Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 2, Issue 1 (2022) p.49-81
https:doi.org/10.52907/jipit.v2i1.206

Eliminating Safe Havens for Transnational Cybercrimes in the African Continental Free Trade Area

*Flora Alohan Onomrerhinor, PhD**

ABSTRACT

The continuous advancement in technology makes cybercrimes effortlessly transnational. Existing literature reveals that the inadequacies of cybercrime-specific legislations, procedural powers, and enforceable mutual legal assistance provisions constitute jurisdictional challenges to the prosecution of transnational cybercrimes (TNCCs). This paper appraises the adequacy of legal responses to jurisdictional challenges of TNCCs in the African region, especially the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention). It argues that the presence of states without substantive or procedural laws on cybercrimes, or both, constitutes safe havens that challenge the effectiveness of such laws in states where they are present. It finds that the Malabo Convention has the potential to be a tool for eliminating safe havens in the African region and given the inter-connection between trade and TNCCs, it suggests that it could be made operational through its annexation as one of the protocols to the African Continental Free Trade Area (AfCFTA) Agreement. The author concludes that purely domestic legal responses to cybercrimes are inadequate and suggests a holistic approach through the operationalization of an effective regional instrument as a way to diminish safe havens for TNCCs in the African region.

Keywords: Jurisdictional Challenges, Transnational Cybercrime, Cybersecurity, Safe Havens, AfCFTA, Trade, Malabo Convention

* LLB, LLM, PhD, BL. Senior Lecturer, Department of Jurisprudence and International Law, Faculty of Law, University of Benin, Benin City, Nigeria. E-mail: flora.alohan@uniben.edu

TABLE OF CONTENTS

I. INTRODUCTION

Cybercrime is a global phenomenon. In today's world, there is an increased dependence on the internet and computer networks. Cybercriminals take advantage of this dependence on the internet to commit cybercrimes (Gercke, 2012, p. 3). A significant feature of cybercrime is that the elements of the crime can occur across several jurisdictions. Moreover, technological advancements have increased the severity and sophistication of incidents of cybercrimes such that they can now be transnational effortlessly (Clough, 2015, p. 3).

Cybercrime refers to any crime committed on a computer network, especially with the use of the internet (Luppicini, 2014, p. 35-37). 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, human trafficking, copyright infringement, and money laundering among others (Ladan, 2015, p. 38-79).

The ease with which information can be shared and stored on the internet renders it vulnerable and makes it a target for criminal activities. The relationship between cybercrime and opportunity is captured by the maxim, 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 (Clough, 2015, p. 6-8).

The well-known dimension and common problems surrounding the normal use of the internet such as ransomware, denial of service (DoS), phishing, and money laundering are highly pres-

ent in Africa. The African continent is one of the fastest-growing regions of the world in terms of internet penetration and the use of mobile-based financial services that it has become an increasingly attractive area for cybercriminals (Kshetri, 2019, p. 77). Similarly, cybercrime in Africa has rendered the use of the internet, particularly for e-commerce purposes a highly risky venture. As in other regions, organised crime groups in Africa use the internet for criminal ends, leveraging digital tools to contact and solicit victims. The Interpol-supported operations in Sarraounia saw the rescue of two hundred and thirty-two victims of human trafficking in Niger (Interpol, 2020). The operation revealed that one hundred and eighty male victims had been recruited online with messages that promised decent work. This incident shows that the internet can be used to facilitate human trafficking.

The African region is a growing global transit hub for goods sold and bought online. Cybercrime accounts for huge financial losses in the African continent. In 2017, Africa's Gross Domestic Product (GDP) was three point three trillion US dollars and the cost of cybercrime for the same year amounted to three point five billion US dollars (Signe & Signe, 2018). Each year, cybercrime costs the South African economy an estimated five hundred and seventy-three million US dollars, the Nigerian economy an estimated five hundred million US dollars, and the Kenyan economy, thirty-six million US dollars (Signe & Signe, 2018). These financial losses are compounded by the loss of productivity. For instance, the 2017 Wannacry cyber-attack forced companies around the world, including African states, to shut down. During the second African Forum on Cybercrime held on the 28th and 29th of June 2021, it was noted that cybercrime is one of the most pressing challenges impacting economic activity in Africa.

With the entire continent becoming a free trade area, there is a need to deter cybercrime by eliminating safe havens. A wide range of collective and far-reaching technical and legal measures can make it more difficult for cybercriminals to attack the security of infrastructures, services, and products (Wang, 2020, p.

233). 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 cyberterrorism. In the face of this reality, some countries have responded to the challenges of transnational cybercrimes by enacting legislation to address online conduct.

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 (Clough, 2015, p. 8; Brown, 2015, p. 55; Kigeri, 2012, p. 471).

Jurisdiction is a state's legitimate assertion of authority to affect legal interests. 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 by criminalizing given conduct and enforcing the authority, inter alia, to arrest and detain, to prosecute, try and sentence, and to punish persons for the commission of acts so criminalized (Oner, 2016, p. 177). Failure to assume jurisdiction over criminal conduct often results in situations where criminals feel safe to engage in criminal conduct in such states. In the author's opinion, this constitutes a safe haven and presents jurisdictional challenges. Furthermore, the reliance on information technology and the internet has become more pervasive in the COVID-19 and Post-COVID-19 African societies (African Pulse, 2021, p. 14). Unfortunately, the targeting and exploitation of computer systems have also become increasingly common (Nabe, 2022). Offences involving computers have grown rapidly in number as well as in sophistication, yet cybercrime and electronic evidence represent transnational challenges (Council of Europe, 2021).

This paper appraises the adequacy of the present legal responses to jurisdictional challenges of transnational cybercrimes in the African region. It is divided into six parts. This part I is

the introduction. Part II discusses the concept of jurisdiction in International Law and identifies jurisdictional challenges or issues of transnational cybercrimes (TNCCs). Part III examines the Council of Europe Convention on Cybercrime (2001) (the Budapest Convention) and the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) as regional instruments for combating cybercrimes. It discusses the potential of the Malabo Convention as a tool for eliminating safe havens in the African region and uses the positive aspects of the Budapest Convention to draw lessons for what could be well-applicable to the Malabo Convention. In part IV, as a recommendation, this paper considers the prospect of using the African Continental Free Trade Area Agreement to make the Malabo Convention operational. Part V contains the conclusion.

II. JURISDICTION AND TRANSNATIONAL CYBERCRIMES

A state's jurisdiction is sometimes regarded as the state's legitimate assertion of authority to affect legal interests (Oner, 2016, p. 177). 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 (Oner, 2016, p. 177). Jurisdiction has also been described as the power of a state in International Law to regulate people, property and circumstances (Shaw, 2016, p. 469).

Put simply, jurisdiction to prescribe refers to a state's authority to criminalize certain conduct. 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 (Brownlie, 1998, p. 301; O'Keefe, 2004, p. 736-737).

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

diction 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 based on the custody of the person committing the offence; and the passive personality principle where jurisdiction is assumed based on the nationality or national character of the person injured by the offence. These criminal jurisdictions can rest on a 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 (Enabulele & Bazuaye, 2014, p. 233).

Transnational crimes are defined broadly to cover not only offences committed in more than one state but also those that take place in one state but are planned or controlled in another. It includes crimes that are committed in one state by groups that operate in more than one state as well as crimes that are committed in one state but have an impact on other states. TNCC, therefore, refers to cybercrimes occurring across several jurisdictions. As stated earlier, jurisdiction refers to a state's authority to regulate the conduct of legal or natural persons and property using its municipal laws.

A. Jurisdictional challenges facing TNCCS

According to Weber (2003) the jurisdictional problems in the prosecution of cybercrimes manifest themselves in three ways: lack of criminal statutes, lack of procedural powers, and lack of enforceable mutual assistance provisions with foreign states (p. 426-427). A critical examination of cybercrimes reveals that they include both offences known to traditional criminal law but facilitated by modern technology as well as new offences made possible by modern or recent technological advancements. As a result, some peripheral aspects of cybercrime could be regulated by traditional penal law. Thus, while it may not 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. This challenge is examined below.

1. Absence of, or inadequacy of cybercrime-specific legislation in some states

Recently at the second African Forum on Cybercrime held in 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 of cybercrime, insufficient standardization which results in identification, collection and use of e-evidence and admissibility issues.

States that are without adequate cybercrime laws are safe havens for cybercriminals and reduce the effectiveness of cybercrime legislation in countries with advanced cybercrime legislation. The presence of safe havens presents a major challenge in the fight against cybercrime. It remains one of the foremost jurisdictional issues that prevent effective prosecution of transnational cybercrimes.

Since the United Nations General Assembly Resolution 55/63 of 4 December 2000, which called on states to ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies, the African region has recorded significant improvements. Twenty-two African countries have enacted cybercrime legislation and the number is progressive (African Union Commission, 2016). Although a good number of states in the African region have enacted cybercrime-specific legislation in the last two decades and others are updating existing ones, there are still some that are yet to do so.

For instance, Mauritius is currently updating its laws on cybercrime (African Union Commission, 2016; Kshetri, 2019, p. 77). Zimbabwe only recently introduced its Cyber Security and Data Protection Bill in May 2020. Further, at the second African Forum on Cybercrime held in June 2021, it was reported that forty-one countries in the African region had substantive criminal law provisions partly or largely in place to deal with cybercrime, and only sixteen countries had procedural legislations to secure evidence necessary for effective prosecution of cybercrime.

However, while it is true that some countries that were once safe havens have now enacted cybercrime-specific legislations, the problem is far from over.[1] It is still true that despite the increased awareness of the threat presented by cybercrimes, states that are yet to enact statutes that specifically criminalize cybercrimes are safe havens and present jurisdictional challenges to the prosecution of transnational cybercrimes in Africa (Lucchetti, 2018). At the same time, the speed of development coupled with its sophistication and the increasing advancement in technology continues to challenge the adequacy of present legal responses to cybercrime in states such as Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda, and Zambia where such legislations exist. (Kshetri, 2019, p. 79). This shows that purely domestic response to TNCCs cannot effectively eliminate the problem of safe havens.

In addition, modern computer networks challenge the use of territorial jurisdiction in the prosecution of cybercrimes. Individuals can now communicate with people living overseas as if they were next-door neighbours and offenders are taking advantage of this development to commit crimes and cause harm where there is internet connectivity. In a study conducted by the United Nations Office on Crime and Drugs in 2013, over half of

[1] As at March 2018, countries such as Libya, Mali, Guinea Bissau, Sierra Leone, Togo, Eritrea, Gabon, Democratic Republic of Congo, Angola, Namibia, Swaziland, Lesotho, Central Africa Republic, Somalia, and Comoros still constituted safe havens.

the responding countries stated that between fifty and hundred per cent of cybercrime acts that are encountered by their police involved a transnational element (UNODC, 2013). The transnational element of cybercrime can best be addressed in the African region through an effective regional instrument with provisions for international cooperation and procedural facilities.

2. Inadequate procedural powers

Procedural powers are specific procedural rules on investigation and preservation of evidence applicable to cyberspace such as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, and interception of content data (Cangemi, 2004, p. 165). They include procedural mechanisms meant to enhance the legal capabilities of law enforcement authorities to investigate and prosecute cybercrime offences such as measures to facilitate the search, seizure, or preservation of digital evidence, or the interception of electronic communications (Orji, 2018, p. 91).

Real-time evidence in cyberspace is volatile, that is, it can be easily lost or destroyed, and preservation has to be done in a short time. Unless there are evidentiary rules and provisions for international cooperation on how such data is to be located and obtained (search and seizure), it can be lost very quickly. Evidence gathering in TNCC is a dynamic, broad, and increasingly significant phenomenon that differs remarkably from evidence gathering in the traditional sense. Adequate procedural powers in the context of TNCCs require novel coercive measures, investigatory powers and tactics, and technical methods that can only be achieved by adjusting traditional principles of procedural justice (Riekkinen, 2016). For example, obtaining real-time evidence requires the power of sudden searches such as conducting digital forensic investigations against computers suspected to be sources or targets of cyber-attacks without judicial warrants where there are reasonable grounds to believe that computer crimes are likely to be committed. This may involve allowing

courts to rule ex parte, without hearing from the other party, upon request by investigators for a production order against a person thought to be in possession of computer data needed for the investigation, or granting a production order even without the presence of the person concerned that could have legitimate reasons to protest an otherwise unreasonable request, as well as disclosure of personal computer data in the course of enforcing such order. Nonetheless, these developments could violate data privacy rights or a mandatory duty to report that would prompt service providers to employ algorithmic bots to automatically detect illegality.

Adequate procedural powers or facilities thus require a balance between efficient criminal investigations and the rights of the individual, which is daunting to uphold. This has led to criticism of the Budapest Convention and the Ethiopian Cybercrime Proclamation (2016), the latter made provision for procedural and evidentiary matters like the preservation and production of computer data by service providers, rules by which computer data or systems could be searched, accessed and seized by investigators, rules on the admissibility of electronic evidence, and related authentication procedures and cooperation with law enforcement bodies of other countries and organizations (Yilma, 2016, p. 448).

Furthermore, the complex technical and legal issues raised by computer-related crimes require each jurisdiction to have individuals who are dedicated to high-tech crime and who have a firm understanding of computers and telecommunications. The complexities of these technologies and their constant 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. Recently, Mauritius reported a steep increase in the number of cybercrimes as a result of the technical challenges that its prosecution presented to law enforcement agencies and prosecutors. This challenge was only

surmounted by the training initiative of the Council of Europe GLACY + project (Council of Europe, 2021). Given the rapidly evolving nature of computer technology, countries must continue to increase their computer forensic capabilities, which are essential in computer crime investigations. Similarly, given the speed at which communication technologies and computers evolve, prompting rapid evolution in criminal tradecraft, experts must receive regular and frequent training on the investigation and prosecution of high-tech cases (Weber, 2003, p. 427). In the absence of such training and facilities, law enforcement agents are unable to prosecute cases of TNCC effectively and this constitutes jurisdictional challenges. An effective regional instrument addressing cyber security in the region should make provision for procedural facilities and cooperation in this regard.

In addition, some states lack the resources and procedural tools necessary to conduct computer crime investigations (digital forensic and technical surveillance). In a November 2016 report of the African Union Commission and the Cyber Security firm, Symantec, about thirty countries in Africa were reported to lack procedural provisions to manage electronic evidence in the fight against cybercrime (Kshetri, 2019, p. 77). A regional instrument such as the Malabo Convention, with provision for procedural facilities, could fill this need. The Malabo Convention and its operationalization is discussed subsequently in part III of this paper.

Given the above, most African states are either unwilling or unable to make adequate procedural provisions in terms of legislation, for the investigation of TNCCs because they require constant adjustments as criminality, technology, and society continue to evolve.

3. Inadequate enforceable mutual assistance provisions

Inadequate enforceable mutual assistance provisions with foreign states are also a jurisdictional issue for TNCCs. Even when both the host and victim states have adequate criminal statutes and investigative powers, prosecution is frustrated by

the absence of enforceable cooperation (Council of Europe, 2021). 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 (Council of Europe, 2021). 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. Inadequate regimes of international legal assistance and extradition can also shield cybercriminals from law enforcement.

What is needed is the rule of law at an international level as a requirement for the effective prosecution of transnational cybercrimes in Africa (2nd African Forum on Cybercrime, 2021). The absence of this presents jurisdictional challenges.

III. COMPARATIVE STUDY OF REGIONAL INSTRUMENTS ON CYBERCRIME

There are several regional instruments that can be construed as responses to TNCC, either because they directly or indirectly criminalize cybercriminal conduct or they act as reference points for mutual legal assistance on the subject. They include the Budapest Convention (2001), the Agreement on Cooperation Among the State Members of the Commonwealth of Independent States in Combating Offences Relating to Computer Information (CIS Agreement 2001), the Shanghai Cooperation Organization Agreement (2009), the Arab Convention on Information Technology Offences (2010), the Malabo Convention, the Organization of American States Comprehensive Inter-American Cyber Security Strategy (2004), and the Commonwealth Model Law.

According to Hakmeh (2017) the Budapest Convention is the most significant international legal instrument aimed at combating TNCC and crime against computer security (p. 10).

This is because the Budapest Convention addresses transnational, regional, and national concerns. It deals with cybercrimes directly and constitutes a binding legal agreement on the subject. Clough (2014) notes that the Budapest Convention is the most important international legislation on the subject because it is binding (p. 698). In addition, the Budapest Convention is the only instrument with the broadest reasonable support from different international organizations. Its provisions are not alien to the needs of the African region as evidenced by the fact that African countries such as Botswana, Egypt, and Nigeria have used the Convention as a model for drafting their laws (Ladan, 2015, p. 360-361).

A. The Budapest Convention

The Budapest Convention was created to address the jurisdictional issues posed by Internet evolution. Its solution was to harmonize cybercrime laws and ensure the existence of procedural mechanisms to assist in the successful prosecution of cybercriminals. It does this by creating a common cross-border criminal policy through the adoption of appropriate laws and fostering international cooperation (Weber, 2003, p. 424-425). The Budapest Convention is a modest effort to create a convergence of procedural laws to ensure that there are no safe havens for cybercriminals and to promote law enforcement cooperation (Aper Review, 2021, p. 7).

Moreover, the Budapest Convention is the first binding multilateral instrument to regulate cybercrime. It opened for signature on 23 November 2001 and entered into force on 1 July 2004 after Lithuania ratified it (Clough, 2014, p. 706). The Budapest Convention stipulates that it would come into force upon ratification by five nations, including at least three member states of the Council of Europe (Article 36(3), Budapest Convention).

Chapter two of the Convention enjoins all signatories to criminalise online activities such as illegal access, illegal inter-

ception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography and offences related to infringements of copyright and related rights (Articles 2-23 of the Budapest Convention). The above nine offences are criminalized in four categories: the first category targets offences against the confidentiality, integrity and availability of computer data and systems (the first five offences above, contained in Articles 2-6); the second category is the computer-related offences (the next two offences contained in Articles 7 and 8); the third category which is contained in Article 9 of the Convention is supplemented by the Additional Protocol Convention on Cybercrime, concerning the criminalization of acts of racist and xenophobic nature committed through computer systems, (2002 Protocol) adopted on the 7 November 2002. The 2002 Protocol is a separate legal instrument from the Budapest Convention and parties agreeing to the main treaty are not obliged to adopt it and it criminalizes the making of any dissemination of racist or xenophobic material through computer systems.

The fourth category of offences is the offences related to the infringement of copyright and related rights. Chapter two also includes ancillary provisions that require the establishment of laws against attempting and aiding or abetting the aforementioned crimes, as well as the establishment of a standard for corporate liability (Weber, 2003, p. 431). Parties to the Budapest Convention thus agree to adopt such legislative and other measures as may be necessary under their domestic law to criminalize the above cybercrimes and to make provisions governing aiding and abetting and corporate liability (Chawki, 2018). Chapter two further stipulates that state parties should require the operators of telecommunications networks or Internet Service Providers (ISPs) to institute more detailed surveillance of network traffic and where possible, real-time analysis.

Chapter three contains provisions for international cooperation. It provides three general principles of international coop-

eration. The first is that international cooperation will be provided among states to the widest extent possible (The Budapest Convention, a. 23) and requires that state parties cooperate in the investigation of cybercrimes by allowing data to be shared among them including cases where the crime being investigated in one state is not a crime in the state in which the information or cooperation is sought (Bannon, 2007, p. 122). This will also help to overcome the problem of dual criminality, which is usually a challenge in cases of TNCC, where one of the states involved is yet to criminalize the requisite conduct.

According to Seger (2011) the Budapest Convention requires state parties to establish specific types of conduct as criminal offences in their domestic legislation; provides criminal justice authorities with effective means of investigations through procedural law tools such as search and seizure, expedited preservation of volatile data, interception of communications and others, and engage in efficient international cooperation through a combination of urgent provisional measures (such as expedited preservation), and police and judicial cooperation.

With respect to jurisdiction, the Budapest Convention requires state parties to establish jurisdiction over offences established in Articles 2 to 11 when the acts are committed within its territory, on board a ship or aircraft flagged or registered under the laws of that party or by one of its nationals if the offence is punishable under the criminal law where it was committed, or if the offence is committed outside the territorial jurisdiction of any state. (The Budapest Convention, a. 22(1)). State parties may reserve the right not to apply, or to limit the application of any of the jurisdictional bases other than territoriality and the Budapest Convention does not exclude the exercise of criminal jurisdiction by a country under its domestic laws. Where more than one party claims jurisdiction over the same act, they are to consult with a view to determining the most appropriate jurisdiction.

Significantly, the Budapest Convention seeks to address some of the issues that present challenges in most traditional extradition treaties. Under Article 24, each of the offences established under Articles 2 to 11 is deemed to be extraditable offences in any extradition treaty between or among the parties. In addition, parties are to undertake to include these offences under any extradition treaty concluded between or among them (Clough, 2014, p. 707). Where parties require the existence of a treaty as a precondition of extradition, but none is in existence, the Budapest Convention may provide the necessary legal basis for extradition (The Budapest Convention, a. 23(4)). State parties that do not require a treaty for the purposes of extradition are to recognise these offences as extraditable ones (Clough, 2014, p. 707).

Articles 27 to 35 define the procedures related to requests for mutual assistance in the absence of enforced international agreements and the necessity to maintain the confidentiality of information requests. In addition, it provides for mutual assistance regarding the urgent precautionary procedures to be adopted regarding stored computer data related to cybercrime. (Hait, 2014, p. 78).

Article 35 requires state parties to maintain a constant point of contact for the purposes of investigations or proceedings concerning criminal offences related to cybercrimes, to collect evidence, to provide technical advice, or to preserve the data. The Group of Eight - G8 (Canada, France, Germany, Italy, Japan, Russia, United Kingdom, and the United States) have a permanent control point for the Internet that operates round the clock and gives a warning as soon as a hacker penetrates the international network. Once the alarm starts, some of the finest specialists work to locate the suspect, tracing their e-mail and identifying the area of their criminal activity. Among the objectives that the European Council is pursuing is to set up a remote inspection system to enable police to inspect a suspect's computer, remotely, and to expand the concept of Internet crime to criminalize access

to any confidential network information that is not dedicated to the public without a license (Hait, 2014, p. 78).

Under the Budapest Convention, the first contracting party is obliged to prosecute its citizen who commits cybercrimes. Where the criminal activity extends outside the state's territory, the convention obliges the prosecuting state to prosecute the criminal as if the crime was committed within its territory, and on the same degree of risk (Hait, 2014, p. 8). Although a regional initiative of the European Union, the Budapest Convention has been ratified by countries from other regions such as Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, South Africa, Sri Lanka, and the United States (Council of Europe, 2021). According to Ladan (2015) the Budapest Convention has broad support. Countries such as Argentina, Botswana, Egypt, Nigeria, Pakistan, and the Philippines have used it as a model and have drafted parts of their legislation in accordance with it without acceding to it formally (p. 360-361).

Notwithstanding the continuous effort of the Working Committee on the Budapest Convention to ensure the utility of the Convention in addressing trends in cybercrime, some commentators are of the view that the Convention's relevance may be limited by the advancement in technology and sophistication of modern cybercrimes. Maurushat (2010) argues that while an increase in the number of state parties to the Budapest Convention will reduce safe havens, the Convention's provisions are now of limited relevance because the use of modern obfuscation tools impacts the ability of law enforcers to combat many forms of cybercrime and the Convention may not be able to address this since it was negotiated in the earlier days of cybercrime, in the late 1990s with a final draft introduced in 2001 (p. 432).

In light of the above, Additional Protocols to the Budapest Convention have been negotiated. At present, plans to adopt the Second Additional Protocol are underway. The Second Additional Protocol aims to enhance international cooperation by providing tools for more efficient mutual assistance between countries.

The provision of tools for direct cooperation with private sector entities located in other states will expedite cooperation in emergencies and data protection safeguards will ensure that personal data shared under the Protocol will be protected. It proposes solutions for enhanced international cooperation including those permitting instant cooperation.

From the above, it is true that while the Budapest Convention is not without flaws, it remains the most significant regional response to TNCC. Its provision for international cooperation is key in addressing safe-havens. The Budapest Convention thus provides a model for the African region, especially in the area of instant cooperation.

B. The African Union Convention on Cybercrime and Cyber Security and Personal Data Protection (The Malabo Convention)

The Malabo Convention is the only document available at the regional level in Africa for addressing cybercrimes. However, there are 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 for Eastern and Southern Africa Cyber Security Draft Model Bill (2011) and the Southern African Development Community Model Law on Computer Crime and Cybercrime (2012).

The Malabo Convention was adopted on 27 June 2014 at the Twenty-third Session of the Summit of the African Union in Malabo, Equatorial Guinea (Tamarkin, 2015, p. 3). The Malabo Convention seeks to harmonize and strengthen the African cyber legislations on electronic commerce, personal data protection, cyber security promotion, and cybercrime control (Schjolberg, 2016, p. 4; Orji, 2018, p. 98). 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 (African Union, 2017). The Malabo

Convention requires states in the African region to adopt laws that criminalise attacks on computer systems (illegal access), computer data breaches (illegal interception), content-related offences (such as disseminating child pornography) and offences relating to electronic message security measures. Additionally, under Article 37 of the Malabo Convention, states of the region are required to enact cybercrime offences that are punishable by effective, proportionate and dissuasive criminal penalties.

Aside from establishing substantive and procedural criminal law provisions on cybercrime, the Malabo Convention also imposes broad obligations on member states to establish national cyber security policies as well as legal, regulatory and institutional frameworks for cyber security governance and cybercrime control (Orji, 2018, p. 100). Article 26 of the Malabo Convention establishes obligations on member states to promote a culture of cyber security amongst all stakeholders such as government institutions, businesses, and civil society that develop, operate, or use information systems and networks (Orji, 2018, p. 103).

The provision for international cooperation is contained in paragraph 1 of Article 28 of the Malabo Convention which obligates member states to ensure that the legislative measures or regulations adopted to combat cybercrimes will strengthen the possibility of regional harmonisation of these measures and respect the principle of double criminal liability. Paragraph 2 of the same article stipulates that member states that do not have mutual assistance agreements on cybercrime shall undertake to encourage the signing of agreements on mutual legal assistance in conformity with the principle of double criminal liability while promoting the exchange of information as well as the efficient sharing of data between the organizations of state parties on bilateral and multilateral bases.

Respect for and conformity with the principle of double criminality is a requirement for cooperation under paragraphs 1 and 2 of Article 28 of the Malabo Convention. Double criminality is

a common requirement of most extradition arrangements. It requires that the offence charged be considered criminal in both the requesting and the requested jurisdictions, usually subject to a minimum level of penalty (Jones & Doobay, 2014, p. 104-196). Double criminality is sometimes referred to as dual criminality. It protects states' rights by promoting reciprocity and safeguards individual rights by shielding the individual from unexpected and unwarranted arrest and imprisonment. Most extradition treaties require this principle to be met before an extradition request can be acceded to (Soma *et al.*, 1997, p. 223).

Extradition is not novel in international cooperation in criminal matters (Rohalska *et al.*, 2022, p. 138). It usually requires not only the existence of an appropriate treaty between the two countries concerned but also that the conduct in question be criminalized in both the referring and the receiving state(s). However, double criminality is not a necessary requirement for international cooperation or extradition under the Budapest Convention. Law enforcement officials in one state can, under the Budapest Convention, be obligated to comply with investigations concerning conduct that may not be illegal within their borders. This results from the Convention's lack of a double criminality provision, which would ordinarily require the conduct to constitute a crime in both countries before one state can procure the police of another state to aid its investigation.

The requirement of double criminality is a double-edged sword. In the context of the elimination of safe havens, it is more of an obstacle than protection. As discussed in part II of this paper, the state of cybercrime legislation in the region is such that African states do not have equal capacity in terms of legal (advanced cybercrime-specific legislation) and procedural (investigation) facilities for use in combating cybercrime. Therefore, the requirement of double criminality could stand in the way of an effective and adequate international cooperation regime that can enable any African state with the requisite facilities to prosecute at material times. Perhaps one way to retain the protection that

double criminality is supposed to provide without it constituting an obstacle is to remove the provision and provide an opportunity for ratifying states to express reservation to its non-inclusion. In order words, states should be allowed to make declarations to the effect that international cooperation will be subject to the double criminality principle, at the time of consenting to the instrument if that is their expectation.

Paragraph 2 of Article 28 also calls on member states without mutual legal assistance agreements or treaties (MLAT) on cybercrime to rectify this deficit (Tamarkin, 2015, p. 3). Although this provision requires states to have MLATs, it does not provide a guide as to what can be done in the absence of such agreements; this is unlike the Budapest Convention, which provides an alternative by stipulating that the Convention will in such cases constitute the necessary legal basis for extradition. By so doing, the Budapest Convention constitutes the necessary MLAT for such international cooperation (The Budapest Convention, a. 24(3)).

Paragraph 3 of Article 28 of the Malabo Convention requires member states to establish institutions that exchange information on cyber threats and vulnerability assessment such as Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). Paragraph 4 requires states to make use of existing channels for international cooperation to respond to cyber threats and improve cyber security and stimulate dialogue between stakeholders. Such channels for international cooperation may be based on international or intergovernmental or regional arrangements, or private and public partnerships (Orji, 2018, p. 108).

Moreover, the first paragraph of Article 24 of the Malabo Convention provides that each state party shall undertake to develop, in collaboration with stakeholders, a national cyber security policy that recognises the importance of critical information infrastructure for the nation and identifies the risks facing the nation in using the all-hazards approach and outlines how the

objectives of such policy are to be achieved (Turianskyi, 2020, p. 8).

Despite the above shortcomings of the Malabo Convention, it is a good starting point and holds some promise in helping to eradicate safe havens in the region. A major significance of the Malabo 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. African states without cybercrime laws will have to enact them in order to meet the obligation assumed under the Convention when they become signatories to it.

The Malabo Convention thus holds several prospects towards promoting regional cyber security in Africa. It increases policy and regulatory awareness on cyber security governance, while also improving the harmonization of national cybersecurity regimes in the African region. Additionally, it imposes positive obligations on member states to establish national cybersecurity regimes and increases the possibility of imposing African Union sanctions on non-compliant member states (Orji, 2018:114).

These positive obligations of the Malabo Convention can provide a basis for holding a member state accountable for failure to fulfil its obligations. The Malabo Convention is also a potential avenue for establishing states' responsibility under the principle of transboundary harm. In the *Corfu Channel Case*, the International Court of Justice (ICJ) held that a state may not knowingly allow its territory to be used for acts that are contrary to the rights of other states.

From the above, the Malabo Convention can be a tool for eliminating safe havens in the African region. But for this to happen, it will first have to become operational. Article 36 of the Malabo Convention states that the 'Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification'. However, as of June 2020, only

fourteen states[2] out of the fifty-five states of the African Union had signed it and eight states[3] had ratified it (African Union, 2020).

The slow pace of member states in signing and ratifying the Malabo Convention is an obstacle to operationalizing it. As a result, nearly one decade after its adoption, the timely achievement of its objectives such as the harmonization of cyber security laws is yet to take place. The number of states that have ratified the Malabo Convention (less than one-third of the region) is suggestive of a lack of the necessary political will to implement its provisions (Turianskyi, 2020, p. 8). It is particularly important that the Malabo Convention be operationalized since most of the states in the region are not signatories to the Budapest convention which is the only significant regional instrument on the subject. In addition, the Malabo Convention provides an opportunity to address trends in cybercrimes that may not have been envisaged in the 1990s when the Budapest Convention was negotiated. Moreover, now that the whole of the continent aims to become a free trade area under the African Continental Free Trade Area (AfCFTA) Agreement, it is imperative that this legal framework for cyber security becomes operational. One way to provide the necessary incentive is to use the Free Trade Area Agreement (FTA). This paper discusses this in the next subsequent part.

IV. ADDRESSING CYBER SECURITY UNDER THE AFRICAN CONTINENTAL FREE TRADE AREA

The AfCFTA Agreement was adopted on 21 March 2018, and it came into force on 30 May 2019 (African Union). It is a trade pact to form the world's largest free trade area by connecting

[2] These states are: Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mozambique, Mauritania, Rwanda, Sao Tome and Principe, Sierra Leone, Togo, Tunisia and Zambia.

[3] The states that have ratified the Malabo Convention are: Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal.

almost one point three billion people across fifty-four countries of the African region (Thomas, 2022). The AfCFTA is a continent-wide free trade area with the end goal of an economically seamless pan-African space where goods can be traded and business transacted fluidly across borders without costly tariffs (Brown, 2021, p. 293). As of 10 February 2022, all the countries of the Africa Union (save for Eritrea) were signatories to this trade agreement and forty-one countries out of this number had deposited their instruments of ratification with the chair of the African Union Commission, making them state parties to the agreement. Trading under the agreement commenced on 1 January 2021 (Thomas, 2022).

With this increase in commerce, there is an added incentive to make the regional instrument on cyber security operational. The absence of a common data protection policy in the AfCFTA Agreement has been noted to be a potential hindrance to establishing a common market for pan-African trade in digital goods and services (Daigle, 2021, p. 1). Similarly, cybercrime accounts for huge financial losses in the African continent.

The introduction of this paper highlights some of the financial losses that African countries record as a result of cybercrimes. In the year 2017, Africa's GDP was three point three trillion US dollars and the cost of cybercrime for the same year amounted to three point five billion US dollars (Signe & Signe, 2018). This is because hundreds of millions of cyber-attacks take place every year in the region (Fassassi & Akoussan, 2016). The figure could be much larger as African companies publish very few figures on cybercrime due to the unavailability of data occasioned by the absence of measuring tools and control of cybercrime (Fassassi & Akoussan, 2016). Annual losses from cybercrime for 2017 were estimated to be six hundred and forty-nine million US dollars for Nigeria and two hundred and ten million US dollars for Kenya. These financial losses are compounded by the loss of productivity. For instance, the 2017 Wannacry cyber-attack forced companies around the world, including African states, to shut down.

With respect to cyber security 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'.[4] This threat will remain and continue to make parties to e-commerce vulnerable unless the operationalization of the Malabo convention is achieved. Thus, the Malabo Convention has a role to play in establishing a credible digital space for electronic transactions, personal data protection and combatting cybercrime. it acknowledges the absence of specific legal rules to ensure cyber security in the region as a major obstacle to electronic commerce. Now that the whole of the continent is becoming a free trade area under the AfCFTA Agreement, it is imperative that this legal framework for cyber security becomes operational**.**

To achieve the above, the African Union should consider annexing the Malabo Convention to the AfCFTA Agreement, after all, paragraph 6 of the preamble of the AfCFTA agreement shows that the African Union is conscious of the need to create a secure market for the goods and services of state parties through adequate infrastructure. Also, the provisions of Article 8(3) of the AfCFTA Agreement, which provide that any additional instruments within its scope, as deemed necessary, shall be concluded in furtherance of the objectives of the AfCFTA and shall, upon adoption, form an integral part of the Agreement, show that not all areas of concern were addressed at the time of its adoption in 2018.

Therefore, it can be argued that cyber security and data protection are critical areas of concern for trade in goods and services that should come under the contemplation of Article 8(3) of the AfCFTA. Already, Article 8(2) envisions protocols, annexes and appendices, which equally form part of AfCFTA (Udombana, 2020). They are the Protocol on Trade in Goods, the Protocol

[4] Preamble, African Union Convention on Cyber Security and Personal Data Protection, 2014.

on Trade in Services, the Protocol on Rules and Procedures on the Settlement of Dispute, the Protocol on Intellectual Property Rights, the Protocol on Competition Policy, the Protocol on Investment and the Protocol on E-Commerce (African Union, 2021). Some of these aspects are under negotiation and the direction they take will play a great role in discerning the correct way forward.

Article 26 of the Malabo Convention, which places an obligation on Member States to promote a culture of cyber security amongst all stakeholders such as governmental institutions, businesses and the civil society that develop, operate, or use information systems and networks, will certainly prove relevant in the free trade area. The need for the promotion of a culture of cyber security arises from the increasing interconnection of networks and the growing integration of networked information communication technologies to many of the essential aspects of trade such as the provision of goods and services, research and development, innovation and entrepreneurship, and the free flow of information amongst individuals and organizations, governments, businesses, and civil society.

This state of affairs implies that cybersecurity governance issues are not meant to be addressed only through the application of law enforcement or technological measures, but rather through holistic governance approaches (Orji, 2018, p. 123). The continental free trade area provides an excellent opportunity for African society to achieve this by boosting the political will of governments to adopt the Malabo Convention. Otherwise, cybercrimes will continue to be a challenge to trade and economic activities in the African continental free trade area and this will hinder its ability to achieve its full potential.

A. Recommendations

African states will not at any given time have equal capacity in terms of legal facilities in combating cybercrime. There is

a need for an effective and adequate international cooperation regime with the capacity to enable any African state with the requisite facilities to prosecute cybercrimes at material times. This paper states that an operational regional instrument with provisions for effective and adequate international cooperation can fill this need. This can be achieved by using the AfCFTA agreements to address issues of cybercrime and cyber security. It recommends that efforts to get the Malabo Convention up and running should be a priority for the continent at this time and where possible, an additional protocol to it should be negotiated to provide for enhanced international cooperation including instant cooperation as the Second Additional Protocol to the Budapest Convention does. This additional protocol should also address the challenges presented by the requirement of double criminality and ways of surmounting it. The provisions under the Budapest Convention for international cooperation should be considered a model in this regard.

The above recommendation is anchored on the fact that Article 8(3) of AfCFTA makes provision for additional protocols to address concerns of businesses and trade. This creates an opportunity to consider annexing the Malabo Convention to the AfCFTA as it addresses critical areas of concern for trade and commerce in a digital era. In addition, the African Union should formally set up a regional monitoring and or working committee to address obstacles to the operationalization of the Malabo Convention. Such a committee could consider ways of providing incentives for states to become signatories to the Malabo Convention.

V. CONCLUSION

Transnational cybercrimes occur across several jurisdictions and the continuous advancement in technology makes cybercrimes effortlessly transnational, but the majority of the laws and policies established to combat cybercrimes in the African re-

gion are largely territorial. Additionally, the presence of safe havens makes it nearly impossible to meet the requirement of double criminality, which is a feature of most MLATs on the subject.

With the entire continent becoming a free trade area, safe havens for TNCCs must be eliminated to reduce the vulnerability in e-commerce and digital marketing. This is because crime follows opportunity; the increase in trade in the free trade area will be an opportunity for cybercriminals to up their games. There is a need to address cyber security and deter cybercrime by creating a cyber security regime for the continent. At present, the only regional instrument in this regard, the Malabo Convention, has not attained the force of law. Efforts to get the Malabo Convention up and running should be a priority for the continent at this time.

Where possible, an additional protocol should be negotiated to provide for enhanced international cooperation including instant cooperation. Additional protocols to the AfCFTA addressing various concerns of business and trade could still be adopted. The Malabo Convention could also be linked to the AfCFTA to reinforce the protection of trade and commerce in a digital era. Further research can be geared towards streamlining the recommended negotiation in order to have a fully-fledged regional policy against cybercrime.

REFERENCES

African Pulse, (2021) *Covid-19 and the Future of Work in Africa: Emerging Trends in Digital Technology Adoption*. Washington, World Bank Group.

African Union (2021), 'Protocols to the AfCFTA Agreement' <https://afcfta.au.int/en/protocols-afcfta-agreement> accessed March 20, 2022.

African Union, 'Agreement Establishing the African Continental Free Trade Area' https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area> accessed March 21, 2022.

African Union, (2020) 'List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection.' African Union, 18 June 2020 <https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf >accessed 17 March 2022.

African Union, (2021) '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.

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

Aper Review. (2021) 'Cyberattacks and Breaches to Cybersecurity' 21 *Asper Review of International Business and Trade Law*, 7.

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

Bannon, A. (2007) 'Cybercrime Investigation and Prosecution- Should Ireland Ratify the Cybercrime Convention?' 3 *Galway Student Law Review* 116.

Brown, A. (2021) 'Establishing an Integrated Judiciary to Facilitate the African Continental Free Trade Area.' 30(2) *Minnesota Journal of International Law*, 291.

Brown, S. D. Cameron. (2015) 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice' 9(1) *International Journal of Cyber Criminology*, 55.

Brownlie, I. (1998) *Principles of Public International Law*. United Kingdom, Oxford University Press.

Cangemi, D. (2004) 'Procedural law Provisions of the Council of Europe Convention on Cybercrime' 18(2) *International Review of Law, Computers & Technology* 165.

Chawki, M. 'A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy' (Computer Crime Research Centre) <www.crime-research.org/article/Critical/> accessed June 21,

2018.

Clough, J. (2014) 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization' 40 *Monash University Law Review* 698.

Clough, J. (2015). *Principles of Cybercrime.* United Kingdom, Cambridge University Press.

Coetzer, J. (2020) '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-an-cybercrime-laws-has-created-deep-vulnerabilities-but-is-change-on-the-way/?slreturn =2020> accessed 17 October 2021.

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

Daghar, M. (2020) 'Cybercrime: Is Kenya the New Playground for Cyber Criminals?' (04 February 2020), <https//www.enactafrica.org/research> accessed 18 October 2021.

Daigle, B. (2021) 'Data Protection Laws in Africa: Pan-African Survey and Noted Trends.' *Journal of International Commerce & Economics*, 1.

Enabulele, A. and Bazuaye, B. (2014) *Teachings on Basic Topics in Public International law*, Benin City, Ambik Press.

Enabulele, A. and Bazuaye, B. (2019) *Basic Topics in Public International law*. Lagos, Malthouse Law Books.

Fassassi M. and Akoussan C. F. (2016) 'Cybercrime in Africa: Facts and Figures' The Trust Project, July 7, 2016, < https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/> Accessed March 17, 2022.

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

Hait, A. A. (2014) 'Jurisdiction in Cybercrimes: A Comparative Study' 22 *Journal of Law, Policy and Globalization* 78.

Interpol, (2020) '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.

Jones, A. and Doobay, A. (2014). *Jones on Extradition and Mutual Assistance*. London, Sweet and Maxwell.

Kigeri, Alex. (2012) 'Routine Activity Theory and the Determinants of High Cybercrime Countries' 30 *Social Science Computer Review*, 470.

Kshetri, N. (2019) 'Cybercrime and Cyber security in Africa' 22(2) *Journal of Global Information Technology Management* 77.

Ladan, M. T. (2015) *Cyberlaw and Policy on Information and Communications Technology in Nigeria and ECOWAS*, (Zaria, Ahmadu Bello University

Press, 2015).

Lucchetti, M. (2018) '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.

Luppicini Rocci, (2014) 'Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research" Global Media Journal 7, no.1 (2014): 35.

Maurushat, A. (2010) 'Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools?' 33(2) *University of New South Wale Law Journal* 472.

Mihai, I. (2016) 'Romanian Legislation on Cybercrime.' 5(2) International Journal of Information Security and Cybercrime 25-30 (Ioan-Cosmin Mihai).

Murphy, S. S. (2002) *United States Practice in International law*, United Kingdom, Cambridge University Press.

Murungu, C. and Biegon, J. (2011). *Prosecuting International Crimes in Africa* Pretoria, Pretoria University Law Press.

Nabe, Cedric. (2022) 'Impact of Covid-19 on Cybersecurity' <https//www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity/> accessed 4 June 2022.

O'Keefe, R. (2004) 'Universal Jurisdiction: Clarifying the Basic Concept' 2 *Journal of International Criminal Justice,* 735.

Öner, M. Z. (2016) 'The Principle of 'Universal Jurisdiction' in International Criminal Law' 7(12) *Law and Justice Review* 177.

Orji, U. J. (2018) 'The African Union Convention on Cybersecurity: A Regional Response towards Cyber Stability,' 12(2) Masaryk University Journal of Law and Technology 91.

Riekkinen, J. (2016) 'Evidence of Cybercrime and Coercive Measures in Finland.' 13 *Digital Evidence and Electronic Signature Law Review*, 49.

Rohalska, V. O. & Buciunas, G. (2022) 'Extradition in the Criminal Procedural Legislation of Ukraine: Compliance with the European Standards.'8(1) *Journal of Liberty and International Affairs* 138.

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

Seger, A. (2012) 'The Budapest Convention on Cybercrime 10 Years on: Lessons Learnt or the Web is a Web' (International Conference on Cybercrime: Global Phenomenon and its Challenge 2-6 February 2012), <https://rm.coe.int/16802fa3e0 > accessed November 21, 2022.

Shaw, M. N. (2016) International Law. United Kingdom, Cambridge University Press.

Signe L. and Signe K. (2018) 'Global cybercrimes and weak cybersecurity threaten businesses in Africa' Brookings, Wednesday May 30, 2018,

https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cyber-crimes-and-weak-cybersecurity-threaten-businesses-in-africa/ accessed March 17, 2022.

Soma T. John, Muther F. Thomas and Brissette M. I. Heidi, (1997) 'Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?' 34 *Harvard Journal on Legislation* 317.

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

Thomas, D. (2022) 'What you need to know about the African Continental Free Trade Area.' (Business Africa, 10 February 2022, < https://african.business/2022/02/trade-investment/what-you-need-to-know-about-the-african-continental-free-trade-area/> accessed March 21, 2022.

Turianskyi, Yarik, (2020) 'Africa and Europe: Cyber Governance Lessons' 77 *South African Institute of International Affairs, Policy Insights* 8.

Udombana, N. J. (2020) 'Step Closer: Economic Integration and the African Continental Free Trade Area' 31(1) *Duke Journal of Comparative and International Law*, 1.

United Nations Office on Drugs and Crime, (2013) 'Comprehensive Study on Cybercrime: Draft–February2013'<unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_ 2013/CYBERCRIME_STUDY_210213.pdf> accessed 18 May 2019.

Wang, F. F. (2020) 'Legislative Developments in Cybersecurity in the EU.' *Amicus Curiae*, 233.

Weber, M. A. (2003) 'The Council of Europe's Convention on Cybercrime' 18 *Berkeley Technology Law Journal*, 425.

Yilma, K. (2016). Some Remarks on Ethiopia's New Cybercrime Legislation. 10(2) *Mizan Law Review*, 448.