Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players*

*Fawzia Cassim***

Abstract

Cyber crime is thriving on the African continent. The increase in broadband access has resulted in an increase in internet users. Thus, Africa has become a 'safe haven' for online fraudsters. African countries are pre-occupied with pressing issues such as poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability and traditional crimes, such as murder, rape, and theft. As a result, the fight against cyber crime is lagging behind. The lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cyber crime at national and regional levels have compounded the problem.

However, attempts are being made by some African countries to address cyber crime. The South African government has taken the lead in introducing cyber legislation to address cyber crime. The ineffectiveness of the South African common law to combat cyber crime, led to the promulgation of the Electronic Communications and Transactions Act 25 of 2002 (ECT). Although South Africa has adopted the Council of Europe's Convention on Cyber Crime CETS N0 185 (CECC) it has not ratified the treaty. Other African countries such as Botswana, Kenya, Uganda and Cameroon have also taken steps to introduce cyber legislation and build regional partnerships to combat cyber crime. This is commendable. However, it is recommended that all African countries should adopt and ratify the CECCC to avoid becoming an easy target for international cyber crime.

---

* This article is based on a paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011.

** BA (Law)(UDW) LLB(UN); LLM (Unisa) LLD (Unisa). Admitted attorney and conveyancer. Associate Professor: School of Law, University of South Africa.

In this article, I shall examine measures addressing cyber crime in South Africa and the way forward. To this end, the ECT, the recent case law, and the efforts to combat cyber crime in the banking sector will be examined. This article will also consider measures adopted to combat cyber crime in other Southern African countries (Namibia, Botswana and Zambia) and in certain African sub-regions such as East Africa (Kenya, Uganda and Rwanda) and West Africa (Nigeria and Cameroon). The article will also propose a way forward.

INTRODUCTION

Cyber crime or 'computer crime' appears to have no precise definition. On the one hand, a computer may become the 'object' of a crime when theft of a computer hardware or software occurs. On the other hand, a computer may become the 'subject' of a crime when it is used as an 'instrument' to commit traditional crimes such as fraud, theft, extortion, 'new' types of criminal activity such as denial of service attacks and malware, identity theft, child pornography, or copyright infringement.[1]

The face of cyber crime has changed recently as a result of new Internet environments, organised cyber crime groups, and new 'smart' viruses. The development of new accessible technologies and the expansion of the Internet have resulted in new forms of criminal behaviour.[2] Cyber crime recognises no borders.[3] It is unnecessary for the perpetrator and the victim of a crime to meet, as the unlawful actions committed by a perpetrator in one country may have a direct and immediate effect in another. This has led to a call for specialised legislation to combat these 'new' criminal activities.

The article looks at cyber legislation formulated to address cyber crime in certain African sub-regions, such as Southern Africa, East Africa and West Africa. The South African position is examined in detail. The study reveals that the inability of national laws to address the challenges posed by cyber crime in African countries has intensified the call for the introduction of

---

1 See S Brenner & LL Clarke 'Distributing security: preventing cyber crime' (2005) *John Marshall Journal of Computer and Information Law* 659–709 at 665–666; and S Brenner & BJ Koops 'Approaches to Jurisdiction' (2004) *Journal of High Technology Law* 1–46 at 7. It should be noted that the terms 'computer crime', 'cyber crime' and 'IT crime' are used interchangeably throughout this article.

2 S Brenner 'Cybercrime investigation and prosecution: the role of penal and procedural law' 2001 *Murdoch University Electronic Journal of Law* 1–16.

3 *Id* at 3. Also see MD Goodman & S Brenner 'The emerging consensus on criminal conduct in cyberspace' 2002 *International Journal of Law and Information Technology* 139–223 at 142, 146–150.

specialised cyber legislation. African countries should take adequate measures to ensure that their criminal and procedural laws can meet the challenges posed by cyber crime. A balanced approach that considers the protection of fundamental human rights and the need for effective prosecution of cyber crime is advocated. African countries should accede to the CECC, to avoid becoming a 'safe haven' for cyber criminals. International and regional cooperation between countries is also required to address the global nature of cyber crime.

CHALLENGES FACING CYBER CRIME IN AFRICA

Cyber crime differs from traditional crimes. It can be committed easily, it requires few resources, and it can be committed in a specific jurisdiction without the offenders being physically present there.[4] Cyber crime does not require physical proximity between a victim and perpetrator. This compounds the problem of detection. Criminal laws regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries.[5] The fact that African countries have long and permeable borders, compounds the problem of detection.

The international character of cyber crime has created problems as illustrated by the 'love bug' virus which demonstrates that the existence of cyber crime laws is a fundamental prerequisite for investigation as well as prosecution. For instance, Philippine's failure to put cyber crime legislation in place, resulted in a Philippine national inflicting damage in twenty countries without suffering any consequence for his actions.[6] The failure to have adequate legislation reverberated around the globe and illustrated the vulnerability of our modern networked society. Therefore, the international character of cyber crime calls for international coordination and cooperation to address computer-related offences worldwide. Police officials cannot prosecute cyber criminals unless countries have adequate laws in place outlawing such criminal activities.[7]

---

4 *Ibid*.

5 Brenner & Clarke n 3 above at 659–709.

6 Goodman & Brenner n 3 above at 142.

7 P Hunton 'The growing phenomenon of crime and the internet: A cybercrime execution and analysis model' 2009 *Computer Law and Security Review* 528–535 at 530.

THE ROLE OF THE EUROPEAN CONVENTION ON CYBER CRIME (CECC)

The cyber crime problem has become a global problem that requires global intervention. It is submitted that many developing countries (including African countries) have inadequate investigative powers or technological capacities to address the problem. Attempts by conventions such as the CECC and the United Nations Convention against Transnational Organised Crime, to harmonise and streamline international cyber crime laws are commendable. However, in order to comply with these conventions, international cooperation by countries is needed, to ensure the integrity of the Internet and address the global nature of cyber crime. The CECC, which was signed in Hungary on 23 November 2001, aims at encouraging countries to combat cyber crime.[8] The CECC criminalises certain computer actions such as the interception of non-public transmission of computer data; establishes corporate liability; calls for the production of stored computer data; and recommends mutual assistance between countries in investigations.[9] The CECC is said to be the first international treaty on crimes via the Internet and other computer networks, which addresses infringements of copyright, computer-related fraud, child pornography, and violations of network security. Its main objective is to advance a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation. Although the CECC aims at international cooperation in prosecuting cyber crime, it contains no provision for cooperation in securing networks. Thus, the Convention's goal to harmonise national laws to facilitate the police's ability to act across national borders is laudable. However, it is difficult to implement in practice.[10]

ADDRESSING CYBER CRIME IN AFRICA: ARE AFRICAN COUNTRIES RISING ADEQUATELY TO THE CHALLENGE?

Cyber crime is said to be growing faster in Africa than any other continent.[11] The increase in broadband services on the continent has led to an increase in

---

8 Anonymous 'Cybercrime law' available at: http://www.cybercrimelaw net/content/cybercrime html (accessed on 15 February 2011).

9 H Jahankhani 'Evaluating of cyber legislations trading in the global cyber village' 2007 *International Journal of Electronic Security and Digital Forensics* 1–11 at 9.

10 Brenner & Clarke n 1 above at 671.

11 E Kisambira 'East Africa to fight cybercrime with CERT' available at: http://news.idg no/cw/art.cfm (accessed on 5 October 2010). Also see N Kumar 'Africa could become the cybercrime capital of the world' available at: http://www.psfk.com/2010/04 (accessed on 6 December 2010).

the number of internet users. This has resulted in an increase in 'phishing'[12] attacks on unsuspecting customers who are lured to 'fake' sites.[13] Thus, Africa has become a 'safe haven' for online fraudsters. African countries have also been criticised for dealing inadequately with cyber crime, as their law enforcement agencies are inadequately equipped in terms of personnel, intelligence, and infrastructure.[14] The private sector is also ineffective in addressing cyber crime.[15] African countries are perceived to be preoccupied with attending to pressing issues such as alleviating poverty, the Aids crisis, the fuel crisis, political instability, ethnic instability, and traditional crimes such as murder, rape, and theft. As a result, the fight against cybercrime is lagging behind.

SOUTHERN AFRICA

South Africa

The Electronic Communications and Transactions Act 25 of 2002 (ECT)

The ineffectiveness of the South African common law to combat cybercrime, led to the promulgation of the ETC.[16] Earlier case law also illustrated the need for specific legislation to address computer crime. The case of *S v Mashiyi and Another*[17] is a case in point where the question of admissibility of computer-generated documents arose. The court held that in terms of the 'prevailing law', it could not admit the disputed documents which contained information that has been processed and generated by a computer into evidence.

The main objective of the ECT is 'to provide for the facilitation and regulation of electronic communications and transactions in the public interest'. The ECT deals comprehensively with cyber crime in Chapter 13. The following offences are punishable offences under the ECT: sections 86(4) and 86(3) introduce new forms of crimes called anti-cracking (anti-thwarting) and hacking law which prohibit the selling, designing or

---

12 The term 'phishing' refers to an e-mail scam that is sent to both consumers and companies in order to obtain either personal information from an individual or confidential information about an enterprise. The term was coined because phishers are 'fishing' for personal information. For more information about phishing, see E Ryan *Sunday Times* 'Ugly world of criminals who go phishing' 27 June 2010 8.

13 M Malakata 'African cybercrime threatens to derail internet banking' available at: http://www.computerworld.com/na/articles/2010/01/29 (accessed on 8 October 2010).

14 *Ibid*.

15 *Ibid*.

16 See AA Ojedokun 'The evolving sophistication of Internet abusers in Africa' 2005 *The International Information and Library Review* 11–17 at 15. Also see J Burchell 'Criminal justice at the crossroads' 2002 *South African Law Journal* 579 at 585.

17 2002 2 SACR 387.

producing of anti-security circumventing technology; e-mail bombing and spamming are addressed in sections 86(5) and 45 of the ECT respectively; whereas the crimes of extortion, fraud and forgery are addressed in section 87.[18]

While the advent of the ECT is lauded, there is still room for improvement. To illustrate this, the criminal sanctions in terms of section 89 of the ECT have been criticised for not being stringent enough.[19] For example, section 89(1) provides a maximum period of one year's imprisonment for most crimes prohibited by section 86, while the crimes prohibited in sections 86(4) and (5) (matters such as denial of service-attacks), and crimes prohibited in section 87 (extortion, fraud and forgery) prescribe a fine or imprisonment not exceeding five years. However, the Regulation of Interception of Communications and Provision of Communications-Related Information Act 70 of 2002 (RICA) prescribes harsher measures.[20] It is submitted that more stringent penalties are needed to deter 'crafty' cyber criminals.

Section 3 of the ECT provides that in instances where the ECT has not made specific provision for criminal sanctions, the common law will prevail. However, other statutory remedies prevail in the prosecution of other cyber crime. For example, the Prevention of Organised Crime (Second Amendment) Act 38 of 1999 (POCAA) and Financial Intelligence Centre Act, 2001 (FICA), regulate the prevention of money laundering and other financially related crimes.[21]

The Act has also created 'cyber-inspectors' who are authorised to enter premises to obtain information regarding cyber crime (in terms of section 82(1)). Cyber inspectors are empowered in terms of the ECT to enter any premises and access information that may impact on an investigation into cybercrime. However, this provision may infringe sections 14 and 25 of the

---

18 Also see S Snail 'Cybercrime in South Africa – hacking, cracking and other unlawful online activities' 2009 *Journal of Information Law and Technology* available at: http://go.warwick.ac.uk/jilt/2009-1/snail (accessed on 28 May 2009).

19 See DP van der Merwe *et al Information and communications technology law* (2008) at 75–78.

20 RICA requires all cell phone customers to register their details with their cell phone providers. The aim is to help law enforcement agencies to identify the users of cell phone numbers and track criminals using cell phones for illegal activities. Section 51 of RICA prescribes fines not exceeding R2 000 000 or imprisonment not exceeding ten years. Regarding juristic persons, fines may increase to a maximum of R5 000 000.

21 It should be noted that POCAA targets organised crime, money laundering and criminal gang activities both nationally and internationally, whilst FICA outlaws money laundering and other unlawful actions.

1996 Constitution, which deal with the right to privacy and right to property respectively.

Case law

There appears to be a dearth of decided case law as many economic crime cases are still pending. In *R v Douvenga*[22] the question was whether an accused employee, Douvenga, was guilty of a contravention of section 86(1) of the ETC. The accused intentionally and without permission, gained entry to data which she knew was contained in confidential databases and contravened the provision by sending this data by e-mail to her fiancé. The accused was found guilty of contravening section 86(1) of the ETC. She was sentenced to a fine of R1 000 or imprisonment for a period of three months. This case illustrates that the crime of hacking is entrenched in section 86(1) of the ETC. Thus any unlawful access and interception of data is regarded as a criminal offence.

The case of *S v Ndiki and Others*[23] demonstrates that the South African courts are adopting a progressive approach. In this case, the state sought to introduce certain documentary evidence consisting of computer-generated print-outs, designated as exhibits D1-D9, during the course of a criminal trial. The court found that because certain individuals had signed exhibits D1 to D4, the computer had been used as a tool to create the relevant documentation. Therefore, these documents constituted hearsay. Exhibits D5 to D9 had been created without human intervention and such evidence constituted real evidence. Therefore, the admissibility of this evidence depended on the reliability and accuracy of the computer and its operating systems. The state bore the onus of proving such accuracy and reliability. The court's progressive approach in regarding part of the computer-based evidence as real evidence has been lauded by certain academics.[24]

A Malawian, Christopher Mbeye, who was working as a waiter was recently jailed for credit card fraud.[25] He was found to be illegally skimming credit cards at a restaurant in Cape Town where he was employed. Mr Mbeye was

---

22 District Court of the Northern Transvaal, Pretoria, case no 111/150/2003,19 August 2003 (unreported case).

23 2008 2 SACR 252.

24 DP van der Merwe *et al* n 19 above at 121–123.

25 The police had confiscated a laptop belonging to Mr Mbeye. The laptop was loaded with a software programme that could read and retrieve stored information from a skimming device that Mr Mbeye had used at the restaurant. See Anonymous 'Waiter jailed for credit card fraud' available at: http://www/news24.com/SouthAfrica/News (accessed on 19 October 2010).

jailed for a year after pleading guilty to ten counts of fraud, eleven violations of the ECT, and one violation of the Immigration Act. He is to be deported after serving his jail sentence.

Cyber crime in the banking sector

Cyber crime is said to be increasing rapidly in South Africa. The South African banking sector and software security companies have expressed concern about the increase in phishing schemes.[26] Phishing is found to be the most common type of online fraud. It involves the online theft of Internet users' identities. Many of the phishing e-mails appear to originate mainly in the Ukraine, Russia and Nigeria (so-called 'Nigerian 419 scam' or advance fee fraud). The South African Banking Risk Information Centre (SABRIC) has reported that the incidence of phishing has more than trebled since January 2011.[27] Cyber criminals have also become quite crafty and sophisticated, and they have constructed different types of phishing schemes that target clients of multiple banks simultaneously.[28] This increases the perpetrator's chances of success.

A new wave of fraudulent internet activities targeting government departments has come to the fore in South Africa. In a recent case, suspected cyber hackers stole R 5,5 million from the bank account of the Mpumalanga Education Department, presumably with inside help.[29] The fraud was discovered when a clerk at the department's bank (Nedbank) noticed that huge amounts that were paid into a woman's account did not fit her financial profile at the bank. The North Gauteng High Court awarded a court order to seize the accounts. However, only a small amount (R 1 543 345) could be recovered. It transpired that the R5 million had been siphoned off and disappeared without trace. The recent bank SMS scam case has also raised serious questions about the security of online banking.[30] It involved a

---

26 N Moodley-Isaacs *The Saturday Star Personal Finance* 'Crafty cyber-crooks going all out to rob you' 1 May 2010: 1. Also see L Samodien *Saturday Star* 'Huge spike in SA internet phishing' 12 February 2011:10.

27 *Ibid*.

28 N Moodley-Isaacs *The Saturday Star Personal Finance* 'What is phishing exactly?' 1 May 2010 1.

29 B Viljoen 'Hackers steal R 5,5 m from department' available at: http://www.legalbrief.co.za (accessed on 25 November 2009). Thieves also recently tried to breach the Land Bank IT security system during the Christmas period. A gang hacked into the Land Bank IT system to transfer R 150 million to dummy companies and false accounts set up with Absa which is the official banker. Fortunately, alert Absa staff noticed the suspicious transfers and froze the accounts in time. See DW Viloen '150-m cyber bank fraud' *Saturday Star* 8 January 2011 1.

30 K Chelemu 'Banks open files for police in SMS scam case' *The Times* 23 June 2009 6.

Vodacom employee who was working with a syndicate to intercept SMS notifications from banks to their customers. It has been reported that some R7 million was siphoned off from customers' accounts as result of this scam.

However, the establishment of organisations such SABRIC to combat cyber crime in the banking industry is a positive move. SABRIC provides the banking industry with crime risk information management services and facilitates inter-bank initiatives to reduce the risk of organised bank-related crime, through effective public private partnerships.[31] The police are collaborating with banks and the IT industry via SABRIC to combat cyber crime and bring cyber criminals to book.[32] It is submitted that the private sector has a vested interest in addressing bank-related crime. Such public-private partnerships are necessary in the fight against cybercrime.

According to the South African Ombudsman for Banking Services, Clive Pillay, banks have an obligation to provide their clients with a safe and secure banking environment. If banks fail to meet their obligations, they could be held liable if their clients fall victims to phishing. Banks have to prove negligence on the part of the client to avoid liability.[33] Banks have been commended for making software programmes available to their clients. This is a step in the right direction in combating phishing.[34] However, clients also have to be vigilant when transacting online, and they must avoid becoming victims to phishing operators. Thus, internet users need to take proper precautions.

South Africa and the CECC

South Africa has adopted the CECC but not ratified it. So far, it is the only African country to have done so. The treaty contains important provisions to assist law enforcement in its fight against transborder cyber crime. Therefore, South Africa needs to ratify the cyber crime treaty to avoid becoming an easy target for international cyber crime. Although substantive obligations are in place, South Africa needs to revise some procedural provisions to comply with the treaty such as introducing a 24/7 contact centre. The South African

---

31 SABRIC was established in 2002 as a wholly owned subsidiary of the Banking Association. Its key stakeholders are the four major South African banks namely, Standard Bank, Nedbank, Absa and First National Bank. For further information, see https://www.sabric.co.za (accessed on 16 February 2011).

32 N Moodley-Isaacs *The Saturday Star Personal Finance* 'What banks are doing' 1 May 2010 1.

33 N Moodley-Isaacs *The Saturday Star Personal Finance* 'Banks must prove that you are negligent' 1 May 2010: 1.

34 E Ryan *Saturday Times* 'Caution paramount for clients and users' 27 June 2010: 8.

government seems to be presently focused on basic service delivery, the Aids issue, and the more traditional crimes given the current situation in the country where crime, poverty, and corruption are rife. However, the establishment of the Computer Security Incident Response Team (CSIRT) indicates that a move to tackle cyber crime is gathering momentum.[35]

The way forward

A website on child pornography has also been introduced to alert service providers of criminal activities.[36] This website was launched by the Film and Publication Board (FPB), to eliminate child pornography in South Africa. The aim is not to prosecute paedophiles and child molesters, but to be a public partner in the fight against child pornography. The increase in broadband speed has raised growing concerns that cyber security is becoming difficult to maintain. However, a recent decision by Vodacom (internet service provider), to block access to a controversial website where users can allegedly solicit sex from minors, has been welcomed by the Film and Publication Board.[37] This is a step in the right direction.

The Protection of Personal Information Bill is regarded as a mechanism for the protection of the right to information. It will be enacted sometime during 2011.[38] It is submitted that the promulgation of information protection legislation in South Africa will impact on *inter alia*, the Promotion of Access to Information Act 2 of 2000 (PAIA) and the ECT, as far as information privacy is concerned.

Although the ECT goes a long way towards addressing cyber crime in South Africa, there is room for improvement. South Africa needs to prescribe harsher penalties to deter cyber criminals. The feasibility of introducing collaborative initiatives involving the police, the private sector, and academia, to combat cyber crime should also be explored. It is important to

---

35 Anonymous 'Computer security gets own response team' available at: http://www.csir.co.za/news/2009 (accessed on 9 October 2009).

36 B Sekoma 'New website fights child pornography' available at: http://www.ngopulse.org/article (accessed on 21 October 2010).

37 Anonymous *Legalbrief Today* 'Vodacom cuts access to sex site' available at: http://www.legalbrief.co.za/article (accessed on 30 November 2010).

38 M Van Eck 'Protection of Personal Information Bill: An overview' available at: http:// www.derebus.org.za (accessed on 20 October 2010). It should be noted that the Protection of Personal Information Bill is presently being debated before parliament. However, the Protection of Information Bill has been criticised for constituting another form of censorship. See D Latham 'Top Writers condemn Protection of Information Bill' available at: http://allafrica.com/stories (accessed on 21 October 2010).

involve all role players in the struggle against cyber crime. However, Jacqueline Fick advocates a proactive rather than reactive approach towards cyber crime.[39] She suggests that the focus should shift to prevention rather than prosecution. To this end, the communications and IT industries should be designing products that are resistant to crime and these products should also facilitate the detection and investigation of cyber crime.[40]

Attempts to address cyber crime in Africa are not, however, restricted to South Africa.

Namibia

The Namibian Electronic Transactions and Communications Bill is presently being tabled before the Namibian parliament.[41] Namibia has also experienced misuse of information communication technologies (ICTs) such as identity theft and the use of pornographic images on cell phones; hence the need for such legislation. The Bill, *inter alia*, addresses the regulation of electronic transactions, communications and information systems management, promotes the use and development of electronic transactions and provides for incidental matters.

Botswana

Although the incidence of cyber crime is low, it is said to be increasing. Initially, the general criminal law applied to cyber crime cases. However, legislation has now been introduced to address cyber crime. The Cyber Crime and Computer Related Crimes Act 22 of 2007 was passed in December 2007. The aim of the law is 'combat cyber crime and computer related crime, to counteract criminal actions perpetrated through computer systems and to facilitate the collection of electronic evidence'.[42] This legislation will enable Botswana to embrace the global information society. However, the next challenge will focus on effective law enforcement. According to Botswana's Chief Prosecution Counsel, Mr Ngakaagae, Botswana should accede to the CECC to entrench international cooperation on cybercrime matters and to avoid becoming an easy target for international

---

39 J Fick 'Prevention is better than prosecution' (2009) *De Rebus* 1–6. Also available at: http://library-lexisnexis.unisa.ac.za/nxt/gateway (accessed on 19 October 2010).

40 *Ibid*.

41 L Khobetsi 'Comunications Bill almost a reality' available at: http://www.ecomomist.com na/index. (accessed on 8 October 2010).

42 T Motlogelwa 'Cyber crime law gets teeth' available at http://www mmegi.bw/index (accessed on 19 October 2010).

cybercrime. As the legislation is based on the EU model, there would be very little impediment to accession.[43]

Zambia

Ignorance has been mooted as one of the main reasons why many African people fall victim to online scams. Therefore, the Zambian government is trying to educate consumers about cyber crime. It has introduced the National Policy Framework on Cyber Crime, which criminalises cyber security criminal activities and computer misuse offences.[44] It has also approved a global cyber security protocol that strives to protect internet users. The global cyber security agenda (GCA) was launched by the International Telecommunication Union (based in Geneva, Switzerland) in May 2007, to coordinate an international response to the growing challenges to cybersecurity. It calls for the development of cyber crime legislation that is globally applicable and consistent with existing national and regional legislative measures. The GCA maintains that countries should harmonize their legal frameworks to combat cyber crime and facilitate international cooperation. [45] However, Zambia has been criticised for lacking skills, equipment and organisational abilities to fight cyber crime.[46]

EAST AFRICA

Kenya

Kenya enacted cyber legislation to combat cyber crime during 2009. The Kenyan Information Communications Amendment Act 2009 was passed by the Kenyan parliament and signed by the President during January 2009 and addresses cyber crime in sections 83 W–Z and 84 A–F. These sections deal with, *inter alia*, unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of computer services, damaging or denying access to computer systems, unlawful possession of a device and data, electronic fraud, tampering with computer source documents and publishing obscene material in electronic form. The enactment of the Kenyan Information Communication Amendment Act,

---

43 Anonymous 'Botswana' available at http://www.cyberplex.africa.com (accessed on 7 October 2010). Also see K Ngakaagae 'Botswana (Experience on Cybercrime)' a paper presented at Octopus Interface Conference – Co-operation against Cybercrime at Strasbourg 23–25 March 2010.

44 Malakata n 13 above.

45 See M Gercke *Understanding Cybercrime: a guide for developing countries* (ITU publication 2009) Also available at : http://www.itu.int/ITU-D/cyb/cybersecurity/legislation/ html (accessed 27 May 2011)

46 Malakata n 13 above.

2009, facilitates the prosecution of cyber crime offenders. Nevertheless, the Act has been criticised for not addressing cross-border crime.[47] Kenya has, together with other East African states (namely, Uganda, Tanzania, Rwanda and Burundi), introduced Computer Emergency Response Teams (CERTs) to address the growing spectre of cyber crime.[48] The aim is to establish and harmonise internet laws and security policies in the East Africa region and to increase regional trade and investment.[49] To this end, the five countries will also establish a collaboration framework for the national CERTs at regional and international levels.

Uganda

Previously, the existing penal laws were used to govern cyber crime in Uganda. The case of *Uganda v Garuhanga and Mugerwa*[50] illustrates the ineffectiveness of past penal laws. This case involved the manipulation of computer data resulting into 3,8 billion shillings loss for Shell Uganda Limited. The accused were charged with embezzlement and false accounting, as there was no enabling law to address charges under computer forgery and computer fraud at the time.

Uganda has been criticised for its inability effectively to address cyber crime because of its inadequate infrastructure and poorly trained prosecution and law enforcement personnel. Criticism has been levelled in the following areas :

- Uganda does not have adequate forensic labs for its cyber crime investigators.
- Prosecutors also lack proper training in cyber crime issues and this could hamper effective combating of cyber crime.
- Uganda may also become a cyber crime haven as the country cannot offer other countries mutual legal assistance with regard to cross-border crime.

There is lack of awareness by the public about the threat of cyber crime.[51]

---

47 K Okuttah 'East Africa: EAC eyes trade growth with cyber laws' available at: http://law/africa.com/stories (accessed on 21 October 2010).

48 E Kisambira 'East Africa to fight cybercrime with CERT' available at: http://news.idg no/cw/art.cfm (accessed on 5 October 2010).

49 *Ibid*.

50 CR 17 of 2004 Bugand Road Court.

51 D Bakibinga 'Cyber crime in Uganda' available at: http://www.dpp.go.ug/perspectives (accessed on 21 October 2010).

However, recently, steps have been taken to address the problem. Uganda has tabled three sets of draft laws before parliament, namely, the Electronic Transactions Bill (to facilitate the development of electronic commerce), the Electronic Signatures Bill (to ensure secure transactions), and the Computer Misuse Bill (to address computer misuse offences such as unauthorised modification of computer material). These Bills were recently passed into law by the Ugandan parliament, namely, the Electronic Transactions Bill Act 2010, the Electronic Signatures Bill Act 2010 and the Computer Misuse Act 2010.[52] The aim of these cyber laws is to improve the security of electronic transactions and devices. Companies and individuals involved in cyber crime face tough penalties in terms of these new laws: companies may be de-registered and individuals may face three years in prison if they are charged with transgressing the law.

Rwanda

Rwanda has also prepared draft information, communication, and criminal law Bills on cyber crime.[53] The Bills cover e-signatures, consumer protection, privacy and content legislation. Bills on digital copyright and e-contracting have also been tabled before the Rwandan parliament.[54]

WEST AFRICA

Nigeria

There is currently no specific legislation to combat cyber crime.[55] Most cybercrime takes place at internet access points or cyber cafés, which makes cyber crime difficult to prove.[56] Nigeria has received worldwide attention and notoriety because of the Nigerian '419 scam' which involves a 'confidential' e-mail from a prominent Nigerian who wants assistance to transfer 'ill-gotten funds' offshore. This practice continues to net hundreds of unsuspecting victims every year. The 'yahoo boys' are behind the 419 scam or advanced fee fraud.[57] The lack of proper law enforcement and the lack of training and

---

52 Anonymous 'Uganda passes cyber laws' *Computing* available at: http://www.balancingact-africa.com/news/en/issue (accessed on 15 February 2011).

53 K Okuttah n 47 above.

54 *Ibid*.

55 See TI Akomolede 'Contemporary legal issues in electronic commerce in Nigeria' (2008) 3 *PER* 1–24 at 13–15.

56 OB Longe & SC Chiemeke 'Cyber crime and Criminality in Nigeria – What Roles are Internet Access Points Playing?' (2008) 6/4 *European Journal of Social Sciences* 132–139.

57 OR Eniman & A Bola 'Cyber crime in Nigeria' 2010 *Business Intelligence Journal* 94–98. See AA Ojedokun n 16 above at 14 regarding further discussion about the Nigerian fee scam.

expertise of police officers have compounded the problem. A call has been mooted for specifically trained cyber police, the introduction of an expert body, and a comprehensive law to combat such crime, and the establishment of a comprehensive forensic commission to train forensic personnel.[58]

However, the government is taking steps to address the problem. The Economic and Financial Crimes Commission (EFCC) has been granted powers to arrest and prosecute individuals and organisations suspected to be involved in the promotion of cyber crime.[59] A Bill on cyber crime has also been tabled before the National Assembly. However, it was not passed. The non-passage of the Bill has been criticised.[60]

Cameroon

The Economic Community of West African States (ECOWAS) has also met to discuss, *inter alia*, the implementation of ICT policy and legislation, access and interconnection regulation, universal access, and to provide guidelines for the gradual transition to open markets.[61] A Bill on cyber crime and cyber security has also been tabled before parliament, to address the increase in hacking and scams on the internet.[62]

CONCLUSION

The global nature of computer technology presents a challenge to African nations to address cyber crime. Domestic solutions are inadequate because cyberspace does not recognise any geographic or political boundaries, and many computer systems can be easily accessed from anywhere in the world. It is also difficult to obtain accurate cybercrime statistics because a number of crimes go undetected and unreported. It is also a costly exercise to develop and maintain security and other preventative measures. It is thus a continuous uphill battle to develop computer crime legislation that applies both nationally and internationally. The CECC's role is important as it attempts to establish consistency in the cyber crime laws of various countries. However, many states still have to sign, let alone ratify, the Convention

---

58 *Ibid*.

59 Longe & Chiemeke n 56 at 135.

60 E Nkanga 'Non-passage of cyber Bill decried' available at: http://www.thisday live.com/articles c (accessed on 27 May 2011).

61 OA Ogundeji 'African states to discuss cybercrime' available at: http://www.thestandard.com/news/2008 (accessed on 21 May 2009).

62 PG Bekono 'The Bill on Cybercrime and Cybersecurity presented to parliamentarians in Cameroon' available at: http://www.diplointernet.governance.org. (accessed on 5 October 2010).

before it will serve as a deterrent. The unanimous participation of all nations is thus required to achieve meaningful prosecution.

There is a growing recognition that cyber crime is thriving on the African continent because of a lack of IT knowledge by the public and the absence of suitable legal frameworks to deal with cybercrime at national and regional levels, Thus, attempts are being made to address cyber crime. When enacting legislation, African countries should follow a balanced approach that ensures the protection of fundamental human rights and the effective prosecution of cyber crime. However, African countries also need international legal, financial and technical assistance to combat cyber crime. African countries need to impose strict penalties on cyber criminals operating from and in their countries, and they also need to accede to the CECC not least because cyber crime is thriving on the African continent.

Although attempts by African countries to address cyber crime are to be encouraged, they need to do more. African countries need to take the following steps to combat cyber crime on the African continent:

- Introduce adequate cyber crime legislation.
- Harmonise their legal frameworks to combat cyber crime and facilitate international cooperation.
- Educate the public about the threat of cyber crime as ignorance has been mooted as one of the main reasons that Africans fall victim to cyber crime. There should be greater public awareness on cyber crime to educate the public about the need for caution with regard to the use of cyber space or transacting online. Children should be taught computer ethics education in schools and the public educated about the risks of transacting online.
- Regulate cyber cafés as most cyber crime occurs at these locations.
- Introduce specialised law enforcement and training skills. There should also be continuous research and training of personnel in the security, finance, judicial and police enforcement sectors to keep abreast with evolving technology.
- Improve computer forensic capabilities through the appointment of competent and experienced staff.
- Build regional partnerships and enter into multilateral agreements with other countries to combat internet crime and corruption.
- Initiate support and training within government, with the help of the private sector and international organisations.
- Ratify and accede to the CECC as the CECC is open to accession by non-member states.