Cyber Crime and Criminality in Ghana: 
Its Forms and Implications

Richard Boateng*  Olumide Longe†  Victor Mbarika‡
Innocent Avevor**  Stephen Robert Isabalija††

*International Center for IT and Development Southern University, richard@pearlrichards.org
†International Center for IT and Development Southern University, longe.olumide@icitd.org
‡International Center for IT and Development Southern University, victor@mbarika.com
**University of Ghana, innoavevor@yahoo.com
††International Center for IT and Development Southern University, robert@icitd.org

This paper is posted at AIS Electronic Library (AISeL).
http://aisel.aisnet.org/amcis2010/507
Cyber Crime and Criminality in Ghana: Its Forms and Implications

Richard Boateng  
International Center for IT and Development  
Southern University, USA  
richard@pearlrichards.org

Olumide Longe  
International Center for IT and Development  
Southern University, USA  
longe.olumide@icitd.org

Victor Mbarika  
International Center for IT and Development  
Southern University, USA  
victor@mbarika.com

Innocent Avevor  
University of Ghana Business School  
University of Ghana, Ghana  
innoavevor@yahoo.com

Stephen Robert Isabalija  
International Center for IT and Development  
Southern University, USA  
robert@icitd.org

ABSTRACT
This paper investigates the prevalence of cyber crimes in Ghana and its impact on ICT adoption. Through a qualitative approach, we explore efforts by organizations and organs of government in Ghana towards curtailing cyber crimes in terms of apprehension, prosecution, reporting, and law enforcement. Findings from our research showed that although awareness of cyber crimes is on the increase, the crimes mostly go unreported. The Ghana Police Service which is the organ of government responsible for arresting and prosecuting cyber criminals also lack the technical know-how and adequate legal support to effectively discharge their duties. We recommend that a multi-stakeholder effort and appropriate technical training for the police and supportive legislation are required. Future research should also explore how social theories in criminal studies can help understand behavior and intention of both the victim and perpetrators in cyber crime.

Keywords
Cyber crime, Internet Fraud, Ghana, Gold Fraud

INTRODUCTION
As compared to some decades ago, information and communication technologies (ICT) penetration and adoption is on the increase across Africa (ITU, 2008). Although rudimentary access to internet and other online facilities in most parts of sub-Saharan Africa still depends on the use of public internet access points such as cybercafés, nations such as Nigeria, Cameroon and Ghana now have facilities for mobile internet access through satellite connections and fiber optic cables. This increase in penetration of ICT, especially along the West African coast, has spurred a growth in ICT-based businesses and services including electronic government, electronic commerce, teledemocracy, telemedicine, and electronic banking services. Unfortunately, this level of globalization that is being facilitated by ICTs has also simultaneously raised the specter
of new criminal activities arising to exploit them. The internet has become a double-edged sword providing opportunities for individuals and organizations and also bringing with it an increased information security risk (Magele, 2005).

We conceptualize cybercrime as criminal activities or crimes in which computing devices or other forms of ICTs are the target source (Pati, 2003). From the perspective of ICT for development, it is not misplaced to say that cyber crime portends some dangers and have the potential to stall the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and usage in Sub-Saharan Africa. Cyber fraud has a potential to widen the digital divide, crumble the information infrastructure and affect consumer confidence in online transactions (Salifu, 2008; Longe et al., 2009; Oumarou, 2007). Literature is, however, sparse on nation-specific extent of these fraudulent cyber activities as well as nation-specific measures put in place to address them. For instance, Ghana, our country of interest, in this research ranked among the top ten for the source of fraudulent cyber activities in the world with Nigeria ranking 3rd in the 2008 Internet Crime Report (ITC, 2008). The Ghanaian government has made concerted efforts to create a ‘knowledge-based economy’ thereby making Ghana an ICT – driven economy. The use of the Internet in Ghana has also seen a significant increase since the liberalization of the telecommunication industry in 1990’s. The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2009). The number of PC ownership doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007). With these developments also comes negative effects and unintended consequences of ICT, particularly, cyber crime. Our effort in this paper is directed towards understanding the extent of fraudulent cyber activities as well as measures put in place to address them in Ghana.

The remaining part of the paper is organized in six sections including the introduction. In the second and third sections we examine the scope of financial cyber crime and the jurisdiction of law in dealing with it. The fourth and fifth sections present the methodology for the research, and findings on cyber crime in Ghana. The sixth section concludes the paper with a summary of findings, implications for research, and practice and future research directions.

FINANCIAL CYBER CRIME – A WAR WITHOUT WALLS

Cases of online fraud pertaining to credit card crimes, contractual crimes, offering jobs, and advanced fee fraud have been fairly documented (Magele, 2005; Longe et al., 2009). Cyber criminals capitalize on system vulnerabilities, ignorance and gullibility on the part of users to perpetrate their heinous crimes. Between 2006 and 2007, financial losses occasioned by cyber crimes in the United States alone increased dramatically from $52.5 million in 2006 to $67 million in 2007 (Richardson, 2008). Internet connectivity makes it much easier for criminals to act beyond national boundaries when conducting their illegal affairs. With over 300 countries connected to the internet and still counting, cyber crime has become a global issue that requires a multi-stakeholder effort including governments, the private sector, civic and legal institutions, and other social organizations (Westby, 2003).

A genre of these fraudulent cyber activities that has emerged internationally and is believed to originate mostly from the West African coast, particularly Nigeria, is the “advance fee fraud” - a type of Internet fraud used to defraud victims willing to succumb to the temptation offered to make some “quick money” (Smith and Grabosky 2001; Cukier et al., 2007). Skirmishes of these incidences are now being increasingly reported in other West African nations such as Senegal, Cote d’Ivoire, Cameroon, Sierra-Leone, the Gambia, Benin republic and Ghana (Oumarou, 2007). The frauds take the form of victims being approached by letter, faxes or, recently, electronic mail, without prior contact. Victims’ addresses are obtained from telephone and email directories, business journals, magazines, newspapers or through web e-mail address harvesters (Longe and Chiemeke, 2006). These “419” mails generally describe the need to move funds out of one nation or the other, usually the recovery of contractual funds, crude oil shipments or over-invoiced payments, all of which are non-existent, and sometimes using apparently legitimate documents emanating from sources such as the Government, Multinationals and Banks. To facilitate arrangements, victims are asked to supply bank account details and later, money to pay legal fees, taxes, bank transfer fees or bribes for a commission, which could be up to 40 percent of the capital involved. Capital sums of US $20-40 million are often mentioned, thus creating a potential reward for the victim of up to US $16 million. These crimes, as Larkin (2006) posited, pose a threat to global well-being. It has made doing business on the Internet more risk-prone than dealing with a conventional customers. Further, anonymity in cyberspace conceals the cyber criminals’ looks and intent (Laudon and Guercio, 2004), and thus, makes measures to address the challenge more difficult to prescribe. Cyber crimes will increasingly be initiated from jurisdictions that have few laws directed against cyber-crime and little capacity to enforce laws against cyber crime. This is the scenario in most of the Sub-Saharan African nations where some of these crimes are purported to emanate. Pati (2003) noted that, “the (de)creativity of human mind cannot be checked by any law. Thus, the only way out is the liberal construction while applying the statutory provisions to cyber crime cases”.

CYBER CRIME AND LEGAL JURISDICTIONS

Research has examined the implications of a globally diverge view on criminal laws as it relates to the apprehension and prosecution of cyber criminals (Brenner and Koop, 2004). Nations have different perspectives on the issue and existing statutes enacted over the past decades in various countries show varying and diverging jurisdiction clauses. The law of jurisdiction must address whether a particular event in cyberspace is controlled by the laws of the state or country where the website is located, by the laws of the state or country where the internet Service Provider is located, by the laws of the state or country where the user is located, or perhaps by all of these laws (Brenner, 2007). However, in some countries, a number of cyber crimes are yet to be captured by national laws. For example, in Brazil hacking alone is not a crime, and under the law, fraud needs to be proved in order to prosecute (BBC, 2004). The burden of proof of online fraud is a daunting task for an ordinary internet user. In 2005, a Miami businessman filed a lawsuit against the Bank of America. Money had been transferred out of the claimant’s bank account; the fraudster was able to get the businessman’s account details through a keylogging virus which had infected the claimant’s computer. The Bank of America said that they were not liable for the theft and transfer, as the transfer had been “completed with appropriate handling and security procedures” and their “own systems were not subject of hacking”. The claimant said the bank was negligent and should have “let him know of the virus threat prior to the transfer” (The Banker, 2005). If the ordinary internet user cannot take recourse from the bank, reporting future incidences will become discouraging.

Even with sophisticated users such as organizations and institutions reporting cyber crime is a question of the trade off of reputation and image and the potential loss of confidence by key stakeholders. A British newspaper reported that banks and other financial institutions are deliberately failing to report incidents of online fraud to the police and attacks on their system, possibly because of the potential damage to their reputations, concerns over public confidence or lack of confidence in the police and legal system to deal with such crimes (Rupert, 2006). Thus, the true loss from the cyber crime could be quite ‘scary’ when unreported cases of online fraud are taken into account.

This challenge in addressing cyber crime in developed countries is not far from that of developing countries. In India, most cyber fraud cases go unreported and this has been one of the drawbacks in fighting cyber crime in that nation. In Sub-Saharan Africa, records of report from victims of cyber crime are very sparse. These cases mostly come into limelight when foreigners are duped or defrauded by the cyber criminals. It is generally believed that victims are usually high profile citizens or rich expatriates who cannot face the embarrassment of people knowing that they have been duped. The implications of cyber crime and the limited options to address the issue are therefore far-reaching and emphasize the need for more research.

This research, in response, seeks to investigate to the state of cyber crime in Ghana and measures being used to address it.

METHODOLOGY

This research seeks to investigate to the state of cyber crime in Ghana and measures being used to address it. To achieve this, the research questions to aid us in gathering baseline information on the subject matter are:

1. What are forms of cyber crimes in Ghana?
2. How is Ghana addressing reported cases of cyber crime?

To develop an in-depth understanding of cyber crime an exploratory case study method was adopted (Yin, 1994). We adopted qualitative interview approach with key stakeholders on cyber crime in Ghana to obtain richness of experiences regarding apprehension, prosecution, reporting, and law enforcement. A total of 40 respondents participated in this study. The respondents represented information and communication technology (ICT) services, banking, law enforcement and legal agencies. The 40 respondents include: 10 personnel of three selected Banks involved in international money transfer, 10 internet café operators, 10 police investigators working at the Commercial Crime unit of the Criminal Investigation Department (CID) of the Ghana Police who are responsible for investigating Internet fraud, 5 legal practitioners who worked on cyber crimes cases and 5 internet fraud victims. The respondents were between 28 and 45 years old with a mean age of 35.

Sixty percent of the respondents (24) had more than a bachelor’s degree, 30 percent (12) had a bachelor’s degree and 10 percent (4) had a diploma or professional certification. With the exception of the internet fraud victims, all respondents (35, 88 percent) selected had a minimum 3 years of working experience in their occupations in the ICT, banking, law enforcement or legal sector. In selecting the sample, the Ghana Police CID and one lecturer in a University of Ghana business school were consulted. The discussions on the research theme led to referrals to the banking and legal agencies and the internet fraud victims to be involved in the study. The referred respondents had collaborated with the Ghana Police CID in cyber crime investigations and were willing to participate in the study without any compensation.
Data was collected over a nine week period from September to November 2009. The primary instrument used in the data collection for the study was interviews - four sets of interviews with the selected respondents; the banks, the internet café operators, the police and the internet fraud victims. The interview consisted of open-ended questions, which enabled the researchers to seek further explanation to issues that might not be covered by the questionnaire. Regarding the banks, the interview questions were tailored towards measures to prevent financial institutions to be used as the medium for defrauding people and the challenges in dealing with cyber crime suspects. Regarding the police and legal practitioners, the interview questions were about the cases reported, their mode of operations in arresting the criminals and the preventive measures if any, being put in place to check the perpetrators of these crimes. Statistical data obtained from the police covered 2006 to 2008; 2009 data on cyber crime was still being collated. Internet Cafe operators were also interviewed about their mode of operations. Regarding the internet fraud victims interviewed, they were all expatriates from the United States, Germany and the UK. They were interviewed in the offices of the police where they were invited from their various countries to assist in investigation based on the complaints they lodged with the police. We failed to have access to any indigenous victims, since the few who usually reported and collaborated with the police opted to stay out from any form of interviews.

The interviews were recorded and transcribed, with copies of transcribed interviews returned to interviewees to check and resolve discrepancies. Data was coded and analyzed in themes (apprehension, prosecution, reporting, and law enforcement) which address our research questions and also provide a better understanding on cyber crime in Ghana.

DATA PRESENTATION AND ANALYSIS

The data collected from the questionnaire and interviews with their analysis in this section.

Internet Café Operators

The main item of the questionnaire requested the respondents (10) to indicate the approximate age of their customers. Figure 1 shows the age distribution table of the customers of the cafes according to the internet café operators.

From the Figure 1, the approximate age between 18 to 30 years constituted about 88 percent of their customers whilst the remaining 12 percent is shared among the ages of 31-35 and above 35 years. The age distribution above tends to suggest that, most of the people who patronize these cafes are young men and were likely to form a majority of perpetrators of the crime. The researchers at the time of administering the questionnaire observed that more adolescent boys below the age of fifteen browsing but in answering the questionnaires, the café operators tend to have reported a lesser number. In corroborating these findings with the police unit interviewed, it was confirmed, as shown in Figure 2, that the majority of cyber crime suspects
are the youth aged between 21-35 totaling 85 percent. The internet café operators stated the internet was being used for crimes including child pornography, hacking sites to get access to credit cards and downloading films for sale. They are aware of these crimes because the print and electronic media had increased awareness. The financial related crimes have been christened “Sakawa” in the country. They also mentioned that monitoring customer activities online will make them lose customers as there is very strong competition among internet cafes for customers. Although they are not sure of the nationality of some of those who engage in cyber crime in their cafes, the accent of some of them suggest they were of Nigerian decent. In corroborating this claim with the police unit, the police stated that, based on the 2008 statistics (figure 2), 40 percent of the arrested suspects are Nigerians and Ghanaians make up 38 percent. The nationalities of Liberia, Cote d’Ivoire and Togo total the remaining 22 percent.

**Banks which operate Money Transfer Services**

The bankers indicated that they have been rendering fund transfer services for over a decade. Respondents were then asked to indicate the procedure a receiver of a transferred money passes before he or she collects the money. They indicated they inspect identity cards of recipients and then make them fill forms. A follow up question was whether they experience any fraudulent practices on the side of the customers. They all answered in the affirmative. One of the interviewees commented that “we don’t report customers who we suspect to be engaged in criminal activities to the police. We only refuse payments, and ask the recipients to go”. Another set of questions tried to find out if the respondents have websites and if yes how secured are they. All the respondents indicated they have but could not adequately comment on the security of their websites. A follow up question was to find out whether or not they render online services and if yes have they experienced any fraudulent acts on the part of customers. They all said they have experienced some online fraudulent deals which had been reported by their customers.

**Personnel of the Commercial Crime unit of the Ghana Police Service**

The Commercial Crime unit of the CID of the Ghana Police Service is the agency of the government that is charged with the responsibility of arresting, investigating, and prosecuting the perpetrators of Internet fraud in Ghana. Ten of the employees of the Unit were interviewed for this research. The respondents indicated that they received complaints about internet fraud that centered on gold deals, inheritance, ‘money in account’ and ‘marriage deals’ and raffles. Regarding gold fraud, the police explained that, the gold fraud suspects send emails to the email addresses of the victims and introduce themselves as friends and later as gold dealers who can help them get gold in Ghana. First, the suspects send a piece of pure gold to the Ghana Precious Mineral Commission for testing. The commission issues report and receipt for amount paid for testing. Second, the suspects scan and email the report to the victim. The victims usually call the commission for verification. However, since the report and the receipt are genuine, the confirmation from the commission increases the confidence of the victim. Hence, the victim sends any amount of money requested for and becomes duped in gold fraud. Some of the receipts are however not genuine. Figure 3 shows a copy of a fake receipt one of the fraudsters sent to his victim in Switzerland after the victim sent $1,850 for the purchase of gold.

Regarding inheritance and money in account fraud, the perpetrators contact victims through faxes, e-mail addresses which they obtain from telephone, web crawlers and business journals. They create letter heads that look very legitimate and from sources such as Ghana Government, Bank of Ghana claiming that they need to move funds out of Ghana. Such funds are usually contractual or inherited funds or over invoiced payments. All of which were non-existence. To facilitate the movement, victims are asked to supply bank account details and later, money to pay legal fees, taxes, bank charges or bribes.
for commissioners of oaths. These amounts if sent by the victim represent the amount stolen or defrauded. Online dating sites have also been used to defraud victims with ‘ladies’ posting pictures and claiming they want husbands. Money sent by interested suitors for marriage rites or plane ticket to join or visit victim abroad are defrauded.

Figure 4 Graph of Nationality of Victims

From figure 4, it could be observed that, victims are mostly from USA and Europe totaling 70% of reported cases. Only 15% of the victims come from Ghana whilst the remaining 15% came from other African countries. One of the respondents (police) commented that “most victims of internet fraud are high profile and/or rich people in our society who feel reluctant to go to the police station and report because of their status in society and the fact that, they don’t want to look stupid before the police”. On the other hand, three of the victims of Internet fraud from Holland, Switzerland and the USA interviewed were of the view that, victims of many of these crimes decide not to report to the Ghana Police because of certain activities of the police that tend to discourage them, for example, the unnecessary delay in persecution of the offenders. However, the police argue that, the delays often stem from obtaining evidence and tracing accomplices to the crime. A number of cases, especially in 2007 and 2008, which had been rushed to the courts without adequate evidence, have been lost. Other cases could not be investigated further, because the complainants are mostly expatriates who refused to come to Ghana to assist in investigation. Table 1 shows the statistics of cases reported to the police between 2006 and 2008.

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of cases reported</th>
<th>No. of cases prosecuted</th>
<th>No. of cases convicted</th>
<th>No. of cases Acquitted</th>
<th>No. of cases Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>2006</td>
<td>257</td>
<td>121</td>
<td>9</td>
<td>9</td>
<td>127</td>
</tr>
<tr>
<td>2007</td>
<td>88</td>
<td>40</td>
<td>5</td>
<td>-</td>
<td>43</td>
</tr>
<tr>
<td>2008</td>
<td>241</td>
<td>125</td>
<td>27</td>
<td>-</td>
<td>89</td>
</tr>
</tbody>
</table>

Table 1 Statistics of Reported Cases

Source: Ghana Police Service Commercial Crime Unit of the Criminal Investigation Department.

The number of cases reported is declining with a drop of about 65 percent between 2006 and 2007. In 2008, the reported cases increased to 241 well above that of 2007. However, the respondents intimated that, the crime is on the increase. In a number of scenarios the victims were criminals who also engaged in internet fraud and therefore could not report when they were defrauded; and in other scenarios, the victims are indigenous public or popular figures and hence, avoided the Police and court. These scenarios often contributed to less cases being reported.

When requested to indicate their computer literacy level, the respondents claimed to have some computer knowledge but failed to state the levels of the computer literacy. A further question as to how they use the computer to detect the fraud or the modus operandi of the suspects. The police explained that, though they have received some help from computer experts,
arrests have been done primarily through the help of the victims by baiting the suspects. For example, upon receipt of complaint from a victim especially from abroad, the victim is asked to fly to Ghana presumably bringing more money without the knowledge of the suspect that, the police are aware of the deal. Upon the arrival of the victim, the suspect meets the victim at a secret location with the intention of collecting more money and they are arrested. Victims that could not come down after their complaint are made to transfer few more money to the suspects. The suspects are arrested when they go in for the said money.

Legal Components for Cyber Crime Prosecution

Respondents in this case consists of legal practitioners and were asked to indicate the type of law in the criminal code of the Republic of Ghana under which the suspects or internet fraud are charged and whether or not it is appropriate to charge them under these laws. All the respondents indicated there is no law in the statute books that address these types of crime. The police still rely on conventional crime laws on false pretence in the criminal Code Act 29/60 Section 131 and its associate statutes. Crimes committed under these laws are bailable offences and carry lesser punishments which cannot therefore deter the fraudsters from committing cyber offences. The respondents also indicated that it is not wholly appropriate to use this law because the facts of some of the cases do not support the charges made against the suspects under that law hence most lawyers capitalize on such technicalities and have their clients acquitted. It was also noted that the Ghanaian Parliament is currently reviewing a bill to pass laws governing a wider perspective of crimes associated with technology and the Internet.

SUMMARY OF FINDINGS

This research does not deviate from other findings relating to the social characteristics and level of expertise of the perpetrators. Offenders are more likely to share a broader range of social characteristics and are likely to be young, clever often without prior criminal records, possessing expert knowledge and often motivated by a variety of financial and non-financial goals (Balkin et al., 2006; Salifu, 2008; Coomson, 2006; Wall, 2001). In Ghana, the perpetrators of the crime are young and have some degree of technical competence to commit computer-related crimes. This research also brought to the fore the fact that cyber crime fast gaining grounds in Ghana and the agencies responsible for investigating, controlling and apprehending online criminals lack the technical knowledge needed to tackle the problem. Analysis of research data also showed that that most cases go unreported due to lack of confidence in the prosecuting process and fear of embarrassment on the part of the victims. Ghana is yet to enact any law to specifically address these forms of crime. The laws under which the suspects are charged are the existing laws on fraud established in 1960. Defense lawyers often win over when the prosecution presents poor evidence. Our findings are indicative of the fact that measures adopted to curbing internet fraud in sub-Saharan Africa in general and in Ghana particular are grossly inadequate and therefore poses a serious danger to investment opportunities in the country and the region.

CONCLUSION

Cyber crime is common to both developed and developing countries. Its impact appears to be worse in developing countries where the technology and law enforcement expertise is inadequate. This shared challenge tends to be reflected in Ghana. The limited options for the police, legal and financial institutions to address cyber crime call for a multi-stakeholder analysis at the national-level.

Concerning practice and policy implications, the research provides the basis for a concerted effort on the part of individual citizens and corporate bodies, to report cyber crime cases and demand that government put in place laws, policies and technologies to curb cyber crime. As with other forms of ICTs, since these laws are critical, there is the need to gain political support. This could be from the government, or political parties, interest groups, private sector advocates, thus key stakeholders who can push for these legislation and rules.

The government should empower the police force by providing the needed training and technical resources required to discharge their duties effectively. The Bank of Ghana which regulates Commercial Banking operations must develop a reporting scheme on all the identity of all recipients of foreign remittances to it or other agencies of the state so as to create a database that can be reviewed regularly and used for investigating suspicious foreign remittances.

Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks. Since cybercrime is a global problem, the need also arise for law enforcement agents in Ghana to collaborate in the
area of information sharing, infrastructure and personnel with other African Countries and major international security agencies such as the Federal Bureau of Investigation and INTERPOL to crack-down on cyber criminals.

Concerning research implications, the need for a multi-stakeholder effort and poor reporting behaviour of victims, emphasizes the social dimension of cyber crime. This calls for research into how DCs or sub-Saharan African countries can draw on their collective culture (Hofstede, 1985) to develop strong interest or civic groups (local and international) who can become the pivot for education and lobbying for laws. Future research can also explore how social theories in criminal studies can help understand behaviour and intention of both the victim and perpetrators in cyber crime.

This research, though not exhaustive, has generated valuable insights which can help frame future research and policies. Not giving the right attention to this challenge is at the risk of ICT development in a sub-Saharan Africa and Ghana in particular.

ACKNOWLEDGMENTS

The authors wish to thank Kwafo Offei, Ebenezer Nketiah, Florence Tsakuor Nartey, Ebenezer Boryor, and Shaibu Abubakar Osei for their support as research assistants. This paper is based upon work supported by the PearlRichards Foundation under the E-business Research Project and National Science Foundation (NSF) under Grant Nos. 0644305, 0927688 and 0929837. Any opinions and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the PearlRichards Foundation and the National Science Foundation.

REFERENCES


