convention requires states in the African region to adopt laws that

80 A Jones and A Doobay, *Jones on Extradition and Mutual Assistance* (Sweet and Maxwell 2014) 104-106

81 The cybercrime legislation discussed above is not exhaustive of countries with cybercrime laws in Africa. Tanzania for instance enacted the Cybercrime Act in 2015 and the provision on jurisdiction is contained in s. 30. However, as is the case with some of the countries discussed above, for Tanzania to assume jurisdiction over a cybercriminal conduct, there must be a connection between the cybercriminal conduct and the United Republic of Tanzania.

82 There are however other sub regional initiatives such as the East African Community Draft Legal Framework for Cybercrime (2008), the Economic Community of West African States Draft Directives on Fighting Cybercrime (2009), the Common Market Eastern and Southern Africa Cyber Security Draft Model Bill (2011) and the Southern African Development Community Model Law on Computer Crime and Cybercrime (2012)

83 Eric Tamarkin, 'AU's Cybercrime Response: A Positive Start, But Substantial Challenges Ahead' (2015) 73 Institute of Security Studies Policy Brief 3

84 Stein Schjolberg, 'A Geneva Declaration for Cyberspace' (2016) 12 Korean Institute of Criminology VFAC Review 4

85 African Union, 'Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa' < http://au.int/en/cyberlegislation> 'accessed 17 June 2018.'

criminalise attacks on computer system (illegal access), Computer data breaches (illegal interception), Content-related offence (such as disseminating child pornography) and Offences relating to electronic message security measures. In addition, African States under this Convention are to enact cybercrime offences that are punishable by effective, proportionate and dissuasive criminal penalties.[86]

The Convention emphasises the importance of enhancing international cooperation to fight cybercrime. Article 28 of the Convention requires states to harmonize cybercrime legislations and regulations to respect the principle of double criminality, in order to facilitate information sharing across border and enhance collaboration on bilateral and multilateral basis. The Convention further calls on member states without mutual legal assistance agreement on cybercrime to rectify this deficit.[87] A major significance of this Convention is that it brings to the fore, the need for African States to address the problems of cybercrime and tackle deficiencies in their cyber security.[88] The vast majority of African States without cybercrime legislation will now have to enact laws to this effect.[89]

However, the Conventions does not contain specific provisions on international cooperation. For example, the Convention does not establish a unified legal framework for all member states, it only guides them towards establishing their own cyber security and data protection laws. This is evident in the provision of article 8 which provides that each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of personal data, and punish any violation of privacy without prejudice to the principle of free flow of personal data and article 24 which stipulates that each State Party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy which recognises the importance of Critical Information Infrastructure for the nation identifies the risks facing the nation in using the all-hazards approach and outlines how the objectives of such policy are to be achieved.[90]

86 African Union Convention on cyber security and personal Data Protection Art 37
87 Tamarkin, 'AU's Cybercrime Response (n 86) 2.
88 ibid 4
89 ibid 2
90 Yarik Turianskyi, 'Africa and Europe: Cyber Governance Lessons' (2020) 77 South African Institute of International Affairs, Policy Insights 8

In addition, the Convention is yet to enter into force. For it to enter into force, the Convention needs to be ratified by 15 member states. As at 18th June, 2020 (six years after its adoption) only 14 states[91] in the African region had signed it and only 8 states[92] have ratified it.[93] The number of states that have ratified the Convention (less than one-third of the region) is suggestive of a lack of the necessary political will to implement the provisions listed in the convention.[94]

In the light of the above, the Budapest Convention is still the only international treaty on cybercrime and electronic evidence that includes substantive, procedural and international cooperation provisions that can be of use to the region. Significantly, five states in the region are full parties to the Budapest Conventions, 5 others have been invited to accede to it and one country have signed the convention but have not yet ratified it. Overall, 70 percent of African countries are using the Budapest Convention as a guideline or source. The African Union Convention and the Budapest Convention are complementary on legislative issues relevant to cybercrime and electronic evidence especially on the substantive part meaning that ratifying or acceding to one partially fulfils the requirement to ratify or accede to the other.[95]

Additionally, there is now a 2nd additional protocol to the Budapest convention on cybercrime which is expected to be adopted and open for signature by the year 2022. The aim of the 2nd additional protocol is to enhance international cooperation through tools for more efficient mutual assistance between countries, provisions for direct cooperation with private sector entities located in other parties, expedited cooperation in emergency situations, data protection safeguards will ensure that personal data shared under this protocol will be protected. It proposes solution for enhanced international cooperation including those permitting instant cooperation. According to George-Maria Tyendezwa, the assistant Director and head of the Cybercrime Unit of the Nigerian Federal Ministry of Justice, without international cooperation, it is impossible to record any success in the fight against cybercrime.[96] Therefore, the

91 Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia

92 Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda and Senegal

93 African Union, 'African Union Convention on Cyber security and Personal Data Protection' <www.au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> 'accessed 20 October 2021.'

94 Turianskyi, 'Africa and Europe: Cyber Governance Lessons' (n 93) 7- 8

95 Council of Europe, 'Second African Forum of Cybercrime' (n 5)

96 ibid

2nd protocol to the Budapest convention on cybercrime, which is a mile stone in fast tracking how international law works is indeed a welcome development, one that that African countries should key into in order to resolve the jurisdictional Challenges to the effective prosecution of transnational cybercrime.

5. CONCLUSION

From the above, it is evident that all the states of the African region will not at any given time have equal capacity in terms of legal (advanced cybercrime specific legislations) and procedural (investigation) facilities for use in combating cybercrime. There is need for an effective and adequate international cooperation. One that will allow or enable any African state with the requisite facilities to prosecute at material times. This article states that an operational regional instrument with provisions for effective and adequate international cooperation can fill this need.

A regional Convention can be used to establish a credible digital space for electronic transactions, personal data protection and combatting of cybercrime. The Malabo Convention acknowledged the absence of specific legal rules to ensuring cybersecurity in the region. With respect to cybersecurity governance and cybercrime control, the Malabo Convention recognizes that: 'the current state of cybercrime constitutes a real threat to the security of computer networks and the development of the information society in Africa.'[97] This threat will remain and continue to make parties to e-commerce vulnerable unless the operationalization of the Malabo convention is achieved.

This article recommends that efforts to get the Malabo Convention up and running should be a priority for the continent at this time and where possible, additional protocol to it should be negotiated to provide for enhanced international cooperation including those permitting instant cooperation as is currently being done by the 2nd additional protocol to the Budapest Convention on Cybercrime. Such additional Protocol should also address the challenges presented by the requirement of double criminality and ways of surmounting same.

The above will significantly address issues of jurisdiction in the African

97 Preamble, African Union Convention on Cybersecurity and Personal Data Protection, 2014.

region as it will ensure one jurisdiction for TNCCs in the African region. The fragmentation of present legal responses will not adequately resolve jurisdictional issues of TNCCs especially in the region. The need for a regional instrument is crucial.

Cybercrime respects no jurisdiction. It is borderless, transnational and sometimes even international, but the majority of the laws and policies dealing with cybercrimes in the region are largely territorial. The only regional instrument in the region, the Malabo Convention does not constitute a binding treaty as it is yet to come into force. Efforts should be made to ensure that the Malabo Convention comes into force and where possible, additional protocol to it should be negotiated to provide for enhanced international cooperation including those permitting instant cooperation as is currently being addressed by the 2nd additional protocol to the Budapest convention on cybercrime which is expected to be adopted and open for signature by the year 2022. In the alternative, states in the region are encouraged to become signatory to the Budapest Convention as it is presently the only binding law specifically dealing with cybercrimes which is international in character.