http://go.warwick.ac.uk/jilt/2009_1/olowu

Journal of Information, Law & Technology

Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa[1]

Dr. Dejo Olowu
Barrister & Solicitor (Nigeria)
Professor of Law & Acting Director
School of Law
Walter Sisulu University, South Africa.
djolowu1@yahoo.co.uk

This is a **refereed article** published on 28 May 2009.

Citation: Olowu, D., 'Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa', 2009(1) *Journal of Information, Law & Technology (JILT)*, <http://go.warwick.ac.uk/jilt/2009_1/olowu>

[1] This paper was presented at the CyberCrime Africa Summit Successful Strategies to Combat, Prevent and Investigate Cyber-Crime in Africa, Johannesburg, South Africa, 10-13 November 2008. I acknowledge the support of the summit organisers and, in particular, Mr. Sizwe Snail.

Abstract

As the world marches deeper into the unknown passageway of digital revolution, it is becoming apparent that the tremendous benefits of the internet age are being challenged by the formidable menace of cyber-crime, not the least in the African region. While African States vary in the degree to which their economies and peoples are affected by cyber-crime, there is no gainsaying the fact that the collective ability of African States to track and trace the source(s) of any criminal use of the internet or cyber-attacks on infrastructures, economies or individuals is central to the deterrence of such attacks as well as to long-term survival of these States. An acknowledged and concerted ability to respond to cyber-crimes, to track, trace and apprehend domestic and international cyber-criminals can forestall future attacks through fear of severe penalties. This paper highlights the general weakness or inertia of African States in curbing the menace of cyber-crimes and particularly draws attention to the inherent limitations and failures in current domestic legal responses to cyber-crime. Acknowledging the complex and often extra-territorial nature of cyber-crimes, this paper makes a case for a redefinition of the notion of sovereignty and its implications for the recurring decimal of cyber-crime against African economies and societies. Extrapolating from learned experiences around the world, this paper explores the trajectory of a regional normative initiative that would streamline and synergise the efforts of African States in responding to the phenomenon of cyber-crimes.

Keywords

Cyber-crimes; Africa; legal responses; jurisdictional limitations; regional collaboration.

1. Introduction

In the world of the twenty-first century, economic and political barriers are being lowered and technological advancements in communications and commerce are on the increase, affirming that ours is indeed a globalised world. The globalisation phenomenon is increasingly producing immense opportunities for students, researchers, tourists, and business people, and at the same time fuelling economic growth and development. However, among those taking advantage of opening up societies and borders are criminals who engage in the human trafficking and drug trade, arms smuggling, fraud, counterfeiting, and other financial crimes, and increasingly in computer crimes (Bequai, 1997, p.25; Bequai, 2001, p.475; Tyson, 2007, p.81). This presents a grave predicament so much that today, it is estimated that international crime is a $1 trillion business (Hale, 2002, pp.5-6; Sullivan, 2004; Swartz, 2004). Cyber-crime has indeed reached epidemic proportions. In a relatively recent survey, more than 90 percent of the respondent corporations and government agencies reported computer security breaches at one time or the other. It is commonplace for disgruntled employees and hackers to commit many cyber-crimes while others are committed by crooks using the Web to perpetrate auction fraud, identity theft and other scams. Financial institutions invariably get hit hard as identity thefts reportedly cost them $2.4 billion in losses and expenses in 2000 alone (Hansen, 2002, p.1).

Hardly any organisation or anyone is immune to the possibility of cyber-crime. What more? Within 2008, the World Bank Group's computer network had 40 of its servers compromised by

cyber-criminals six times while French President Nicolas Sarkozy's personal bank account suffered intrusions that resulted in considerable financial loss to him within the same year.[2] What more? The Georgia Tech Information Security Centre (GTISC) published its GTISC Emerging Cyber Threats Report for 2009, warning that there will be an increase in the sophistication of cyber-crime and outlining the five areas of higher threats to be malware, botnets, cyberwarfare, VoIP, and mobile devices (GTISC, 2009, p.1).

Numerous writers, policymakers and law enforcers have called for stringent and innovative laws to prevent and punish computer crimes. Others fear that such initiatives will compromise human rights. Yet, others want legislation to make computer software companies liable for damages caused by their software-security failures. Responding to the challenges of cyber-crime has indeed engendered a cacophony of ideas.

What exactly is cyber-crime? Are all unlawful activities involving computers and the Internet simply to be classified as 'criminal'? Can cyber-crime also engender civil liability? In light of the transnational implications of cyber-crime, how are states responding to the problem and what practical implications do such responses portend for African states?

An attempt is made to tackle the foregoing plethora of questions relating to the problems arising out of efforts at formulating appropriate legal responses to cyber-crime. While the focus is on the African region, this paper nonetheless draws on the experiences and existing frameworks of other world regions as much as necessary.

2. Curbing Cyber-Crimes: Some Conceptual Dilemmas

One might not find the word 'cyber-crime' in contemporary lexicon, but it is a very popular term describing the criminal activities related to cyberspace or the cyber-world. While scholarly consensus on a single definition of the terminology is yet to be achieved, it would appear that writers and law drafters are more comfortable with describing various elements constituting cyber-crime than in defining it. According to the Council of Europe (COE), for instance, cyber-crime involves 'action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data….'[3]

Casey offered another dubious definition of cyber-crime as 'any crime that involves computers and networks, including crimes that do not rely heavily on computers' (Casey, 2004, p.8). Other authors have resorted to simply describing the role of computers and the internet in the promotion of crime (Collier, 2004, pp.322-328; Bazelon, Choi, and Conaty, 2006, p.261-264) while others sought to classify cyber-crime into computer-related and content-based species (Walden, 2003, p.295; Lewis, 2004, pp.1355-1356) or between 'true cyber-crime'– dishonest or malicious acts that would not exist outside online environment and 'e-enabled crime' – criminal acts already known to the world but now promoted through the internet (Burden, Palmer, and Lyde, 2003,

[2] Nkanga, E, 'Cybercrimes Hit World Bank', This Day, Thursday 16 October 2008; Moscaritolo, A, 'French President Sarkozy's Bank Account Hacked', SC Magazine, 20 October 2008.
[3] Council of Europe (COE), Convention on Cybercrime, 2001, preambular paragraph 8 <http://conventions.coe.int>.

p.222). Yet, there have been debates about whether unlawful activities involving computers and the internet should be classified as crimes or civil wrongs (Barton, and Nissanka, 2003, p.401).

These theoretical problems are further complicated by the emergence of new terminologies, novel dimensions and innovative tools. The threat landscape once dominated by the worms and viruses unleashed by irresponsible hackers and script-kiddies is now ruled by a new breed of cyber-criminals. Cyber-crime is motivated by fraud, typified by the bogus emails sent by 'phishers' that aim to steal personal information. The tools driving their attacks and fuelling the black market are crimeware - bots, Trojan horses, and spyware (Lininger, and Dean, 2005, p.7).

The explosive growth of online fraud has made 'phishing', and to a lesser extent 'pharming' part of nearly every Internet user's vocabulary in most recent time. Phishing and pharming are two popular forms of fraud that aim to dupe victims into believing they are at a trusted Web site such as their banks, when in fact they have been enticed to a bogus Web site that intends to steal their identity and drain their financial resources (Brenner, 2004, p.6; Chawki, and Abdel-Wahab, 2006). While spyware has occupied the centre stage of late, it is but one of the tools behind today's rash of cyber-crime. Deceptive Trojan horses, multi-purpose bots, and spyware programmes form the crimeware arsenal of today's hackers and are regularly bought and traded on the illicit market. The price tag of crimeware is often based on their ability to steal sensitive data such as bank and credit cards while remaining undetected by the victim. Whatever the case, it is obvious that cyber-crime may be targeted against natural persons, property, or institutions.

The definitional quandary surrounding 'cyber-crime' is more than being just theoretical and goes to the root of the broader dilemmas in the field of curbing it. What, for instance, is 'cyberspace' where much of cyber activities take place? Who is in charge of that territory? Gibson (1984) has convincingly demonstrated that 'cyberspace' is a convenient but fictitious notion describing 'the network of networks' constituting the internet, the communication and services provided through it. This basic understanding explains why it has been extremely difficult if not impracticable for States and their law enforcement agencies to trace, apprehend and punish perpetrators of cyber-crimes beyond their respective territories because by the very nature of international law, a State's sovereignty is limited to its territory, subject to very few traditional exceptions that did not envisage the internet age (Bequai, 1996, p.22; Johnston, and Post, 1996, p.1367). As our experience shows, while numerous states have put in place wide ranging legislation to stem the tide of cyber-crimes within their territories, applying such domestic legislation abroad has proven to be a cumbersome act where there is no reciprocity among States.

This is where this paper makes its entry point: the increasing recognition among judges, policymakers, and scholars in many countries around the world to reconstruct territorial jurisdiction in a way that tackles the cross-border and complex nature of cyber-crimes, and the profound implications of these normative trends for the African region.

3. Contextualising Cyber-crimes in Africa

Cyber-crimes indeed constitute a worldwide problem and no State is beyond vulnerability. However, to understand why cyber-criminality in Africa differs from other areas in the world, one should understand the state of information security in this region which is affected by factors such

as the growth of user base, poor security awareness, lack of training for law enforcements, lack of regulations and weak cross-border collaboration.

Africa has seen a phenomenal growth in Internet connectivity in recent years. With the increasing availability of broadband connections and the decrease in subscription fees, the number of new online users in Africa is outpacing the rest of the world. According to Internet World Stats, Internet use in Africa had reached 2.3 per cent of the total worldwide use by December 2007.[4] Africa's internet usage from 2000 to 2007 increased by 423.9 per cent compared to 180.3 per cent for the rest of the world. This high number of users in Africa has made the Internet a popular means of communication as well as opening new opportunities for online enterprise, and likewise, a similar increase in cyber-criminal activities requiring an increased effort across the region to strengthen the information infrastructure, educate users in security awareness, and develop cyber-crime regulations.

The potential for internet abuse is even greater in and for Africa. Due to the lack of security awareness programmes or specialised training for the law enforcement agencies, many online users are becoming victims of cyber-crime attacks and the incidence of successful attacks is increasing with impunity. So much has been written about staggering incidents of cyber-based fraud emanating from African states and it serves no useful purpose revisiting the wealth of literature on the subject.

Further complicating the incidence of cyber-crimes is under-reporting. Whereas Hale (2002, pp.5-6, 24-26) asserted that globally, only about ten per cent of all cyber-crimes committed are actually reported and fewer than two per cent result in a conviction, against the backdrop of ill-trained police and security agents and in the absence of cyber-crimes records, one can only conjecture that the statistics of reporting and conviction will inevitably be lower for Africa (Ojedokun, 2005, p.14).

It will suffice to mention, however, that while the cocaine cartels and other criminal organisations in Europe and Latin America may be better known, criminal organisations are becoming big business in Africa too. Of course, at the mention of Africa-based criminal organisations, the ones that come to stereotyped minds are Nigerian drug couriers, which are indeed among the most sophisticated in the world, and the various financial scams known as '419' frauds (Oriola, 2005, p.239). However, it will be foolhardy to assert that criminal enterprises in Africa are limited to Nigeria. The South African Police estimate that their country is home to more than 190 criminal organisations, many of which are sophisticated and international in scope. Various African states are fast becoming safe havens for drug traffickers, for gun runners and for cyber-criminals (Mutume, 2007, p.3).

The investment in ICT infrastructure in Africa is becoming extensive, especially in the richer States but there is more to network infrastructure security than the initial implementation of the system – upgrades and ongoing maintenance must be taken into account. While financial institutions and corporations in Africa would often assert they have the best and most expensive security systems that guarantee the protection of customers' deposits and investments, financial

[4] Internet World Stats, 'Internet Usage Statistics for Africa: Africa Internet Usage and Population Stats' <http://www.internetworldstats.com/stats1.htm>

experts are discovering that over the past few years, banks in the region lost approximately one billion dollars to organised cyber-crimes.[5]

Additionally, most banks in the region are vulnerable to phishing attacks, which should send a strong warning signal to allocate more investments to ICT security systems and awareness. Investments in information infrastructure have increased the value of e-commerce and e-governments and have created great opportunities for small businesses in the region, thus helping with the unemployment problem. However, not all investments are directed toward including and implementing security solutions while developing the infrastructure. The prevailing wisdom would seem to be business first, security later.

Furthermore, internet service providers (ISPs) in the region have been rapidly deploying broadband Internet connections without implementing security solutions – a major problem in the region. Without sufficient security policy to protect their businesses against spammers, most ISPs in the region are blacklisted and marked as sources of spam by the vigilant regime of cyber security in the US and the UK (Leyden, 2008). A culture of information security must therefore become foremost in Africa as no African State is immune to cyber-crimes: the Zambian government sites have been attacked by hackers, an incident that cost it some loss of public confidence (Ojedokun, 2005, pp.13-15).

Information security awareness is crucial for combating cyber-crimes. In Africa, there is a significant lack of security awareness among users, whether the general public or organisations and enterprises. Comparing security awareness in Africa to Europe or the US, one would see far less effort being made to raise awareness among users. One of the major factors that make information security awareness programmes ineffective in the region is that most ICT security awareness programmes available are in English, making them difficult to implement in a region where the overwhelming majority are French, Arabic, or Portuguese speakers. This lack of security awareness is also a big problem inside ICT companies in the region as most ICT decision makers in Africa are not aware of the cyber-crime problem, thinking Africa is still immune. Besides, they do not have good security policies.

Poor security awareness means that investments to fight cyber-crimes are minimal, leaving businesses across Africa vulnerable to cyber-crimes or online attacks. The African continent is in dire need of strong ICT security awareness training, targeting native speakers to educate users, employees and law enforcers to understand the risks and prevent attacks.

Many watchers are warning that Africa is becoming a major source of cyber-crimes; for example, Nigeria is ranked as the leading State in the region as the target *and* source of malicious internet activities; and this is spreading across the West African sub-region (Ribadu, 2007; Mazzitelli, 2007, p.1071). Egypt is also reputed to be one of the most phished countries in the world with about 2000 phishing incidents, followed closely by other countries in the region such as South Africa (Ojedokun, 2005, p.14; Viljoen, 2007, p.25), and lately Ghana.[6] It is not hard to see that cyber-crimes are increasing in the region due to the growth of user base with poor security awareness and the lack of adequate regulations.

[5] See, e.g., 'Nigerian Banks Lost NGN 7.3 Billion to Cyber Criminality', Economic Confidential, 28 August 2008.
[6] Yarney, J 'Africa Confronts CyberCrime' <http://www.itworld.com>

Another important factor making Africa a source and target of much cyber-criminal activity is the growth of international banking and money-laundering. The unique opportunities of a quickly developed financial infrastructure allowing anyone to transfer monetary fund to any State, anonymously and through tangled routes have caught the attention of cyber-criminals. Electronic transfers are an efficient tool for concealing sources of money intakes and laundering illegally earned money. There are many well-known online money laundering cases involving victims in Africa who were tricked in order to steal their identity or transfer money from their real accounts using phishing and scams (Ojedokun,, 2005, p.14; Oriola, p.238).

Cyber-criminals also attack popular sites in the region like many social networking websites. Many corporate employees and home-based internet users are into social networks. Studies have now revealed that social networking can open a backdoor into corporate ICT platforms, putting businesses and individuals at risk of information compromise, identity theft and other malicious attacks. Cyber-criminals are looking for sites that have many users with poor security awareness to infect, and social networking sites are an excellent place to hunt (Bazelon, Choi, and Conaty, 2006, p.259).

Like other world regions, Africa is home to numerous social networking sites which can be used by hackers to infect users with malware or redirect them to phishing websites, stealing passwords, accounts and opening security holes in the victim's machine. Local social networks in Africa are not secured enough to protect users' or members' privacy and sensitive information. One frequently hears reports of new cyber-crimes in Africa that happened to someone using social networking.

Users in Africa also utilise international social networks such as *Facebook* and *Myspace* for communications, friendships, blogging and other activities that, if not taken with caution, can lead to identity theft and malicious activities against home users and employees in both private and public sectors as long as there is no policy. The risk is very high not only in social networks but also in peer-to-peer networks, Web 2.0, chatting and popular applications that can be exploited. Again, the need for security awareness training in Africa is great.

What is driving the menace of cyber-crimes in Africa? Most African countries are contending with high unemployment problems; the numbers are increasing daily and will promote the growth of cyber-crimes in the region if not comprehensively addressed. According to the World Bank, 'African States are to face great challenges; they have to work by themselves to generate 100 million new job opportunity by 2020 or the region's instability will increase' (World Bank, 2008, p.15). Statistics reveal that the unemployment rate is very high among youth in the region, most of whom are university graduates with computer and Internet competency. Even if they do not have access to Internet at home, cyber-cafés are readily available throughout the region at relatively low rates for Internet access. All these factors combine to create a new generation of local hackers and cyber-criminals. Most of these people are script kiddies working for financial motives. They do not have deep programming knowledge like experienced hackers who can create their own malware or viruses, but they take advantage of many websites available for free that help them understand the basics behind hacking techniques with links to underground hacking sites and even

free tools to use. Script kiddies represent the biggest risk in Africa; they have time on their hands, low cost Internet access and cyber-cafés that can be infected to launch their attacks easily.

Added to the above is the reality that most African States do not have Internet-specific laws, although some are beginning to adopt these laws. A few countries in the region are trying to shape new legislation and legal definitions for cyber-crime, such as Botswana, Egypt, Lesotho, Mauritius and South Africa, but there is still need for more specific laws for cyber-crime activities. It may be worth mentioning that the Nigerian Computer Security and Critical Information Infrastructure Protection Bill submitted to the country's National Assembly in 2005 has stagnated ever since.

In many of the few countries with specific legal framework against cyber-crimes, the existing laws lack the potential to tackle the transnational aspects of the phenomenon. For instance, the Nigerian draft Bill mentioned above limits all powers of search, arrest, prosecution and punishment to the extent of the country's territorial jurisdiction.[7] The South African approach in the Electronic Communications and Transactions Act, 2002, does not hold better as the powers of 'cyber inspectors' to search, seize or arrest only envisage cyber-crimes within the South African territory.[8]

Due to the style of criminal justice and law enforcement techniques in Africa, most countries in the region, including Burkina-Faso, the Gambia, Ghana, Kenya, Senegal, and Zimbabwe are using emergency laws and *ad hoc* approaches instead of establishing ascertainable cyber-crime laws and policies against the phenomenon. Other countries in the region are trying to prevent such activities by blocking access to certain websites. Regular laws and emergency laws in Africa are not designed specifically to deal with cyber-crimes, and there is no definition for such activity inside the statute books.

Nigeria comes into view as the manifestation of one of the most extra-legal approaches to cyber-criminality. A State whose law enforcement and security agencies are yet to fully shed the military culture of repression, it has become routine for police officers and other security agents to swoop on cyber-cafés and arrest all users of the internet in such cyber-cafés without considering that there may be honest and innocent patrons. In a country where an accused person is hardly afforded the safeguards of criminal procedures, the incessant practice of swooping on cyber-cafés has opened further doors for the corrupt enrichment of police and security agents. However, both actions are neither effective nor sustainable. Also, that sort of action may put innocent people in jail with cyber-criminals.

Lack of regulation invariably equals lack of law enforcement training, tools and techniques used to investigate cyber-crimes. Most African countries also do not have specific laws for cyber-based intellectual property violation. According to an empirical study, several African States rank high in virus infection (Symantec Threat Report, 2007). It is well known that viruses spread through files which can be downloaded or distributed through peer-to-peer networks or through pirated software, and this indicate that African States also rank high in cyber-based intellectual property violations and software piracy.

[7] Sections 23-31.
[8] Electronic Communications and Transactions Act, 2002, ss. 80-84.

Grossly inadequate as the landscape of laws against cyber-crimes portends in Africa, the scenario of inadequate legislative and policy frameworks also manifests at the wider regional level. Apart from isolated pockets of diplomatic interactions at sub-regional levels, such as the one-day meeting of the Ministers of Telecommunications in the Economic Community of West African States (ECOWAS) sub-region in October 2008,[9] there has been no specific continent-wide agenda for establishing concrete collaborative initiatives against cyber-crimes.

While African States indeed have the primary responsibility to tackle cyber-crime single-handedly and handle the complex challenges arising from cyber-criminality, a reality that brings us to the point of examining the dimension of multinational legal responses to overcome the impediment of jurisdictional limitations to anti-cyber-crime efforts.

4. Collaborative Legal Responses to Cyber-crimes: A Survey

Today, cyber-crimes and cyber security have become perhaps some of the most critical issues for almost all governments that are significant actors on the global economic field. For many informed governments, therefore, it has become a matter of life or death – because the survival of their economies now revolves on the dynamics of ICT. ICT is now accepted, not only as the common currency, but indeed, represents the centre of gravity of the new world and new economy of the twenty-first century.

Against the backdrop of the massive negative consequences of cyber-crimes, there have been various legal and policy interventions by various inter-governmental institutions in recent times, in particular, from the United Nations, the Council of Europe (COE), and the Group of Eight Industrialised States (G-8). It is noteworthy that all their initiatives to date were borne out of the stark realities of singularly fighting a phenomenon that cuts across multiple national frontiers (Pounder, 2001a, p.311; Nykodym, and Taylor, 2004, p.390; Kshetri, 2005, p.541). I shall not revisit literature on existing models but will only consider under this segment their most significant aspects for our present discussion.

4.1 United Nations (UN)

Being the largest and most prominent inter-governmental organisation and assembly of sovereign States, it would have been expected that the United Nations (UN) would be in the vanguard of collaborative initiatives against cyber-crimes. However, the reality is that the UN has been quite lethargic in assuming leadership of any global anti-cybercrime agenda, preferring to serve as 'an impartial overseer' (Nykodym, and Taylor, 2004, p.391). To its credit, the UN General Assembly adopted two notable resolutions on the subject of cyber-crimes.[10]

While both Resolution 55/63 (2000) and Resolution 56/121 (2001) contained admonitions to States to take initiatives in the areas of strengthening anti-cyber crime laws, training of law

[9] See 'ECOWAS Telecommunications Ministers Adopt Texts on Cyber Crime, Personal Data Protection', Standard Times, 17 October 2008, p. 7.
[10] 'Combating the Criminal Misuse of Information Technologies', UN GA Resolutions 55/63 (2000) and 56/121, 19 December 2001.

enforcers, and promoting public awareness to prevent and combat cyber-crimes, the two instruments emphatically urged States to cooperate in establishing joint legal regimes for combating cyber-crimes; information sharing and mutual legal assistance in the investigation, apprehension and prosecution of cyber-criminals.[11]

Although these two resolutions resonate with the calls for concerted global action against cyber-crimes, they are nothing more than exhortations as resolutions of the UN General Assembly have no binding force on member States (Boyle, 2006, pp.142-143).

4.2 Group of Eight (G8)

The Group of Eight industrialised States, otherwise known as the 'G8', comprises Canada, France, Italy, Germany, Japan, Russia, the UK, and the US. Statistically, the G8 is reputed to jointly hold 48 per cent of the entire wealth of the world,[12] a fact that identifies the G8 as an iconic organisation that could lead the formulation of global collaborative legal agenda against cyber-crimes. While the G8 has commendably been active in initiating a transnational arrangement for computer experts, establishing forensic and ethical principles for computer usage in situations where digital evidence obtained from one State requires authentication in the courts of another State, and making proposals for tracking cross-border criminal communications (Sussman, 1999, pp.451, 481; Westby, 2003, pp.103-4; Nykodym, and Taylor, 2004, p. 91). Apart from technical initiatives, however, the G8 has not been able to come up with any legal framework specifically addressing cyber-crimes, even among its members.

Promising as the G8's initiatives might have been, the organisation's capacity is greatly limited by its inability to enlist the participation of the weaker and poorer States which are often safe havens for all sorts of cyber-crimes.

4.3 Council of Europe (COE)

After many years of rigorous debates, planning and drafting, the COE, which consists of 44 member states, including the entire European Union (EU), adopted the Convention on Cybercrime in Budapest, Hungary, on 23 November 2001, a treaty defining several acts that would constitute cyber crime offences. While numerous scholars have examined the making, progress and challenges of this treaty, there is no intention to use this medium for a critique of the COE treaty. It suffices to assert that the COE Convention on Cybercrime (CCC) proved to be a piece of groundbreaking treaty in the field for three reasons:

(a) against the backdrop of the controversy surrounding what amounts to 'cyber-crime', the CCC describes and prohibits a wide range of conducts that each State Party should proscribe. Among these are intentional and serious computer hacking, illegal interception, forgery, fraud, child pornography, intellectual property infringement, and aiding or abetting any of these acts;[13]

[11] Ibid, paragraphs b, c, f, and g.
[12] G8 Information Centre, 'What is the G8?' <http://www.g7.utoronto.ca/what_is_g8.html>
[13] Sections 2-11.

(b) in order to ensure that the initiatives against cyber-crimes are not abusive or arbitrary, the CCC includes description of a wide range of human rights and procedural safeguards that must inform national law enforcement and investigative mechanisms in the jurisdictions of State Parties;[14] and
(c) in response to the inherent weaknesses in sole reliance on national legal approaches against cyber-crimes, the CCC includes several provisions emphasising international cooperation, mutual assistance and information sharing in investigating, arresting, prosecuting and punishing cyber-criminals.[15]

Since the treaty came into force on 1 July 2004, it has garnered a total number of 23 ratifications and 22 signatures from States within and outside the Council of Europe.[16] It is significant to note that while Canada, Japan, and the United States, countries that have notable domestic legal frameworks against cyber-crimes enlisted their interests to be participants in the framework afforded by the CCC, only South Africa is a signatory to the treaty from the entire African region.

Even though it was never the intention of the initiators of the CCC that its coverage should spread all over the world, there is no gainsaying the fact that the treaty portends unmistakable implications for the African region in terms of a model framework and, in the absence of a regional treaty on the subject, as a possible platform to drive anti-cyber-criminality across borders in Africa. I shall reflect more on this proposal in the next segment.

4.4 African Union (AU)

While most international and regional organisations have made visible efforts to encourage cyber-security awareness at the domestic level, as of today, there has been no regional initiative at the level of the African Union (AU), to address the problem of cyber-crimes. Further, in pursuance of its mandate for the harmonisation of national legal frameworks against cyber-crimes, Interpol's African Working Party on Information Technology Crime Projects is trying to persuade the African states to sign and ratify the Convention on Cybercrime, albeit with no tangible outcome to show for the efforts.

From the foregoing discussion, it becomes apparent that despite active international co-operation on cyber-crimes, Africa remains an insignificant actor in the global scheme of legal approaches against the problem. Apart from the obvious apathy among majority of African States to critically engage the cyber-crime phenomenon in a cogent way, one formidable possibility to formulating a comprehensive regional agenda against cyber-crimes could be the question of limited jurisdiction to pursue cyber-criminals across borders. How then should Africa address this challenge? What are the ways forward?

5. Tackling Cyber-crimes in Africa: Issues and Strategies

[14] Sections 16-22.
[15] Sections 23-25.
[16] Council of Europe, 'Convention on Cybercrime, ETS No. 185, Status as of 25 October 2008' <http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=&DF=> .

While national legal frameworks against cyber-crimes may be effective within national borders, however, if legal controls are to be effective beyond borders, the harmonisation of domestic laws at a regional level becomes imperative. At a glance, the normative and policy frameworks against cyber crimes in Africa present a scenario of cacophony and discordant initiatives. Although there have been numerous national approaches around the continent attempting to create a stable online environment domestically, the approaches have been few, isolated and uncoordinated. Some of these approaches also conflict beyond national borders and disputes often arise in the process of cross-border arrest, prosecution and punishment where such a process is pursued at all.

In light of the many challenges identified in the experiences of other inter-governmental organisations concerning the subject of cyber-crimes, it would appear that two options are available for Africa's engagement with the menace. One, African States could decide to accede into the CCC while they are considering the possibility of a cyber-crime treaty tailored for Africa. Ratifying the CCC is particularly commendable for African States because throughout the treaty, multiple provisions are included that indicate where States may have divergent treatment of the procedural or substantive legal provisions. These were included on matters that were recognised by the Convention's drafters as possible sources of conflicts among States (Pounder, 2001b, pp.382-383). Additionally, the Convention allows for any nation at the time of signing or at ratification or accession, to submit declarations or reservations with respect to obligations under any provision of the Convention.[17] In the alternative, African governments could begin to engage the option of an immediate formulation of an Africa-specific anti-cybercrime treaty similar to what obtains under the COE regime.

Admittedly, a State that exercises jurisdiction in a self-centred manner will not only contravene rules of international law but may also upset the international legal order and generate reprisals in the attempt to track and prosecute cyber-criminals. This is where African States will have to collectively take a stance that will be beneficial for the entire region. Since African States have in the past expanded their jurisdictional reach in matters such as peer review, conflict resolution, and human rights protection, there should be no obstacle to extending this trend of pan-African approach to cyberspace. This idea seeks a move toward a rule calling for 'universal jurisdiction' over cyber-criminals in all African States based on the cause-and-effect principle and the ubiquitous nature of many cyber-crimes. If such a rule is adopted continent-wide, cyber-criminals would be subject to the jurisdiction and differing laws of every African State whose government, economy or people have suffered detriment.

It will therefore appear that an integrative pan-African approach concerning cyber-criminality may be the only viable way to effectively combat the phenomenon. To this end, the African Union (AU), through its numerous technical agencies and commissions could assume responsibility for designing the framework for a continent-wide legal approach, after all, responding to this continent-wide challenge, even though not specifically mentioned in its founding instrument can be read into it. According to the Constitutive Act of the AU, 2001, the objectives of the AU are to:

> (a) achieve greater unity and solidarity between the African countries and the peoples of Africa;

[17] Articles 4(2), 6(3), 9(4), 10(3), 11(3), 14(3), 29(4), 41(1) and 42, CCC.

(b) defend the sovereignty, territorial integrity, and independence of its Member States;
(c) accelerate the political and socio-economic integration of the continent;
(d) promote and defend African common positions on issues of interest to the continent and its peoples;
(e) encourage international cooperation, taking due account of the Charter of the United Nations and the Universal Declaration of Human Rights;
(f) promote peace, security**,** and stability on the continent;
(g) promote democratic principles and institutions, popular participation and good governance;
(h) promote and protect human and peoples' rights in accordance with the African Charter on Human and Peoples' Rights and other relevant human rights instruments;
(i) establish the necessary conditions which enable the continent to play its rightful role in the global economy and in international negotiations;
(j) promote sustainable development at the economic, social, and cultural levels as well as the integration of African economies;
(k) promote co-operation in all fields of human activity to raise the living standards of African peoples;
(l) coordinate and harmonise the policies between the existing and future Regional Economic Communities for the gradual attainment of the objectives of the Union**;**
(m) advance the development of the continent by promoting research in all fields, in particular science and technology;
(n) work with relevant international partners in the eradication of preventable diseases and the promotion of good health on the continent.

Applying the basic rules of statutory interpretation, it is safe to posit that a valid platform exists in the AU's Constitutive Act to mandate its structures to engage in formulating a comprehensive initiative against cyber-crimes in Africa. In terms of resource a constraint, which has always been the mantra in African regional arrangements, the AU could seek technical assistance from the technologically advanced States of the world. Above all, the AU must not play the ostrich game to a menace hurting Africa and Africans.

Beyond the foregoing, African researchers must begin to investigate the problems occasioned by the use of internet in Africa in order to discover the origins, methods, and motivations of cyber-crimes. Policy-makers in governments, business, and law enforcement must react to this emerging plane of challenges. Laws, policies, investigative skills and innovative prosecutorial methods must be developed to apprehend cyber-criminals and prevent future nefarious activities on the internet.

6. Conclusions

The internet has certainly provided unprecedented opportunities to criminals and crooks to perpetrate their acts and, therefore, developing a universal model for tackling cyber-crimes is especially challenging given the transnational nature of ICT. Purely domestic solutions are proving inadequate because 'cyberspace' has no geopolitical borders and more so, computer systems can be stealthily accessed or compromised from any location in the world.

In clear terms, this paper has demonstrated that cyber-crimes in Africa have global repercussions while cyber-crimes elsewhere negatively impact on Africa. It has been shown in this discourse that despite the progress being made, most countries in Africa still rely on obsolete laws to combat cyber-crimes. Establishing and implementing effective and cyber-crimes specific regulations should therefore be of concern to all African governments and peoples.

African States should learn from others and should prepare themselves for the ever-dynamic phenomenon of cyber-crimes in the region as it is not only affecting Africa but also affecting its relations with others around the world. A strong case has been made that African governments must develop security awareness training and education programmes to help minimise the menace of cyber-crimes. Governments and private sectors should invest more in information infrastructure security, employees' awareness and compliance. Beyond that, African government authorities must understand the real risk of cyber-crimes and they should train and re-train their law enforcement personnel for the novel challenges engendered by advancements in ICT.

The African region is already replete with problems, varying from political to economic, and all these issues are likely to increase the number of cyber-criminals. For those who think some African societies may still be immune from cyber-criminality, they should understand that we all inhabit an increasingly connected world. It does not matter where one lives or what one does, reality dictates that every one of us gets affected sooner or later.

Far from being an *ex cathedra* pronouncement on all the dynamics that should inform the control of cyber-criminality in Africa, this paper would have served its purpose if it stimulates further intellectual responses.

References

Books

Buys, R (2004), Cyberlaw @ SA, (2nd Ed.), (Pretoria: Van Schaik Publishers).

Casey, E (2004), Digital Evidence and Computer Crime (St. Louis, MO: Elsevier Press).

Georgia Tech Information Security Centre (GTISC) (2008), Emerging Cyber Threats Report for 2009 (Atlanta, GA: Georgia Tech).

Gibson, W (1984), Neuromancer (New York, NY: HarperCollins).

Reed, C (2004), Internet Law: Texts and Materials, (2nd Ed.) (Cambridge: Cambridge University Press).

Westby, JR (2003), International Guide to Combating Cybercrime (ed.) (Chicago, IL: American Bar Association Publishing).

Lininger, R and Dean, R (2005), Phishing, Cutting Identity Theft Line (Toronto: Wiley).

Chapters in Books

Boyle, A (2006), 'Soft Law in International Law-Making', in Evans, MD, (ed.) International Law, (2nd Ed.), (Oxford: Oxford University Press)

Colliers, D (2004), 'Criminal Law and the Internet' in Buys, R, (ed.) Cyberlaw @ SA (2nd Ed.), (Pretoria: Van Schaik Publishers)

Journal Articles

Barton, P and Nissanka, V (2003), 'Cyber-crime – Criminal Offence or Civil Wrong?', 19(5) Computer Law and Security Report, 401.

Bazelon, DL, Choi, YJ and Conaty, JF (2006), 'Computer Crimes', 43 American Criminal Law Review, 259

Bequai, A (2001), 'Organised Crime Goes Cyber', 20(6) Computers and Security, 475.

Brenner, S (2004), 'Cybercrime Metrics: Old Wine, New Bottles', 9 Virginia Journal of Law and Technology, 6.

Burden, K, Palmer, C and Lyde, B (2003), 'Cyber-Crime: A New Breed of Criminals?', 19(3) Computer Law and Security Report, 222.

Hale, C (2002), 'Cybercrime: Facts & Figures Concerning the Global Dilemma', 18(65) Crime and Justice International, 5.

Johnston, DR and Post, DG (1996), 'Law and Borders – The Rise of Law in Cyberspace', 48 Stanford Law Review, 1367.

Kshetri, N (2005), 'Pattern of Global Cyber War and Crime: A Conceptual Framework', 11(4) Journal of International Management, 541-562.

Lewis, BC (2004), 'Prevention of Computer **Crime** amidst International Anarchy', 41 American Criminal Law Review, 1353.

Mazzitelli, AL (2007), 'Transnational Organised Crime in West Africa: The Additional Challenge' 83(6) International Affairs, 1071-1090.

Mutume, G (2007), 'Organised Crime Targets Weak African States', 21(2) African Renewal, 3.

Nykodym, N and Taylor, R (2004), 'The World's Current Legislative Efforts against Cyber Crime', 20(5) Computer Law and Security Report, 390.

Sommer, P (2004), 'The Future for the Policing of Cybercrime', 1 Computer Fraud and Security, 8.
Ojedokun, AA (2005), 'The Evolving Sophistication of Internet Abuses in Africa', 37 The International Information and Library Review, 11.

Oriola, TA (2005), 'Advance Fee Fraud on the Internet: Nigeria's Regulatory Response', 21 Computer Law and Security Report, 237.

Pounder, C (2001a), 'Cyber crime: the backdrop to the Council of Europe Convention', 20 Computers & Security, 311.

Pounder, C (2001b), 'The Council of Europe Cyber-Crime Convention', 20 Computers & Security, 380.

Sussman, MA (1999), 'The Critical Challenges From the International High-Tech and Computer-Related **Crime** at the Millennium', 9 Duke Journal of Comparative and International Law, 451.

Tyson, D (2007), 'Cyber Crime: A Pervasive Threat', Security Convergence, 81.

Treaties

Council of Europe Convention on Cybercrime, ETS No. 185, 2001.

United Nations, Combating the Criminal Misuse of Information Technologies', UN GA Resolutions 55/63 (2000) and 56/121, 19 December 2001.

Statutes

Computer Security and Critical Information Infrastructure Protection Bill, 2005.

Electronic Communications and Transactions Act, 2002.

Reports

US House of Representatives (1998), *Combating International Crime in Africa*, Hearing before the Subcommittee on Africa of the Committee on International Relations House of Representatives, One Hundred and Fifth Congress, Second Session, 15 July 1998, US Congress Record 50–884 CC.

World Bank (2008), Global Monitoring Report 2008 (Washington, DC: World Bank).

Newspapers and Magazines

Bequai, A (1996), 'Prosecuting Cyber-Crimes', Computer Audit Update, April 1996, 22.

Bequai, A (1997), 'Organised Crime: Manipulating Cyberspace', Computer Audit Update, December 1997, 25.
'ECOWAS Telecommunications Ministers Adopt Texts on Cyber Crime, Personal Data Protection', Standard Times, 17 October 2008.

Moscaritolo, A 'French President Sarkozy's Bank Account Hacked', SC Magazine, 20 October 2008.

'Nigerian Banks Lost NGN 7.3 Billion to Cyber Criminality', Economic Confidential, 28 August 2008.

Nkanga, E 'Cybercrimes Hit World Bank', This Day, Thursday 16 October 2008.

Viljoen, M 'In Pursuit of Cyberpirates', De Rebus, October 2007, 25.

Internet Sources

G8 Information Centre, 'What is the G8?' <http://www.g7.utoronto.ca/what_is_g8.html>

Internet World Stats, 'Internet Usage Statistics for Africa: Africa Internet Usage and Population Stats' <http://www.internetworldstats.com/stats1.htm> .

Leyden, J 'Booming CyberCrime Economy Sucks in Recruits' Crime, 24 November 2008 <http:www.theregister.co.uk/2008/11/24/cybercrime_economy>.

Sullivan, B 'Foreign Fraud Hits US E-Commerce Firms Hard', *MSNBC*, 1 April 2004 <http://www.msnbc.msn.com/id/4648378/>.

Swartz, J 'Crooks Slither Into Net's Shady Nooks And Crannies Crime Explodes as Legions of Strong-Arm Thugs, Sneaky Thieves Log On', USA Today, 21 October 2004 <http://www.usatoday.com/printedition/money/20041021/cybercrimecover.art.htm> .
Yarney, J 'Africa Confronts CyberCrime' <http://www.itworld.com> .

Conference Proceedings

Ribadu, N (2007), 'Cyber-crime and Commercial Fraud: A Nigerian Perspective', presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL, Vienna, Austria, 9-12 July 2007.

Others

Chawki, M and Abdel-Wahab, M (2006), 'Identity Theft in Cyberspace: Issues and Solutions' (LexElectronica) [Spring 2006].