CATCHING UP WITH THE REST OF THE WORLD: THE LEGAL FRAMEWORK OF CYBERCRIME IN AFRICA

by

Oluwabukola Adelaja

LLB, GradDip(Legal Practice), LLM(Media and Technology Law, ongoing – UNSW)

IINTRODUCTION:

In recent times, there has been a rapid growth in ICT especially the internet in Africa. This has caused a growing concern among relevant stakeholders on the increase on cybercrime in Africa. This poses a risk of cyber attack exposure to critical economic and government sectors within Africa. Compared to other developed countries, only an average 15% of the African population uses the internet. Even though this is low in relative terms, Africa is fast becoming a hot spot for the perpetration of cybercrime. This is largely due to the expansion of broadband internet and the absence of regulatory measures to crack down on cyber criminals.

The main challenge that is emerging is that the continent seems generally ill equipped to address the issue of cybercrime. The US and the UK are among the leading countries with a high rate of cybercrime. However, they are able to balance this out through implementing regulatory and technologically advanced measures to curb cybercrime.

This paper will argue for the need to implement anti cyber crime legislation in Africa. It will start off by looking at the current legislative efforts in the continent. This will be achieved by a selective case study of key countries in regions on Africa, namely the northern, western, eastern and southern parts of Africa.

Legislative effort is only part of the whole process. This paper will also argue for the need and importance of collaborative alliances within the regions through regional bodies such as the South African Development Co-operation (SADC), East Africa Community (EAC) and Economic Co-operation of West African States (ECOWAS). This

should also extend outside the region and through the involvement and developments of experts in the field. This will be achieved by looking at current collaborative efforts in other parts of the world. This will be done bearing in mind the workability of such collaborations or technological implementations in Africa. Is the technological terrain in Africa ripe for such a move? Are there other social, political or economic constrains that exist to make this move difficult? Are there any current anti cybercrime efforts in place?

WHAT IS CYBERCRIME

The world is waking up to the existing problem of cybercrime. With the advancement of technology came great technological innovations in all facets of life that have had a hugely positive impact in these areas. With this advancement came the phenomenon of cybercrime. Individuals, Corporations, organizations and countries have experienced cybercrime in one form or another. In this day and age, ignorance of what is cybercrime and its resultant effect could pose a serious consequence.

Cybercrime in simple terms are crimes committed against the computer or information found on computers or crimes involving computer and communication technologies[1]. The Cybercrime Convention of the Council of Europe 2001 does not directly define cybercrime. However, it makes provisions for those activities that member states are required to legislate upon. These include:

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Offences related to child pornography

[1] W Jayawickrama, Cyber Crime – *Threats, Trends and Challenges*, Computer Security Week 2002 – Brisbane, 3

- Offences related to infringements of copyright and related rights
- Attempt and aiding or abetting

The above can be summarized to mean that the convention defines cybercrime as any prohibited act involving use of the computer system for the purposes of Illegal access, Illegal interception, Data interference, System interference, Misuse of devices, Computer-related forgery, Computer-related fraud, Offences related to child pornography, Offences related to infringements of copyright and related rights and attempt and aiding or abetting.

The US Department of Justice defines it as:

"any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution."[2]

The internet really took off in the last decade with it growing from 361 users in 2000 to over 2 billion users in 2010. It a melting pot for social and business interaction and a meeting point of sorts. The success of social media in recent years as seen it become an attraction for cyber crooks to carry out various forms of cybercrime.

TYPES OF CYBERCRIME (IN THE AFRICAN CONTEXT)

Advanced Fee Fraud – This is popularly referred to as the "Nigerian scam" due to the origin of the crime or "419 scam" due to the section of the Nigerian criminal code that outlaws this type of crime. " The scammers usually contact you by email or letter and offer you a share in a large sum of money that they want to transfer out of their country. They may tell you about money trapped in central banks during civil wars or coups, often in countries currently in the news. Or they may tell you about massive inheritances that are difficult to access because of government restrictions or taxes in the scammer's

[2] American Bar Association website, *Whitecollar criminal statutes*, 25 June 2002, 1, available at: http://apps.americanbar.org/buslaw/newsletter/0001/materials/whitecollar.pdf

country. Scammers ask you to pay money or give them your bank account details to help them transfer the money. You are then asked to pay fees, charges or taxes to help release or transfer the money out of the country through your bank. These 'fees' may even start out as quite small amounts. If paid, the scammer makes up new fees that require payment before you can receive your 'reward'. They will keep making up these excuses until they think they have got all the money they can out of you. You will never be sent the money that was promised".[3] These types of scams are very popular in Africa because they do not require an exceptional knowledge of computers and the Internet.

Phishing – this involves cybercriminals posing as reputable organizations or businesses in order to obtain confidential information from their victims. This is often carried out through sending emails or utilizing phony website. An example of this is where victims are asked to enter their login details on "bank" websites where they are then redirected to the fake website allowing the cybercriminals to then record their information. Phishing (sometimes called carding or brand spoofing) is often linked to identity fraud. Financial and personal details obtained fraudulently from victims are used to gain access to funds and this has cost businesses and financial institutions billions of dollars. Phishing scams increased 12 percent from January to March 2011 than during the same period in 2010.[4]

Spamming - *"Spam is the common term for electronic 'junk mail'—unwanted messages sent to your email account or mobile phone. The Spam Act 2003 (Spam Act) regulates the sending of commercial electronic messages and prohibits the sending of these messages except in certain limited circumstances"*. [5]

Spamming has become a very viable option for advertisers mainly because of the low operating cost, which mainly involves the management of mailing lists. This comes at a

[3] Australian Competition & Consumer Commission, ScamWatch website, available at: http://www.scamwatch.gov.au/content/index.phtml/tag/Nigerian419Scams
[4] PhishTank website – January 2011 stats, available at: http://www.phishtank.com/stats/2011/01/
[5] Australian Communications and Media Authority (ACMA), *A Consumer's Guide to Spam*, available at: http://www.acma.gov.au/webwr/_assets/main/lib100234/fs%20163%20-%20consumer%20guide%20to%20spam.pdf, p1

very costly expense to internet users. The estimated figure of spamming in 2011 is around seven trillion. It has therefore become a major source of legislation in different jurisdictions. Various countries have laws that address the issue of spamming in various degrees. A person who creates electronic spam is referred to as a spammer.[6]

Emerging cybercrimes – following the expansion of the internet and broadband access into Africa, some other types of cybercrimes are being introduced into the continent. For example, hacking and hackers were viewed as urban legends of fairytales. They were seen as acts that only took place in countries such the US due to their advanced internet technology. This notion is changing and becoming less of an unrealistic phenomenon. For example, internet access has become a more viable option for South Africans due to a developed telephone system. This allows for ease of internet connectivity within homes. As a result, hacking became a hard reality in the country with its own hacking personalities and organizations being developed underground.

Website cloning is another emerging cybercrime activity in Africa. "Website cloning refers to the copying or modification of an existing website design or script to create a new website".[7]Website cloning allows designers to create websites without the need to write scripts from scratch. This method is used to perpetrate cybercrime by deceiving victims into believing the cloned website is the real website. It often involves obtaining private and financial details of the victims such credit cards details and passwords. "Fraudsters cloned the website of a savings and loans company in Ghana in 2009 and provided contact numbers purported to be that of the company. Using a gmail e-mail account they sent unsolicited mails to potential victims requesting them to act as next of kin for a deceased account holder who had $1,000,000 in his account. Victims were made to pay $1,200 as processing fee for the money to be transferred through Citibank, UK".[8]

---

[6] Wikipedia website, *Spam (Electronic),* available at: http://en.wikipedia.org/wiki/Spam_%28electronic%29
[7] ehow website, *What is Website Cloning*, available at: http://www.ehow.com/facts_6816849_website-cloning_.html
[8] I E Quist, *Addressing Emerging Cybercrime Trends in West Africa: The Ghana Police Perspective*, available at:

CYBERCRIME IN AFRICA

All the types of common cybercrime activities explained above are present in one form or another in the African continent. In fact, Africa has become a fertile ground for cybercrime for reasons ranging from under developed technology, high crime rate and archaic legislation. The latter reason will be the focal point of this paper because it has the power to bring about a change for the better in the other areas serving as contributory factors or fuel to a thriving cybercrime climate in Africa.

"Cybercrime is growing at a faster rate in Africa than on any other continent in the world, according to statistics presented at a conference on the matter in Cote D'Ivoire in 2008. Cybersecurity experts estimate that 80 percent of PCs on the African continent are already infected with viruses and other malicious software. And while that may not have been too worrisome for the international economy a few years ago (just like the continuing war in the Democratic Republic of the Congo does not affect our daily lives), the arrival of broadband service to Africa means that is about to change. The new undersea broadband Internet cables being installed today will make Africa no further away from New York than, say, Boston, in the virtual world".[9]

The introduction of broadband internet to Africa does not only spell doom for the continent but it has a potentially huge impact on the world. With this development, the internet world becomes an even smaller global village. This means that it becomes much easier to perpetrate cybercrime from within Africa into any part of the world with just the press of a button.

What happens in the cyber world in Africa should not only concern those within the continent but also those outside because of the impact cybercrime coming out of Africa can have on the world. Africa will become more attractive to cybercriminals from all walks of life due to the lack of protection for users activities over the internet.

---

http://waccs.web.officelive.com/Documents/Addressing%20Emerging%20Cybercrime%20Trends%20in%20West%20Africa%20-%20The%20Ghana%20Police%20Perspective%20by%20Isaac%20Quist.pdf, 6

[9]Foreign Policy News website, 24 March 2010, available at: http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd

CURRENT LEGISLATION AND LEGISLATIVE EFFORTS ON CYBERCRIME IN AFRICA

In this section, the focus will be placed on specific countries representing the different regions of Africa. This is due to the fact that time will not permit one to examine every country in the continent.

Nigeria (West Africa) – over the last decade, there has been a plethora of activities in clamoring for cybercrime legislation in Nigeria. There is currently no cybercrime legislation in Nigeria. Till date, there are over 100 IT related bills before the Nigerian legislature – the National Assembly none of which have been passed into law. Some of these bills are: the Cybersecurity and critical Infrastructure bill, the Privacy bill, the Electronic Commerce bill, Computer Security Protection bill; Electronic Transaction bill; the Intellectual Property Commission bill; Evidence Act Amendment bill among others.[10]

Nigeria finds itself in a disadvantaged position with this development especially with the recent expansion in its broadband networks with the recent introduction of two submarine cables of MainOne and Glo1 in 2010, complementing the already existing SAT 3 and the coming of MTN's WACS later this year. The lack of legislation will serve as a hindrance to the expansion of the broadband network in Nigeria and cement its status as the third country with the highest rate of cybercrime in the world after the US and the UK.

Some efforts have been made by industry groups and relevant agencies such as the Nigeria Internet Group, Association of Telecommunications Companies of Nigeria and the National Information Technology Development Agency. These efforts include organizing training sessions for the legislators on the importance of this exercise. It is obvious that more efforts are required by these groups and more industry players to achieve the desired result.

[10] It is interesting to note that Ghana another West African country has passed into law the Electronic Transactions Act and the National Information Technology Agency Act in December 2008.

South Africa (Southern Africa) – Being the most advanced economy in Africa comes with its disadvantages. This has seen South Africa having to deal with a fast increase in cybercrime. It passed the Electronic Communication and Transactions Act in 2002. "The main objective of the legislation is to enable and facilitate electronic transactions by providing for its enforceability and thus creating public confidence in electronic transacting. The Act also provides for the appointment of cyber inspectors whose duties include investigation of activities of cryptography and authentication service providers and also inspection of websites".[11] Crimes outlawed under chapter 13 of the Act are grouped into four categories: those involving unauthorized access to data, interception and interference with data and computer related extortion, fraud and forgery.

South Africa has also formed an alliance with European countries and it is the only African country to ratify the European cybercrime treaty, which outlaws cybercrime and provides for treaty member states to make laws criminalizing cybercrime and cooperate in the combat against cybercrime.

Kenya (East Africa) – Kenya passed the Communication and Information Act into law in 2008. This law governs and regulates the telecommunications sector in the country. There is no specific provision for the prohibition of cybercrime in the law. The Act only gives the Communication Commission of Kenya the power to protect the right to privacy of all persons. It is worthy of note that section 83U of the legislation prohibits unlawful access to computer systems. Recently during the launch of a computer emergency response team in the country the Minister of Information, Samuel Pohgisio was stated that "as the dependency on ICT increases, identifying and monitoring of risks involved in their use has become an important but challenging task."[12]

---

[11]United Nations Economic and Social Council (UNESCO) website, *Workshop on Legal and Regulatory Framework for the Knowledge Industry*, available at: http://www.uneca.org/codist/codist1/lrf/content/CODIST-1-LRF-Full_Report-en.pdf , 4

[12]All Africa.com website, *Kenya Sets Up Cyber Crime Team*, available at: http://allafrica.com/stories/201107261874.html

Tunisia (North Africa) – "was ranked top of African countries on deployment of ICT in its economy and in development of enabling environment and infrastructure. It enacted the Electronic Commerce law (2000). It covers the areas of application of e-commerce, tax filing, e-banking etc. Tunisia has made remarkable progress in e-payment. It developed an e-payment system called e-EDinar which allows internet sales and purchases and internet banking called CCPNet which allows e-banking activations."[13]

Cameroon (Central Africa) – after Nigeria Cameroon comes in second as the country with the most prevalent cybercrime activities. "A 2010 report by the McAfee cyber security firm cites Cameroon as the world's riskiest destination for internet surfers with more than a third (36.7%) of websites hosted in Cameroon being suspicious (McAfee Inc, 2009). In line with this, the country through its Ministry of Post and Telecommunications and the National Agency for Information and Communication Technologies advanced a bill to parliament that allows them to set up a cyber police force, define major crimes, determine legal procedures to help fight cybercrime. Also, the Cameroon parliament voted a bill to set up a cyber police force to fight the alarming rate of cybercrime in the nation."[14]

CYBERCRIME LEGISLATION AND COOPERATIVE ALLIANCES IN THE UNITED STATES, UNITED KINGDOM AND AUSTRALIA

Having examined the anti cybercrime legislative framework in Africa, we will now have a look at the position in countries with advanced technology such as the United States, the United Kingdom and Australia.

United States of America

Due to being one of the countries with the most advanced computer technologies in the world, it comes as no surprise that the US also has one of the most established legislative and cooperative frameworks on cybercrime. These include:

---

[13] UNESCO article,

[14] E Akuta et al, *Combating Cybercrime in Sub-Sahara Africa: A Discourse on Law Policy and Practice*, available at: http://www.interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al.pdf, 132

- A federal criminal code related to computer intrusions that include a number of federal criminal statutes relating to computer intrusion.[15]
- Sentencing guidelines relating to computer intrusions. [16]
- US ratified the Cybercrime convention in August 2006 and the convention entered into force in the US on 1st January 2007.

In the US there are more than 40 federal statutes that govern the prosecution of computer-related crimes, as well as various state statutes. There are also several key players in the field helping in the fight against cybercrime. These include:

- The Department of Justice
- The FBI
- The Computer Emergency Response Team (CERT)
- Computer Crime Research Centre
- Centre for Democracy and Technology

Key among the US cybercrime responsive alliances is the United States Computer Emergency Responsive Team (US-CERT). US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.[17] This involves a collaborative responsive effort with other CERT or similar organization in the world. There are over 250 CERT organizations worldwide and the US-CERT cooperates with them through the CERT Coordination Centre in coordinating a response to security incidents.

[15] Code is accessible via http://www.gpoaccess.gov/uscode/
[16] Accessible via http://www.ussc.gov/Publications/Guideline_Manuals_and_Amendments/index.cfm
[17] see http://www.us-cert.gov/aboutus.html

United Kingdom

The legislative responses to cybercrime in the UK include:

- The Computer Misuse Act of 1990, which prohibits unauthorized access to computer material, unauthorized access with intent to commit or facilitate commission of further offences and unauthorized modification of computer material.
- The Data Protection Act of 1998 provides for requires organizations to store personal data held by them securely.
- The Privacy and Electronic Regulation (EC Directive) 2003, made to address the problem of spam.
- The UK signed the Cybercrime Convention in 2001 but only ratified it in May 2011.[18]

Key players in the field are:

- Serious and Organized Crime Agency (SOCA) set up to reduce organized crime including cybercrime via its e-crimes directorate. The National High Tech Crime Unit (NHTCU) was amalgamated into SOCA.
- Child Exploitation and Online Protection Centre (CEOP)
- Communications Electronics Security Group (CESG)

Australia

Australia is one of the front runners in the fight against cybercrime with a mixed record of success. Apart from its cybercrime legislation, it's consistently involved in forming alliances with other countries to improve the efficiency in combating cybercrime on a global scale. The main legislation in the country is the Cybercrime Act of 2001. It prohibits the following:

[18] reported via: http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/

- Unauthorized modification of data to cause impairment
- unauthorized impairment of electronic communication
- Producing, supplying or obtaining data with intent to commit a computer offence

Other related legislations and key players are:

- Electronics Transactions Act of 1998
- Spam Act of 2003
- Crimes Act 1914
- Australia CERT[19]

Similar laws have also been put in place in the different states. Recently, Australia introduced new anti cybercrime law bills into its parliament. In the words of the Attorney General Robert McClelland "The increasing cyber threat means that no nation alone can effectively overcome this problem and international cooperation is essential,"[20] The laws once passed aims to improve cooperation with cybercrime organizations overseas allowing for better access by security agencies to overseas information during cybercrime investigations. In the same vein, Australia is currently meeting with the US, Britain, Canada and New Zealand on forging an alliance in responding to global cybercrime and the creation of binding international cybercrime laws.[21]

[19] see: http://www.cert.gov.au/www/cert/cert.nsf
[20] comment reported via:
http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2011_SecondQuarter_22June2011-Strongerlawstotacklecybercrime
[21] reported via: http://www.smh.com.au/technology/technology-news/five-nations-to-discuss-pact-on-cybercrime-law-20110707-1h4wm.html#ixzz1XcPWCsha

CHALLENGES FACED BY AFRICAN COUNTRIES IN LEGISLATING ON CYBERCRIME

One of the main challenges faced by African nations in legislating on cybercrime is the lack of uniformity and consistency in laws (current or proposed) in this field. This is also marred by a slow law making process. While there have been separate efforts by countries or regions to make a head way in this area, the need for uniformity is important to foster more effective cooperative alliances within the continent.

There have been some coordinated efforts within the continent to form cross border alliances in the fight against cybercrime. Examples of these involve efforts by regional bodies such as ECOWAS, EAC, SADC and CEMAC to harmonize laws, organizing training sessions for parliamentary and law enforcement officers and forming partnerships with international organizations. This has seen some success on an information sharing level; however no action has been taken to implement these ideas. The African Union therefore has to take it upon itself to push for the implementation of harmonized laws and cooperative alliances in the continent. The disparity in the cybercrime laws of different African countries is laid bare in the fact that cyber criminals are able to move their activities from Nigeria to Ghana for example, so as to take advantage of loopholes in the legislation.

Another challenge is lack of funding. Harmonization of laws and efforts alone are not adequate to fight cybercrime. There is a need for African governments to realize that cyber attack or defense is a highly technological venture. New and advanced technologies are being developed to aid the perpetration of cybercrime. For example, there are obfuscation programs available to help cybercriminals hide their identities making it difficult to trace the source of these attacks. "In 2009 Kenya sent 18 police officers to the US for in-service training on ways of using modern equipment to detect and investigate cybercrime. This is a laudable move that needs to be encouraged".[22] However, funding is needed to equip law enforcement or relevant agencies in detecting

[22] *Combating Cybercrime in Sub-Sahara Africa* at 134 and 135

these cyber attacks. Adequate funding coupled with the right training is a formula for success and a step in the right direction.

A common trend is the lack of political will by African governments to provide the resources and implement laws prohibiting cybercrime. This is where informational sessions for law makers pointing out the importance of having a legislative framework at the very least are imperative.

LEARNING FROM OTHER COUNTRIES (AUSTRALIA AS CASE STUDY)

Over the years in Australia, successive governments have enacted various specific laws in relation to computer offences in the Criminal Code Act 1995. "The technological aspects of cyber crime also pose particular challenges to the investigation of crimes against computers or that use communication technologies."[23] As a result, the police have been given the power to obtain relevant evidence needed to prosecute cyber criminals.[24]

The following are some key facts on cybercrime legal framework in Australian law:

- Computer offences are introduced into the Criminal Code Act by the Cybercrime Act of 2001.[25]
- The constitution grants the commonwealth of Australia the power make laws prohibiting offences carried out through the use of computer systems or via a telecommunications service.
- Nonetheless, state and territories laws apply in other state/territories therefore providing a national coverage.

[23] R Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004, 1.
[24] Attorney-General's Department (AGD), *Submission 44 to the House Standing Committee on Communications ,available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44.pdf,* 16; *Telecommunications (Interception and Access) Act 1979* (Cth)*; Crimes Act 1914* (Cth).
[25] Part 10.7 Divisions 477 and 478 of the Criminal Code

- Computer offences are often combined with crimes relating to identity fraud such as fraud and forgery.
- The Australian Federal Police expressed the view that criminal offences to tackle cyber crime are sufficient, the difficulty lies more in enforcement and the trans-national nature of most cyber crime.[26] In the same vein, The AGD also said that while some aspects of the law and law enforcement could be strengthened existing Australian laws are appropriate.[27]
- Australia is party to around 25 bilateral treaties on mutual assistance in criminal matters.[28]
- The recently introduced Cybercrime Legislation Amendment Bill 2011 will enable Australia to accede to the Budapest Cybercrime Convention. The aim is to strengthen Australia's cybercrime laws and work towards achieving uniformity in international cybercrime laws.
- A recent study by Microsoft analyzing the Australian cybercrime laws against the provisions of the convention found that there was a strong alignment between both legal frameworks.[29] Microsoft Australia stated in its study that: "… Australia has demonstrated a solid commitment to robust legislation … Australia has already been playing an important role in achieving regional and global consistency. It is effectively functioning as a policy bellwether for the region".[30]

---

[26] Australian Federal Police *Submission 44 to the House Standing Committee on Communications* ,available at, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub25_1.pdf, .9.
[27] AGD, *Submission 44*, available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44_1.pdf, 7
[28] AGD, *Supplementary Submission 44.2*, available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44_2.pdf, 4.
[29] Microsoft Australia, *Submission 35 to the House Standing Committee on Communications*, available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub35.pdf. 7.
[30] Microsoft Australia, *Submission 35*, 8.

RECOMMENDATIONS

Having looked at the current legislative framework in Africa and its equivalent in other key countries outside the continent, the following recommendations are made:

- That African countries, through the various regional bodies, work towards implementing laws that are uniform coupled with a consistent approach in tackling or responding to cyber attacks. Keys areas that must form part of this law reform are the need for laws addressing identity theft and laws protecting the privacy of individuals and organizations in Africa.
- That each country or region set up or nominate an appropriate agency to develop clear and defined procedures for gathering cybercrime information and data. This should include agreements on the manner of information sharing between government agencies and relevant industry bodies. This could take the form of a Computer Emergency Response Team or a Computer Security Incidence Response Team (CERT/CSIRT).
- That each country or region establishes a cybercrime reporting agency to provide a portal or system of reporting cybercrime incidents online, via the telephone or face to face. This incident reporting system should be made available free of charge to both individuals and small/medium or large scale businesses. This can also be implemented through CERT/CSIRT organization.
- That the various law enforcement agencies set up working groups to ensure that information is shared across borders to provide an effective means of successfully prosecuting cybercrime.
- On an ongoing basis, adequate and up to date training should be provided to law enforcement officers to ensure that they are well equipped to responding to cyber attack prosecution. This should be done in liaison with IT and industry experts and organizations within and outside Africa.
- That various governments through the relevant bodies set up national or regional strategies for public awareness on prevention and control of cybercrime.

CONCLUSION

In conclusion, this paper has been able to identify the need for a harmonized legal framework in responding to the problem of cybercrime in Africa. Promulgating relevant laws is one step in the right direction. African governments also need to recognize the importance of forming cooperative alliances in the fight against cybercrime. Cybercrime is a unique type of crime mainly due to the fact that it is global in nature. It is a crime that can transcend beyond boundaries and one that possesses ability to have huge economic impact on victims. It is not a crime that stays within borders but one that brings the harsh realities that need to be addressed and responded to on the same level

BIBLIOGRAPHY

- Microsoft Australia, *Submission 35 to the House Standing Committee on Communications*, available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub35.pdf
- Australian Federal Police *Submission 44 to the House Standing Committee on Communications* ,available at, http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub25_1.pdf
- Attorney-General's Department (AGD), *Submission 44 to the House Standing Committee on Communications ,available at: http://www.aph.gov.au/house/committee/coms/cybercrime/subs/sub44.pdf*
- R Smith, *Impediments to the Successful Investigation of Transnational High Tech Crime*, Trends and Issues in Crime and Criminal Justice No. 285, Australian Institute of Criminology, October 2004.
- Sydney Morning Herald Online, news reported via: http://www.smh.com.au/technology/technology-news/five-nations-to-discuss-pact-on-cybercrime-law-20110707-1h4wm.html#ixzz1XcPWCsha
- Comment reported on Emergency Management Australia website via: http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2011_SecondQuarter_22June2011-Strongerlawstotacklecybercrime
- Computer Emergency Response Team website: www.cert.gov.au

- The Register Online, news reported via: http://www.theregister.co.uk/2011/05/25/uk_ratifies_cybercrime_convention/
- E Akuta et al, *Combating Cybercrime in Sub-Sahara Africa: A Discourse on Law Policy and Practice*, available at: http://www.interesjournals.org/JPGDS/pdf/2011/May/Akuta%20et%20al.pdf
- All Africa.com website, *Kenya Sets Up Cyber Crime Team*, available at: http://allafrica.com/stories/201107261874.html
- United Nations Economic and Social Council (UNESCO) website, *Workshop on Legal and Regulatory Framework for the Knowledge Industry*, available at: http://www.uneca.org/codist/codist1/lrf/content/CODIST-1-LRF-Full_Report-en.pdf
- Foreign Policy News website, 24 March 2010, available at: http://www.foreignpolicy.com/articles/2010/03/24/africas_cyber_wmd
- I E Quist, *Addressing Emerging Cybercrime Trends in West Africa: The Ghana Police Perspective*, available at: http://waccs.web.officelive.com/Documents/Addressing%20Emerging%20Cybercrime%20Trends%20in%20West%20Africa%20-%20The%20Ghana%20Police%20Perspective%20by%20Isaac%20Quist.pdf
- Wikipedia website, *Spam (Electronic),* available at: http://en.wikipedia.org/wiki/Spam_%28electronic%29
- ehow website, *What is Website Cloning*, available at: http://www.ehow.com/facts_6816849_website-cloning_.html
- Australian Communications and Media Authority (ACMA), *A Consumer's Guide to Spam*, available at: http://www.acma.gov.au/webwr/_assets/main/lib100234/fs%20163%20-%20consumer%20guide%20to%20spam.pdf
- PhishTank website – January 2011 stats, available at: http://www.phishtank.com/stats/2011/01/
- Australian Competition & Consumer Commission, ScamWatch website, available at: http://www.scamwatch.gov.au/content/index.phtml/tag/Nigerian419Scams

- American Bar Association website, *Whitecollar criminal statutes*, 25 June 2002, 1, available at: http://apps.americanbar.org/buslaw/newsletter/0001/materials/whitecollar.pdf
- W Jayawickrama, Cyber Crime – *Threats, Trends and Challenges*, Computer Security Week 2002 – Brisbane