Article

The Need for Harmonised and Specialised Global Legislation to Address the Growing Spectre of Cybercrime

Rapuluchukwu Ernest Nduka
https://orcid.org/0000-0002-8617-1833
J. R. Nduka and Co.
Nnamdi Azikiwe University, Nigeria
bishopraps@gmail.com

Vinesh Basdeo
https://orcid.org/0000-0002-5149-7198
University of South Africa

Abstract

Modern advances in technology have made the world a global village, and the impact of this on almost all spheres of life and society is phenomenal. The rapid growth of information and virtual technology in most spheres of life and society as well as the interconnection of computers through super highways and international computer networks have made cybercrime more diverse, more dangerous, more global and more challenging to fight. The ubiquity of the internet and the connectivity of virtually every computer to the global community hold ramifications that have yet to be determined. Cybercrime does not require physical proximity between the victim and the perpetrator for the commission of the offence. Cybercrime is unbounded, in that the victim and the perpetrator can be in different cities, states, or even countries. Deterring and punishing cybercriminals require an international legal framework to investigate and prosecute cybercrime.

Keywords: Cybercrime; criminal justice; comparative analysis; legislative framework

UNISA university of south africa PRESS
Southern African Public Law
https://unisapressjournals.co.za/index.php/SAPL
#8112 | 22 pages

https://doi.org/10.25159/2522-6800/8112
ISSN 2522-6800 (Online), 2219-6412 (Print)

Introduction*

Academics and practitioners lament the fact that the criminal justice field is simply not keeping pace with crime in the computing context.[1] The threat posed by the prevalence of cybercrime is felt not only by developed countries but equally by developing countries. The global nature of cybercrime dictates that any legislative intervention adopted to tackle cybercrime should be a global initiative requiring global co-operation.[2] Many legal scholars have advocated for a globally harmonised cybercrime legislative framework which should be driven by an international legal entity such as the United Nations.[3] Unfortunately, evolving a regional or national cybercrime legislative framework has been easier than creating an international harmonised one. For instance, in 2010 a proposal for the emergence of a global cybercrime treaty was rejected by the United Nations when there was disagreement between Russia, China and a few developing countries, on the one hand, and the United States, United Kingdom, Canada and the European Union on the other.[4]

This article observes that the apparent divergence in the various existing cybercrime taxonomies and legislative frameworks contribute to the growing menace of cybercrime. This article also posits that reliance on national or regional legislative initiatives to tackle a global threat is inadequate and only a global legislative framework will adequately address the impact of cybercrime. Further, this article highlights differences in cybercrime taxonomies and legislation between countries and identifies the inherent disadvantages these differences pose in forming a unified front by various countries in the fight against cybercrime. This article proposes the use of a common taxonomy to address the issue of cybercrime and it also focuses on the need for harmonised cybercrime legislation. It analyses various steps already taken by international and regional bodies to create a harmonised cybercrime treaty and the attendant failures. Finally, this article concludes with a proposal for a harmonised legislative framework and proffers necessary steps that will lead to the proposal coming to fruition.

* Part of this article is based on the LLD thesis submitted by Rapuluchukwu Ernest Nduka in completion of his LLD thesis at the University of South Africa. The authors are grateful for the assistance provided by the National Research Foundation in the completion of this article.

1 Robert Moore, *Search and Seizure of Digital Evidence* (LFB New York 2005) 1.

2 Brian Harley, 'A Global Convention on Cybercrime?' (2010) 1(3) Columbia University LJ <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/> accessed 14 December 2019.

3 Xiang Li, 'International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene' (2007) 4(3) Webology <http://www.webology.org/2007/v4n3/a45.html> accessed14 December 2019.

4 Greg Masters, 'Global Cybercrime Treaty Rejected at UN' (*SC Magazine*, 2013) <http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/> accessed 14 December 2019.

Varying Definitions and Approaches to Cybercrime

The clearly different interpretations and definitions of the nature and classification of what amounts to information technology crime[5] have led to a wide range of divergent classifications and a cacophony of answers to the attendant menace of cybercrime. Because of the varying taxonomies, an activity that will amount to cybercrime will be dependent on the classification it falls under, and this varies across jurisdictional precincts. Jurisdictional boundaries therefore, will determine cyber activities that would amount to criminal activities. For example, the Australian High-Tech Crime Centre classified electronic crime under two categories, namely computer-enabled crime and computer-enhanced crime.[6] Carter classifies cybercrime as a computer as target; a computer as instrumentality; a computer as incidental to other crimes; and crime connected with the prevalence of a computer.[7] Parker classifies high-tech crime as an activity where the computer is the object of the crime, or the computer is the subject of the crime, or the computer is used as a tool for executing or planning the crime, or where the computer can be used to deceive or intimidate.[8] The United States Department of Justice classifies cybercrime as a criminal activity in which the computer is the target of the activity or in which the computer is used as a weapon in committing an offence or in which the computer is an accessory.[9]

Having a consistent approach is essential in fighting cybercrime as it will enhance crime reporting, collaborative co-operation among agencies, knowledge sharing and ease communication between law enforcement agencies.[10] It will also enhance consistent interpretation and consistent best practices among law enforcement agencies, irrespective of jurisdictional boundaries or constraints since the consistent classification will highlight similar characteristics.[11] This will enable agencies to manage the impact of cybercrime across jurisdictions in order to take appropriate steps to tackle the crime.

The absence of a common definition and approach will hamper knowledge sharing and crime reporting on the extent of cybercrime and it will endanger international co-operation in addressing the menace of cybercrime. For instance, Broadhurst has pointed out that in many jurisdictions where cybercrime is reported law enforcement agencies are unable to differentiate cybercrime from other fraud reports, commercial crimes,

5 Information technology crime and cybercrime are used interchangeably.

6 Ali Alkabaai, George Mohay, Adrian McCullagh and Nicholas Chantler, 'Dealing with the Problem of Cybercrime' (2010 International Conference on Digital Forensics and Cybercrime) <http://www.afp.gov.au/~/media/afp/pdf/f/fighting-the-invisible.ashx> accessed 14 December 2019.

7 Evan Axelrod, *Violence Goes to the Internet: Avoiding the Snare of the Net* (Charles C Thomas Publishers Springfield 2009) 5–16.

8 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Elsevier Waltham 2011) 35–48.

9 ibid.

10 Alkabaai and others (n 6).

11 Martin Maidment, 'Taxonomies in the Public Sector' (2012) <http://www.nglis.org.uk/tips/tipsben.htm> accessed 14 July 2019.

criminal damage statistics or other categories of criminal offences thus making the extent of information technology crime uncertain.[12]

The mode of classification that several researchers and agencies rely upon to classify cybercrime is dependent on certain factors as perceived by the researcher or the agency proposing the classification.[13] For instance, the mode of classification may be dependent on the role of the computer system in the commission of the crime, or on the perpetrators of the offence. Thus, when the definition is perceived from the role the computer system played in the commission of the crime, cybercrime can then be classified as computer-enabled crime and computer-enhanced crime, or as crimes perpetrated using computers and traditional crimes facilitated by means of computers.

On the other hand, a proponent may classify cybercrime in terms of the threat such offence poses. In that case, cybercrime may then be classified as a computer infrastructure attack and computer-assisted threat.[14] It is submitted that the mode of classifying cybercrime should be based on the role of the computer system in the commission of the offence. This classification should be coined in a broad sense to accommodate all forms of cybercrime plaguing various jurisdictions that are currently in existence, and to accommodate new genres of crime that may be created in future. This will alleviate the need for reclassification upon the emergence of new offences. It is submitted that based on the benefits of establishing a common approach, cybercrime should be classified broadly into two categories based on the role of the computer system or the role the network plays in the commission of the cyber-criminal activity (computer-enabled crime), or where the computer is the tool in the commission, and where the computer is the target of the offence.

A Harmonised Cybercrime Legislative Framework

In addressing the divergent national cybercrime legislative frameworks, it is prudent that a country's interest in criminalising certain cyber-criminal activities should not be for the protection of its citizens or individuals within its national borders alone, since cyber-criminal activities are not confined to national boundaries.[15] Cybercriminals

12 Roderic Broadhurst, 'Developments in the Global Law Enforcement of Cyber-crime' (2006) International Journal of Police Strategies and Management 408–433.

13 Maidment (n 11).

14 This is the classification posited by the G8 Summit. See <http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-6.html> accessed 18 December 2019.

15 Susan Brenner and Marc Goodman, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3(1) Intl J of L and Technology <http://www.isrcl.org/Papers/Brenner.pdf> accessed 14 July 2019. A major problem is that electronic evidence is often not located in the territory of the investigating criminal justice authority. Data are increasingly stored, mirrored, or fragmented or moving between servers somewhere in the cloud, in possibly multiple or unknown jurisdictions, while criminal justice authorities are normally limited by the principle of territoriality. Even if data are stored in the territory of an investigating authority and a server or device could be lawfully searched and seized, this will not be enough if the natural or legal person in possession or control of

exploit the opportunities in the divergent national legislative frameworks to perpetuate their nefarious activities, and in some cases law-abiding citizens may be obeying their national laws but violating the laws of another country because of the divergent legislative frameworks.

The nature of cybercrime which erodes the principles of sovereignty and jurisdiction makes transnational consistency imperative in order to address the menace of cybercrime. According to Brenner et al, one way of achieving this consistency is by creating a single code of legislation that would govern the commission of cybercriminal activity anywhere in the world.[16] This single piece of legislation will have to be agreed upon by the various national authorities.[17] Brenner et al also suggest the creation of a set of regulatory codes or laws that adequately covers all facets of high-tech crime which countries can adopt in enacting its cybercrime legislation.[18] Broadhurst further maintains that having legislative consensus is the best strategy for the suppression of cybercrime, but also points out that achieving a strict enforcement agenda is not feasible.[19]

It is submitted that a harmonised cybercrime legislative framework is imperative in addressing the menace of information technology crime. This legislative framework can simply be ratified by nations, or where a country already has its national legislative framework in place, the country will be obliged to update its legislation to be in alignment with the global harmonised legislative framework. A harmonised global legislative framework will address inconsistencies in the criminalisation of offensive conduct and will eliminate the emergence of safe havens.[20] For instance, where conduct is criminalised in a certain jurisdiction and the same conduct is not criminalised in another jurisdiction, the second jurisdiction becomes a lucrative haven for offenders who perpetrate such activities. These safe havens will frustrate the efforts of law enforcement agencies since the ubiquitous nature of the internet still makes them susceptible to the criminal activities of offenders who are protected by the laxity of the legal framework in the 'safe haven'.

---

the data, that is, the person with the keys to the data is elsewhere. The question, therefore, is how electronic evidence can be secured lawfully and effectively for criminal justice purposes while meeting human rights and rule of law requirements and respecting the principles of State sovereignty. Hence, the need for harmonised and specialised international legislation.

16 ibid.

17 ibid.

18 ibid.

19 Broadhurst (n 12) 408–433.

20 Lewis C Bande, 'The Making of Cybercrime Legislation in Malawi: A Comparative Analysis of Malawi's Proposed Cybercrime Law Against International Standards and Best Practices' (2018) 12(1) Intl J of Cyber Criminology <https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf> accessed 12 September 2019.

Uniformity in the legislative framework enhances the co-operation of varying jurisdictions in tackling crime, since the principles of reciprocity and double criminality are the main pivots driving international co-operation in criminal jurisprudence and extradition of offenders.[21] The ubiquitous nature of the internet dictates that a harmonised global cybercrime legislative framework is essential to ensure international co-operation in addressing the menace of cybercrime and is a veritable step that must be taken if the growth and attendant problems associated with cybercrime are to be addressed. The initiatives embarked upon by several countries in enacting and updating their national legislation on cybercrime have yielded positive results. For example, the United States Department of Justice reports that between the years 2006 and 2010, approximately 1,177 persons were convicted and sentenced for various cyber-criminal activities.[22] In South Africa, the Deputy Minister of Justice reported that a success rate of 97.6 per cent in cybercrime prosecutions has been achieved,[23] and the Economic and Financial Crimes Commission of Nigeria reported that it had recovered over USD170 million, intercepted over 12,000 scam e-mails, and secured over 300 convictions.[24]

However, approaching cybercrime from a limited jurisdictional perspective and the inconsistencies in the legislation of different countries have been a barrier to effectively tackling cybercrime. The desired zenith has not been attained. For instance, a study conducted by Norton reveals that in 2012, 1.5 million persons were victims of cybercrime resulting in a cost of about USD110 billion over a period of twelve months.[25] This has increased to about 700 million victims while the cost is projected to get to USD6 trillion by 2021,[26] thus implying that existing global efforts have not yet yielded desired results. Several countries, regional bodies and international agencies have taken various steps to provide a unified or consistent cybercrime legislative approach to address the gaps created by the inconsistencies in cybercrime legislation within their sphere of influence. Some of the measures adopted towards achieving a harmonised legislative cybercrime approach by certain international and regional bodies are examined below.

21 ibid.

22 Catherine Marcum, George Higgins and Richard Tewksbury, 'Doing Time for Cyber Crime: An Examination of the Correlates of Sentence Length in the United States' (2011) 2(1) Intl J of Cyber Criminology 824–835.

23 John Rademeyer, 'Conviction Rates An Unreliable Benchmark of NPA Success' (12 April 2013) <http://africacheck.org/reports/conviction-rates-an-unreliable-benchmark-of-npa-success/> accessed 29 December 2019.

24 Nir Kshetri, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies' in *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan Hampshire 2013) 152–170.

25 David Goldstein, 'Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually' (5 September 2012) <http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02> accessed 29 December 2019.

26 Aimee O'Driscoll, '100+ Terrifying Cybercrime and Cybersecurity Statistics and Trends' (Comparitech 2018) <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref> accessed 29 September 2019.

United Nations

The United Nations, as the international body entrusted with the responsibility of engendering the promotion of global peace has taken several steps in advocating various strategies to create harmonised cybercrime legislative instruments. The United Nations General Assembly has come up with a number of resolutions to initiate the enactment of consistent cybercrime legislations across member states.[27] For instance, in 1985 the United Nations passed Resolution 40/71 requesting governments and international organisations to 'take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade.'[28] The United Nations Commission on International Trade Law (UNCITRAL) further requested governments to take steps to review their legal rules in relation to the use of computer records as evidence during trials and to ensure such rules are consistent with current technological trends.[29] Resolution 55/63 of the United Nations General Assembly stipulated that the laws and practice of member states should be modelled to eliminate safe havens for cybercriminals; law enforcement agencies should cooperate in their investigation and prosecution of cyber-criminal activities, and member states' legal systems should be modelled to 'protect the confidentiality, integrity, and availability of data and computer systems from unauthorised impairment.'[30] The Resolution also requires states to protect individual freedom and privacy, and make individuals aware of the need to prevent and fight cybercrime while mandating governments to increase its capacity to combat cybercrime.[31]

In a bid to engender some level of legislative consistency, Resolution 56/121 further encourages member states to consider the work and policies of other international or regional organisations when developing its national laws, policies and practices that will address cybercrime.[32] Several UN institutions such as the International Telecommunication Union (ITU) and United Nations Office on Drugs and Crime

27 The Resolutions of the United Nations General Assembly are not legally binding on member states, although they can lead to legally-binding conventions and treaties. See also <http://www.un.org/cyberschoolbus/untour/subgen.htm> accessed 21 September 2019.

28 Dean Lewis, *The Interpretation and Uniformity of the UNCITRAL Model Law* (Kluwer Law International 2016) <http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf> accessed 21 August 2019. See also 'United Nations Commission on International Trade Law Yearbook: 1985 Vol XVI' (United Nations Publication 1988) 47.

29 ibid.

30 Resolution 55/63 of 4 December 2000 on Combating the Criminal Misuse of Information Technologies. See also <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf> accessed 21 August 2019.

31 Resolution 55/63 of 4 December 2000 on Combating the Criminal Misuse of Information Technologies. See also <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf> accessed 21 August 2019.

32 Resolution 56/121 of 19 December 2001 on Combating the Criminal Misuse of Information Technologies. See also <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf> accessed 21 August 2019.

(UNODC) have also taken certain initiatives towards propelling the harmonisation of cybercrime legislations among UN member states. The ITU brought together a High-Level Experts Group (HLEG) upon the launch of the Global Cybersecurity Agenda (GCA), to provide a platform that will create a framework for global discourse and cooperation aimed at proposing strategies that will enhance security in cyberspace.[33] The central strategy and plan of the GCA as it relates to legislative measures embarked upon by member states, are the amplification of strategies for the creation and growth of a harmonised model of cybercrime legislation that is globally applicable.[34] Various proposals have therefore been made to the ITU as a template for a model harmonised cybercrime legislation that should be adopted by the UN as part of the panacea to tackling the lacunae created by divergent national or regional legislations. For instance, Schjolberg[35] and Ghernaouti-Helie proposed a global treaty on cybersecurity and cybercrime.[36]

The Asia-Pacific Economic Cooperation

The Asia-Pacific Economic Cooperation (APEC) is made up of 21 inter-governmental bodies of the Asia-Pacific region.[37] The body has taken steps to compel member-economies to adopt adequate legislative measures to address the menace of cybercrime in the member states' jurisdiction and the Asia-Pacific region. In addition, it has taken steps to create a harmonised cybercrime legislative framework in the region. The focus of APEC originally revolved around the promotion of economic growth and trade, and thereafter also moved on to issues affecting cross-border police cooperation.[38] In line with technological developments, APEC has also focused on other areas relevant to cybercrime enforcement.[39] For instance, in 2001, the Telecommunications and Information Working Group of APEC requested the co-operation of member-states in

33 Stein Schjolberg and Solange Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime* (Black Swan 2011) <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf> accessed 21 August 2019.

34 Stein Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation–The Road to Geneva' <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf> accessed 21 August 2019.

35 Stein Schjolberg was the Chairperson of the High-Level Experts Group (HLEG) for ITU's Global Cybersecurity Agenda (GCA). See <http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/foreword_chair.html> accessed21 August 2019.

36 Schjolberg and Ghernaouti-Helie (n 33). The draft code requires member states to criminalise certain cyber activities such as illegal access; illegal interception; data interference; system interference; misuse of information technology devices; computer-related forgery; computer-related fraud; identity theft; offences relating to child pornography massive and coordinated cyber-attacks against critical communications and information infrastructures; terrorism and serious cyber-attacks; and preparatory acts that will enable the commission of an offence.

37 ibid.

38 Broadhurst (n 12) 433.

39 ibid.

providing adequate security from cyber attacks, and to share information with respect to member states. Another notable step by APEC, in facilitating the harmonisation of cybercrime legislation among member economies, was the institution of the Cybercrime Legislation and Enforcement Capacity Building Conference of Experts and Training seminar, which was aimed at promoting the growth of comprehensive legal frameworks among member economies, providing assistance in the development of law enforcement e-crime units, and improving the cooperation between the industry and law enforcement units in combating cybercrime.[40]

The Council of Europe

The Council of Europe (CoE) as a regional body has taken various initiatives in addressing the threat of cybercrime commencing with the Council of Europe Conference on Criminological Aspects of Economic Crime which took place in Strasbourg in 1976.[41] In an effort to create harmony among national legislative frameworks, the CoE selected a team of experts to look into the legal issues involving computer-related crime, and this resulted in the emergence of guidelines for national legislatures to adopt.[42] The recommendations which outlined substantive cyber offences were non-binding on member states and therefore had a limited ability to create a harmonised legislative framework across member states.[43] Driven by the need to create a more harmonised legislative initiative which will enhance the ability of law enforcement agencies to effectively address the growing threat of cybercrime, the CoE created a more binding treaty and opened it for signatures of both member states and non-member states.[44] As at September 2019, sixty-five countries are signatories to the Convention and sixty-one countries have ratified the Convention, while four countries have signed but not ratified the Convention.[45] The Convention clearly specified certain conduct that national legislative initiatives should proscribe. These include offences

40 Jody Westby, *International Guide to Cyber Security* (American Bar Association 2005) 35–102.

41 At the conference, categories of computer crime were introduced. See Schjolberg (n 33).

42 The guidelines were presented in the Recommendation of 1989. The Recommendation stipulated the minimum list of offences that should be criminalised by various national legislatures, namely unauthorised access; unauthorised interception; computer fraud; computer forgery; damage to computer data; computer sabotage; unauthorised reproduction of a protected computer programme; and unauthorised reproduction of a topography. See Stein Schjolberg and Amanda Hubbard, 'Harmonizing National Legal Approaches on Cybercrime' <http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf> accessed 3 September 2019.

43 Schjolberg and Hubbard (n 42).

44 The Council of Europe Convention on Cybercrime (adopted 23 November 2001) 2001 ETS 185 was opened for signature in 2001 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> accessed 3 September 2019.

45 ibid.

against the confidentiality, integrity and availability of computer data;[46] computer-related offences;[47] content-related offences;[48] and offences related to infringements of copyright and related rights.[49] The CoE, in line with the growing acts of racism and xenophobic tendencies perpetrated and targeted on individuals with the aid of the computer system, adopted measures to address such acts through the drafting of an additional protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[50] The Convention makes adequate provision for the establishment of harmonised procedural rules by adopting conventional measures such as search and seizure, and creating new measures, such as real-time collection of data, interception of data and expedited preservation of data, to enable the effective investigation and prosecution of IT crime.[51]

Broadhurst points out that the Convention includes strong procedural guarantees and, except in cases of official criminal investigations, the Convention does not validate the surveillance of private communications by either service providers or law enforcement agencies.[52]

The Convention also addresses the issue of jurisdiction by establishing the criteria upon which parties to the Convention can assume jurisdiction over the criminal offences stipulated in the Convention. Parties can assume jurisdiction where the offence was committed within 'its territory; or on board a ship flying the flag of that state party, or on board an aircraft registered under the laws of that state party, or by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state.'[53]

The Convention also requires international cooperation and mutual assistance among parties, and requires states to consult with a view of determining the most appropriate

46 Article 2 proscribes illegal access of a computer system; Article 3 proscribes the illegal interception of data to and from a computer system; Article 4 proscribes data interference; Article 5 proscribes system interference while Article 6 proscribes the misuse of computer-related devices including the production, sale, procurement for use, import or distribution or otherwise making available of such device. See also Broadhurst (n 12) 429. See also The Council of Europe Convention on Cybercrime (adopted 23 November 2001) 2001 ETS 185 (Convention on Cybercrime).

47 The traditional crimes of computer-related forgery and computer-related fraud fall under this category. See Articles 7 and 8 of the Convention on Cybercrime (n 44).

48 Child pornography falls in this category of offences and it also criminalises the procurement, possession or distribution of child pornography. See Article 9 of the Convention on Cybercrime (n 44).

49 Article 10 of the Convention on Cybercrime (n 44) makes it an offence to willfully infringe on a commercial scale the copyrights or related rights when such infringement was done by means of a computer system.

50 Additional Protocol to the Convention on Cybercrime concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems 2006 ETS 189.

51 Broadhurst (n 12) 429. See also Articles 16–21 Convention on Cybercrime (n 44).

52 Broadhurst (n 12) 429.

53 Article 22 of Convention on Cybercrime (n 44).

jurisdiction where more than one party can assume jurisdiction over an offence.[54] The Convention, in its effort to create harmony in addressing cybercrime, established the legal basis for an international computer crime assistance network. This requires states to designate contact points that are available 24 hours daily to ensure immediate assistance when a cyber criminal activity takes place.[55] Although regarded as the most significant international cybercrime agreement the Convention has certain flaws which contribute to its inability to translate into an instrument accepted by all nations. One such flaw is that the Convention is a regional binding agreement which in its scope of operation is limited to parties to the Convention that have ratified the Convention. Thus, the Convention is not a global agreement. The Convention has been ratified by 61 countries and even at regional level not all CoE members such as Russia are signatories to the Convention.

Another flaw is that there are several reservations on the human rights implications of the enforcement of the Cybercrime Convention among parties. For instance, according to the Electronic Privacy Information Centre, the Convention infringes upon an individual's right to privacy and lacks a 'dual criminality provision'[56] which would enable a foreign law enforcement agency to investigate an activity which, although legal in the United States is a crime in the investigating state, and the United States will be compelled to cooperate with that state.[57]

Most civil liberty organisations also objected to the Convention stating that the requirement for the retention of data on customer activities by internet service providers was a derogation on the privacy rights of citizens and encourages improper monitoring of private communications.[58] They also pointed out that article 14 of the Convention, which sets out the conditions for the search and seizure of stored computer data, lacks essential procedural safeguards to protect the rights of the individual and to ensure due process of law since there is nothing to ensure that an independent judicial review takes place before the search and seizure.[59]

A further concern is that the Convention validates the transfer of personal data to countries without adequate data protection laws.[60] However, most of the concerns raised by various bodies, especially by the civil liberty organisations on the human rights

54 ibid.

55 This 24/7 point of contact network would enable states to respond more appropriately to the law enforcement challenges posed by information technology crime. See Broadhurst (n 12) 424. See also Article 35 of the Convention on Cybercrime (n 44).

56 '*Dual criminality* requires that an accused be extradited only if the alleged criminal conduct is considered criminal under the laws of both the surrendering and requesting nations.' See Charles Doyle, *Extradition to and from the United States* (Nova Science Publishers 2008) 7.

57 Doyle (n 56) 9.

58 ibid.

59 ibid.

60 ibid.

implications of the Cybercrime Convention, have been debunked as unsubstantiated.[61] Certain scholars have stressed that individual human rights are properly protected by the provisions in the Convention and the existing national legal framework that guarantee the protection of human rights.[62] Certain other scholars have also identified other underlying reasons that contribute to the inability of the Convention on Cybercrime to translate into an instrument accepted and adopted by all nations.

Some leading world economies such as China, Russia and other authoritarian regimes drive policies that discourage transnational cooperation.[63] For instance, Russia opposes the Convention on the grounds that the Convention permits criminal investigations in a foreign jurisdiction without prior notice to the local authorities.[64] Most authoritarian countries take serious objection to any international initiative that may impinge on their sovereignty or meddle in their domestic affairs.[65] Any international cybercrime agreement that will engender the harmonisation of cybercrime legislations will require a high level of international cooperation which the policies of most authoritarian regimes do not encourage.[66]

It is also important to note that where major world powers take divergent positions on global issues, the likelihood of success of any effort to tackle such global issues will be very little. A further major impediment to the success and acceptance of the Convention is the fact that the negotiation and development of the Convention revolved around a few states and it did not receive wide coverage and consultation.[67] The Convention was drafted by a committee of experts on crime in cyber-space formed by the CoE with no input from most non-member states who were urged to become parties to the agreement.[68] This further diminishes the status of the Convention on Cybercrime from assuming global status to being a mere regional agreement.

Some scholars have posited that the appropriate approach will be the drafting of a more global treaty with greater international participation in its drafting.[69] As pointed out by Archick, countries that took part in the negotiations of the Cybercrime Convention are

61 Sara Marler, 'The Convention on Cybercrime: Should the United States Ratify?' (2002) New England LR 183–219.

62 Robert Lemos, 'International Cybercrime Treaty Finalized' (2002) <http://news.cnet.com/2100-1001-268894.html> accessed 28 September 2019.

63 ibid.

64 Keir Giles, 'Russia's Public Stance on Cyberspace Issues' in Czosseck C, Ottis R and Ziolkowski K (eds), Papers delivered at 4th International Conference on Cyber Space Conflict (5–8 June 2012, Tallinn, Estonia) 63–75.

65 ibid.

66 ibid.

67 Brian Harley, 'Crosswires: International Co-operation on Cyber Security' The Columbia Science and Technology Law Review blog (23 March 2010) <http://stlr.org/2010/03/> accessed 28 September 2019.

68 The United States, Canada and South Africa were the only non-CoE nations that at some stage participated in the drafting of the Convention.

69 Harley (n 67).

not the 'problem countries' that provide a safe haven for cybercriminals, but rather the countries that are already fighting cybercrime and have some measure of existing legislative framework to tackle the issue of cybercrime.[70] These safe havens are exploited by the perpetrators of cybercrime in routing their nefarious activities which do not criminalise their activity, thereby relying on the principle of jurisdiction as a shield from the law.[71]

Despite the criticisms levelled against the Convention on Cybercrime, it remains the leading treaty that can be used to engender harmonisation of national legislative initiatives on cybercrime. Unfortunately, this regional effort which seeks to propel the harmonisation of various national cybercrime laws has not attained the success anticipated by its proponents and many nations are not taking the necessary steps to become party to and/or to ratify the said Convention. For instance, of all the African countries only South Africa, Mauritius, Morocco and Senegal have signed the treaty and only Mauritius, Morocco and Senegal have assented to it.[72] The inconsistencies in national cybercrime legislative frameworks are further exacerbated by the reluctance of many countries to be part of existing efforts by international bodies to create harmonised legislation, and this has greatly hampered efforts to properly address the menace of cybercrime. Because of the ubiquitous nature of the internet, the usefulness and impact of the Cybercrime Convention will be felt when more states accede to the Convention and enforce the provisions of the Convention.[73].

The African Union

The African Union (AU) is a regional body with the highest concentration of developing and underdeveloped countries as its members. A few of the nations within the AU have taken steps to enact cybercrime legislation. Of the fifty-four countries that make up the AU only a few countries[74] have enacted distinct national cybercrime laws.[75] A few other

70 Kristin Archick, 'Cybercrime: The Council of Europe Convention' (2006) <http://fpc.state.gov/documents/organization/58265.pdf> accessed 28 September 2019.

71 ibid.

72 ibid.

73 ibid.

74 These countries include South Africa, Kenya, Mauritius, Cameroon, Zambia, Uganda, Algeria, Namibia and Botswana. See Loucif Kharouni, 'Africa: A New Safe Harbour for Cybercriminals?' (2012) <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf> accessed 30 September 2019. See also Kizito Sikuka, 'Southern Africa: Region Cracks Down on Cyber Crime (2012) <http://allafrica.com/stories/201204120866.html> accessed 30 September 2019. See also Patrick Mwaita and Maureen Owor, 'Workshop Report on Effective Cybercrime Legislation in Eastern Africa' (2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf> accessed 30 September 2019.

75 Ruth Becker, 'How Many Countries in Africa? How Hard Can the Question Be?' (2012) <http://africacheck.org/reports/how-many-countries-in-africa-how-hard-can-the-question-be/> accessed 30 September 2019.

countries within the AU have drafted cybercrime bills which have been passed to its national assembly for consideration and eventual enactment as law.[76] Within the AU measures are being adopted by various regional blocs to propel members of such blocs to create some form of cybercrime legislation and to engender harmonisation of the bloc's member states' national cybercrime legislation. For instance, the Southern African Development Community (SADC)[77] has held several meetings and made recommendations geared towards engendering harmonised cybercrime legislation amongst its member states.[78] The member states with some form of cybercrime legislation are Botswana, Mauritius, South Africa and Zambia. The other eleven member states are either developing cybercrime legislation or have started national consultations on the matter.[79] The East African regional bloc[80] of the African continent is working on steps that will propel the emergence of a harmonised set of cybercrime laws within the bloc as a means of facilitating regional trade.[81] The AU, as a body in its attempt to propel the harmonisation of cybercrime legislation among its member states, drafted a Cybercrime Convention that will help to chart the course in addressing the menace of cybercrime in Africa.[82] However, it is submitted that in light of the fact that Africa is made up of a large number of developing and underdeveloped countries, has limited internet penetration, is plagued with poverty and has very limited existing national legislations on cybercrime, very few member states will embrace the draft AU Cybercrime Convention.

South Africa[83]

In South Africa, dedicated ICT legislation dealing with computer crime has been slow to appear.[84] The Electronic Communications and Transactions (ECT) Act is the first piece of legislation to address this area.[85] In South Africa, the criminal legislative

76 These countries include Tanzania and Angola. See Nir Kshetri, 'Cybercrime and Cybersecurity in Africa'(2019) 3 Journal of Global Information Technology Management 165–166.

77 The Southern African Development Community (SADC) is an inter-governmental body that seeks to promote the integration of economic development in countries in the Southern African region. Its member states include Angola, Botswana, the DRC, Lesotho, Madagascar, Malawi, Namibia, Mozambique, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. See 'History and Treaty SADC' (1992) <http://www.sadc.int/about-sadc/overview/history-and-treaty/> accessed 01 October 2019.

78 Kizito Sikuka, 'Southern Africa: Region Cracks Down on Cyber Crime' (2012) Cybercrime Electronic <http://allafrica.com/stories/201204120866.html> accessed 01 October 2019.

79 ibid.

80 The East African Community (EAC), an Intergovernmental Regional Organisation on the African continent, has five member states which include Burundi, Kenya, Rwanda, Tanzania, and Uganda.

81 Mark Okuttah, 'EAC Eyes Trade Growth with Cyber Laws'(2010) International Information and Library Review <http://www.businessdailyafrica.com/EAC-eyes-trade-growth-with-cyber-laws/-/539444/945130/-/xd5eh7z/-/index.html> accessed 2 October 2019.

82 ibid.

83 Dana Van der Merwe, *Information and Communications Technology Law* (Juta 2016) 51–52.

84 ibid.

85 Act 25 of 2002.

provisions in the ECT Act are currently the most important statutory countermeasures against cybercrime. These provisions are found in Chapter XIII of the ECT Act, entitled 'Cyber Crime', namely sections 85 to 89. Although the chapter title appears to be like another category of crime targeting computers in the 'cyber' world, closer scrutiny of the statutory crimes themselves makes it apparent that data are the real legal interest that stands to be protected. The first primary section of the ECT Act in this regard is section 86(1), which criminalises any unauthorised 'access to or interception of data'. It significantly adds a new prohibited action, namely 'interception of' to 'unlawful access' and 'modification'. Section 86(2) specifically prohibits any unlawful modification of data by outlawing 'interference with data' that would cause such data to be 'modified, destroyed or erased or otherwise rendered ineffective'. This section should be able to cover the creation and distribution of computer 'virus' programs, provided that, together with the other elements of a crime, the necessary causal link and *mens rea* can be proved. The last element will probably on many occasions take the form of *dolus eventualis*, together with *dolus generalis*. This type of recklessness is closer to intent (*dolus*) than to negligence (*culpa*). This is important in view of the fact that subsections (1) and (2) of section 86 specifically require that the prohibited actions be committed intentionally. Section 87 of the Act creates statutory and data-related versions of the common law crimes of extortion, fraud, and forgery. This raises the question already, namely whether these types of activities might not already be adequately covered by existing common-law crimes. It is difficult to gauge exactly what success the criminal provisions of the Act have had because there are yet no reported cases in which these provisions have been judicially interpreted. Academic opinion is not very copious. Collier,[86] for example, simply repeats the substantive provisions of Chapter XIII *verbatim* before criticising some of the procedural provisions.[87] Maat[88] is complimentary about the fact that the Act deals with the currency of 'data' instead of using the terms 'computer' or 'computer system': 'This is advantageous since the scope of the Act is not limited to a computer, especially in the light of the revolution in information technology.'

Concluding Remarks and Recommendations

Being comfortable with technology that underpins the Fourth Industrial Revolution ushering in the Information Age is non-negotiable for those who must investigate twenty-first century crimes and crime scenes.[89]An international legal framework is required to deter and to prosecute cybercrime. The criminal justice system cannot ignore the real world limits of local, state, national sovereignty and jurisdiction.

86 Debbie Collier, 'Criminal Law and the Internet' in Reinhardt Buys and Francis Cronje (eds), *Cyberlaw @ SA II: The law of the Internet in South Africa* (2nd edn, Van Schaik Pretoria 2004) 322–328.

87 This topic is dealt with in para 4.5 below.

88 Sandra Maat, 'Cyber Crime: A Comparative Law Analysis' (LLM thesis, Unisa 2004) 58.

89 Annamart Nieman, 'Search and Seizure, Production and Preservation of Electronic Evidence' (LLD thesis, North West University 2006).

The task of obtaining information from foreign countries, especially on an expedited basis, can be very challenging. This is particularly true when the other country is in a different time zone, uses a different language, has different legal rules, or does not have trained experts available.[90] Essentially, a harmonised and specialised international legal framework will entail the harmonisation and enactment of adequate domestic and transborder coercive procedural measures to facilitate effective international cooperation; harmonisation of the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of computer systems or evidence in relation to such offences in electronic form, and the setting up of a fast and effective regime for international cooperation. The international legal framework should supplement and not supplant existing multilateral and bilateral treaties and arrangements between countries.

Therefore, regarding general matters, the parties to the international legal framework should in principle apply such other existing treaties or arrangements. However, in respect of specific matters dealt with only by the international legal framework, the rule of interpretation *lex specialis dergat legi generali* provides that the parties should give precedence to the rules contained in the international legal framework. The international legal framework should require all parties to have a legal basis to carry out certain specific forms of cooperation if its treaties, laws and arrangements do not already contain such provisions. These specific minimum forms of cooperative measures are:

(i) expedited preservation of stored cyber data;

(ii) expedited disclosure of preserved cyber data;

(iii) accessing of stored cyber data;

(iv) transborder access to stored cyber data with consent or where publicly available;

(v) real-time collection of cyber data;

(vi) interception of cyber data; and

(vii) maintenance of a 24-hour, 7-day a week network.

The international legal framework should require parties to establish jurisdiction over criminal offences relating to cybercrime based on the following principles:

90 Albert Aldesco, 'Notes and Comments - The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime' 88–90 <htto:/Ielr.lls.edu/issues/v23-issue1/aldesco.odf> accessed 3 October 2019.

(i) territoriality, if the crimes are committed in its territory, and

(ii) nationality, by obliging the nationals of a member state to comply with its domestic law, even when they are outside its territory, and if the conduct is also an offence under the law of the state in which the offence is committed, or if the conduct has taken place outside the territorial jurisdiction of any state. These bases of jurisdiction are not exclusive and any other basis of jurisdiction in conformity with the domestic law of a member state are permitted.

The international legal framework should include the following conditions and safeguards[91]:

(i) It must generally be subject to the conditions and safeguards provided for under the domestic law of each party (including the right against self-incrimination, legal privileges and the specificity of individuals or places);

(ii) It must generally be subject to some common standards or minimum safeguards aimed at balancing the interests of law enforcement on the one hand, and respect for fundamental human rights on the other, arising pursuant to obligations undertaken by a party under applicable international human rights instruments (including the right of everyone to hold opinions without interference; the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers; and the right to privacy);

(iii) It must specifically be subject to (judicial or other independent) supervision by competent authorities, inter alia, to consider the grounds justifying the application of the mechanisms and the limitation on its scope and duration;

(iv) The mechanisms must specifically incorporate the principle of proportionality in accordance with the relevant principles of the domestic law of a party (such as reasonableness requirements for searches and seizures, limitations on overly broad search warrants and production orders and the limitation on coerced cooperation with the provision of information that is reasonably necessary to enable a search and seizure intervention);

(v) It must specifically bring into the equation, to the extent consistent with the public interest and, particularly, the sound administration of justice, the impact of the mechanisms upon the rights, responsibilities and legitimate interests of third parties, and the means to mitigate such an impact (including the means to minimise a disruption to consumer services, the protection of proprietary interests, protection from liability for disclosure, the engagement and financial compensation of witnesses and experts, and

91 See also Nieman (n 89).

notification of a surreptitious search and seizure intervention without prejudicing the investigation);

(vi) In respect of preservation and production mechanisms, parties must specifically introduce an additional obligation of confidentiality; and

(vii) In respect of production mechanisms, privileged data or information may specifically be excluded from the application of production orders.

It is imperative that international co-operation is provided among countries to the widest possible extent and that obstacles thereto such as reservations, postponements, and the imposition of conditions to the provision of assistance be strictly limited. An international transborder legal framework should meet the following requirements:

(i) It must (through the application of international instruments on international cooperation in criminal matters, arrangements agreed upon the basis of uniform or reciprocal legislation and domestic laws) enable criminal justice processes relating to cyber information located within its national territory, on behalf of another party;

(ii) It must enable an expedited criminal justice process for the benefit of another party, where there are grounds to believe that the relevant cyber information is particularly vulnerable to loss or modification, or otherwise where the relevant treaties, arrangements or laws provide for such expedited cooperation; and

(iii) It must allow for unilateral access through a computer system in a party's own territory to cyber information in the territory of another party (without that party's authorisation) if the required cyber information is an open source, or if a party has obtained the lawful and voluntary consent of a person authorised to disclose the cyber information.

It is clear that cybercrime is a growth industry internationally.[92] Precisely because of its international nature, such crimes create many political and jurisdictional problems and problems arising from the incompatibility of criminal and criminal-procedure codes. It is therefore of the greatest importance that countries, including South Africa ratify international documents such as the Convention on Cybercrime. Failing to do this will create 'crime shelters' similar to tax shelters' created by the legislation (or lack of it) in certain States.

This piece of international 'legislation'[93] is a major step forward in combatting international cybercrime. One of the major problems with cybercrime is precisely its international nature, which gives rise to problems of jurisdiction, incompatible procedural law systems and so forth. Although originating in Europe, the Convention is

92 Van der Merwe (n 83) 51–52.

93 The Council of Europe Convention on Cybercrime.

flexible enough to be adopted by any country and South Africa has, in fact, taken the first steps to do so. The first part of the Convention deals with substantive law measures.[94] Signatories are supposed to ensure that the following types of offences are prohibited nationally.[95]

- 'Offences against the confidentiality, integrity and availability of computer data and systems', which include the illegal interception of, or interference with data; the illegal access to, or interference with a computer system; and the misuse of devices, including making available a tool or password for the purpose of committing any of the above offences.[96]
- 'Computer-related offences', including computer-related forgery and computer-related fraud.[97]
- 'Content-related offences' relating to online child pornography in its various formats.[98]

Finally, treaty countries have to criminalise copyright-related offences. South Africa has complied with most of the substantive treaty obligations. Most of the offences referred to have been criminalised by sections 86 and 87 of the ECT Act,[99] others by the Films and Publications Act[100] and the South African Copyright Act.[101] The second part of the Convention deals with procedural law matters. Certain conditions and safeguards must be laid down for human rights to be protected adequately while the computer data necessary for possible prosecutions are obtained. These might include production orders for data controlled by any person or service provider within the territory concerned. Chapter 3 of the Convention deals specifically with international co-operation in the investigation and prosecution of criminal offences. This might involve extradition for trial to a member country, and includes an international point of contact staffed by trained operators 24 hours a day, 7 days a week.

As far as the second and third part of the Convention are concerned, South Africa has definitely not yet passed (or amended) the legislation necessary to ensure the country's

94 The Council of Europe Convention on Cybercrime (adopted 23 November 2001) 2001 ETS 185 was opened for signature in 2001 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> accessed 3 September 2019.

95 ibid.

96 ibid.

97 ibid.

98 ibid.

99 Electronic Communications and Transactions Act 25 of 2002.

100 Act 65 of 1996.

101 Act 98 of 1978. While on the subject of copyright offences, it is interesting to note that it was only as recently as 2004 that a piracy offender was sent to jail for the first time in South Africa. The Pretoria Commercial Crimes Court sent Craig Marnoch to jail for the maximum term of three years in terms of the Copyright Act. He had tricked hundreds of South Africans into purchasing pirated Microsoft software and pirated DVDs. See *Legalbrief* 4 December 2004.

compliance with its international obligations. Such steps might also have constitutional implications, but until something positive is done at the legislative level we may never find out.[102]

References

Aldesco A, 'Notes and Comments—The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime' (2012) <Ielr.lls.edu/issues/v23-issue1/>

Alkabaai A, Mohay G, McCullagh A and Chantler N, 'Dealing with the Problem of Cybercrime' (2010) International Conference on Digital Forensics and Cybercrime <https://doi.org/10.1007/978-3-642-19513-6_1>

Archick K, 'Cybercrime: The Council of Europe Convention' (2006) <http://fpc.state.gov/documents/organization/58265.pdf>

Axelrod E, *Violence goes to the Internet: Avoiding the Snare of the Net* (Charles C Thomas Publishers Springfield 2009).

Bande LC, 'The Making of Cybercrime Legislation in Malawi: A Comparative Analysis of Malawi's Proposed Cybercrime Law Against International Standards and Best Practices' (2018) 12(1) International Journal of Cyber Criminology <https://lirias.kuleuven.be/bitstream/123456789/404618/1/The+Making+of+Cybercrime+Legislation+in+Malawi+Pdf.pdf/>

Becker R, 'How Many Countries in Africa? How Hard Can the Question be?' (2012) <http://africacheck.org/reports/how-many-countries-in-africa-how-hard-can-the-question-be/>

Brenner S and Goodman M, 'The Emerging Consensus on Criminal Conduct in Cyberspace' (2002) 3(1) International Journal of Law and Technology <http://www.isrcl.org/Papers/Brenner.pdf/>

Brian H, 'A Global Convention on Cybercrime?' (2010) 1(3) Columbia University Law Journal <http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/>

Brian Harley, 'Crosswires: International Co-operation on Cyber Security' The Columbia Science and Technology Law Review blog (23 March 2010) <http://stlr.org/2010/03/>

Broadhurst R, 'Developments in the Global Law Enforcement of Cyber-crime' (2006) International Journal of Police Strategies and Management <https://doi.org/10.1108/13639510610684674>

Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (Elsevier Waltham 2011).

102 Van der Merwe (n 86) 52.

Collier D, 'Criminal Law and the Internet' in Buys R and Cronje F (eds), *Cyberlaw @ SA II: The law of the Internet in South Africa* (2nd edn, Van Schaik 2004).

Greg M, 'Global Cybercrime Treaty Rejected at UN' (*SC Magazine* 2013) <http://www.scmagazine.com/global-cybercrime-treaty-rejected-at-un/article/168630/>

Goldstein N, 'Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually' (5 September 2012) <http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02/>

Keir G,'Russia's Public Stance on Cyberspace Issues' in Czosseck C, Ottis R and Ziolkowski K (eds), Papers Delivered at 4th International Conference on Cyber Space Conflict, 5–8 June 2012, Tallinn, Estonia.

Kenneth W, *Oxford Studies in Normative Ethics* (Oxford University Press 2016).

Kharouni L, 'Africa: A New Safe Harbour for Cybercriminals?' (2012) <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf>

Kshetri N, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies' in *Cybercrime and Cybersecurity in the Global South* (Palgrave Macmillan Hampshire 2013) <https://doi.org/10.1057/9781137021946>

Lemos R, 'International Cybercrime Treaty Finalized' (2002) <http://news.cnet.com/2100-1001-268894.html.>

Lewis D, *The Interpretation and Uniformity of the UNCITRAL Model Law* (Kluwer Law International 2016) <http://www.uncitral.org/pdf/english/texts/electcom/computerrecords-e.pdf.>

Marler S, 'The Convention on Cybercrime: Should the United States Ratify?' (2002) New England Law Review.

Maidment M, 'Taxonomies in the Public Sector' (2012) <http://www.nglis.org.uk/tips/tipsben.htm/>

Marcum C, Higgins G and Tewksbury R, 'Doing Time for Cyber Crime: An Examination of the Correlates of Sentence Length in the United States' (2011) 2(1) International Journal of Cyber Criminology.

Mwaita P and Owor M, 'Workshop Report on Effective Cybercrime Legislation in Eastern Africa' (2013) <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/Octopus2013/2571_EastAfrica_WS_Report.pdf/>

O'Driscoll A, '100+ Terrifying Cybercrime and Cybersecurity Statistics and Trends' (Comparitech 2018) <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#gref>

Rademeyer J,'Conviction Rates An Unreliable Benchmark of NPA success' (12 April 2013) <http://africacheck.org/reports/conviction-rates-an-unreliable-benchmark-of-npa-success/>

Robert M, *Search and Seizure of Digital Evidence* (LFB 2005).

Schjolberg S and Ghernaouti-Helie S, *A Global Treaty on Cybersecurity and Cybercrime* (Black Swan 2011) <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>

Schjolberg S and Hubbard A, 'Harmonizing National Legal Approaches on Cybercrime' <http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf>

Sikuka K, 'Southern Africa: Region Cracks Down on Cyber Crime' (2012) <http://allafrica.com/stories/201204120866.html/>

Southern African Development Community, 'History and Treaty SADC' (1992) <http://www.sadc.int/about-sadc/overview/history-and-treaty/>

United Nations, Resolution 56/121 of 19 December 2001 On Combating the Criminal Misuse of Information Technologies <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf/>

Van der Merwe D, *Information and Communications Technology Law* (Juta 2016).

Westby J, *International Guide to Cyber Security* (American Bar Association 2005).

International Treaties and Conventions

Council of Europe Convention on Cybercrime (adopted 23 November 2001) 2001 ETS 185 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>.