Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) DOI: 10.7176/JLPG
Vol.84, 2019

Cybercrime in Ghana and the Reaction of the Law

Daniel Ennin[1] Ronald Osei Mensah[2]
1.M.Phil. Graduate, Department of Sociology, University of Ghana
2.M.Phil. Graduate, Department of Sociology and Anthropology, University of Cape Coast

Abstract
Since the advent of the internet, the world has become a global community. This is because through the worldwide web links information is being passed on and received almost instantaneously or in real time. People from different locations are able to communicate with one another by exploring social media platforms to advance their course. However, the increasingly use of the internet has fueled the emergence of cybercrime in Ghana and concerns have been raised by people in the position of trust about whether our current laws are robust to deal with the menace. The main thrust of the study was therefore to examine how the law enforcement agencies, especially the police and the judiciary are reacting to the cybercrime peril in the country. A total of nine (9) respondents took part in the study. Structured interview guide was employed as data collection instrument. In the data analysis, each of the in-depth interviews was transcribed as soon as the information is gathered and developed them into codes. The study revealed that the Ghana Police Service efforts to thwart the menace are being limited by factors such as computer crime investigators, ultramodern equipment, and cooperation from the Internet Service Providers to adduce electronic evidence. In addition, the Electronic Transaction Act of 2008, (Act 772) needs to be reviewed to accommodate the new challenges that have emerged in the cyber ecosystem. It was concluded from the discussions that a progressive capacity building programmes should be organized for law enforcement agencies to enable them acquire ICT skills to deal with cyber laws.
Keywords: cybercrime, reaction, law.
DOI: 10.7176/JLPG/84-04
Publication date: April 30th 2019

1.0 Introduction

In the last quarter of the twentieth century, a technological revolution centered on information has transformed the way we think, produce, consume, trade, communicate, and even how we make love (Castells, 2000). The availability of information technology around the world is linking up valuable people and activities while switching off from conventional networks of power and wealth. To a large extent, cyberspace is the manifestation of postmodern society whereby novel technologies have created new social environment and a new reality.

We are now living in an era of simulations, where humans are constantly "substituting signs of the real for the real" (Baudrillard, 1995). The line between reality and unreality is blurred, and in the postmodern world, it is difficult to tell the real from those things that simulate the real (Ritzer, 1996).

Bauman (2000) also coined the term "Liquid Modernity" to describe the fragmented nature of contemporary life, and society's inability to provide the stable environment to serve as a frame of reference. Liquid life is where nothing is fixed; everything changes very quickly when we are still learning how to cope with the situation, meanwhile the reality has changed. Individual achievement cannot solidify into lasting possession because conditions of actions designed to respond to them age quickly and become obsolete. Extrapolating past events to solve current problem becomes more risky and often misleading because the strategies might not support the technological advancement.

The establishment of cyberspace has also collapsed the constraints of space and time that limit interaction in the real world. Borrowing from the sociological accounts of globalization as 'time-space' compression, Harvey (1990), theorized that cyberspace makes possible instantaneous encounters between spatially distant actors and these create possibilities for ever-new forms of association and exchange. In the same vein, Castells (2000) elaborated how the collapsing of time and space affects the global business. For instance, in his concept of 'timeless time' he argued that the internet has unified the global financial market. The same capital is shuttled back and forth between economies in just a matter of hours, minutes as a result of powerful computer financial analysis software. Therefore, Jones (1993) espoused that individuals sitting at the global nodes of telecommunications network are generating billions of dollars every day in the stock market. The qualitative change in the human experience has affected the industrial paradigm of increasing subcontracting and offshore production business in the global environment.

Notwithstanding the success chalked in the Information and Communication Technology (ICT), society is now witnessing sophisticated crime wave, called cybercrime. It has affected all sectors of the economy of scale, resulting in monetary losses and reputational damage to institutions that relied on some form of ICT as part of their day-to-day operations.

2.0 Statement of the problem

The computer technology has become a ubiquitous component in modern life and it has unlocked possibilities we could just barely imagine a generation ago.

Individuals are utilizing their laptops, desktops, tablet computers, smart phones to engage in all facets of social life, from communications to finance (Smith, 2011). Social networking sites like Facebook, WhatsApp, Viber, Twitter, and many more allowed us to stay in touch with our friends and family to share and exchange ideas around the world while streaming media services entertain individuals twenty-four (24) hours a day on demand.

The rise in technology and online communication has not only produced a dramatic increase in the incidence of crime, but has also resulted in the emergence of what appears to be new varieties of criminal activities and these poses a challenge to the legal system as well as the law enforcement community (Brenner, 2007). In the 7th December, 2017 edition of the Daily Graphic, a popular newspaper in Ghana highlighted that the growth of the ICT sub-sector, including the introduction of e-payment platforms, cashless systems, mobile money, e-learning among others has led to the significant rise in cyber-related threats. The current Inspector-General of Police in Ghana, Mr. David Asante-Apeatu has also expressed concern that the emergence of ICT-facilitated crimes had become one of the many challenges confronting the adjudication of criminal offences, especially with regards to the presentation of satisfactory evidence in the court of law to ensure successful criminal prosecution (Daily Graphic, 25/10/2017). It is in the light of these that the study seeks to explore how the law enforcement agencies especially the police and the judiciary are reacting to the cybercrime menace in the country.

3.0 The purpose of the study

The general objective of the study is to explore how the existing laws are reacting to address the cybercrime activities in Ghana.

4.0 Research questions

The emergence of cyber ecosystem in Ghana has left the central government and the law enforcement agencies with various puzzle questions:

For instance, how does one define what cyber activities are legal and what cyber activities are not legal?

How does one enforce cyber laws when the relationship between the victim and the offender is often virtual?

The internet allows people to interact with each other across borders, so whose jurisdiction is the offence committed?

What are some of the policy recommendations to address cybercrime menace in Ghana?

5.0 Significance of the study

The study hoped to provide the readers an understanding of what cybercrime is and raises awareness about how the existing laws are being administered to contain the situation in the country. It will serve as a reference material for government, security agencies and other stakeholders in the policy formulation to address the problem. Given that there is a little research on internet scams, the study seeks to add to the body of knowledge.

6.0 Literature review

6.1 Definition of cybercrime

The basic problem for the analysis of cybercrime is the lack of a consistent and statutory definition for the activities that constitute cybercrime (Yar, 2005). According to Smith, Grabosky & Urbas (2004), defining cybercrime raises conceptual complexities and varied information. In addition to the difficulty of definition, it is also called by variety of terms such as computer crime, computer-related crime, digital crime, information technology crime, internet crime and virtual crime. Cybercrime could reasonably include a wide range of criminal activities and it would appear that scholars, writers and law enforcement agencies are more comfortable of describing the various elements constituting cybercrime than defining the term (Olayemi, 2014).

Suman, Srivastava & Pandit (2014:334) defined cybercrime as "unlawful acts wherein the computer is either a tool or a target or both". It means that on one hand, a computer may be the object of the crime when there is theft of computer hardware, or software. Also a computer may be the subject of a crime when it is used as an instrument to commit conventional crimes such as fraud, theft, extortion, or new types of criminal activity such as denial of services attacks and malware, identity theft, child pornography, copyright infringement, and mail fraud. Snail (2009:2), further explains that cybercrime can be defined as any criminal activity that involves a computer and can be divided into two categories- crimes that can only be committed using a computer which were hitherto not possible before the dawn of the computer such as hacking, sniffing and the production and dissemination of viruses, and crimes that have been in existence for centuries but now committed within the cyber environment such as fraud, possession and distribution of pornographic materials.

Drawing from the foregoing definitions, it is significant to note that there is no consistent and statutory definition for cybercrime, and it is simply committed with the aid of a computer connected to the internet. This

creates a 'save heavens' for the perpetrators because the speed, convenience and anonymity that modern technology offers provide diverse range of criminal activities which make it difficult for the security agencies to track.

6.2 Cybercrime Legislations in Ghana

With the recognition that cybercrime is increasingly a real threat to the country, the government of Ghana, through the Ministry of Communications has come out with some Acts to regulate the conduct of people in the cyber space. These Acts consist of Electronic Transactions Act, 2008 (Act 772), National Information Technology Agency Act, 2008 (Act 771), Data Protection Act, 2012 (Act 843), and some related provisions in the Criminal Code. The subsections will hint on the spirits and limitations of these acts.

6.2.1 Electronic Transactions Act (ETA), 2008 (Act 772)

The Parliament of Ghana in December, 2008, passed the Electronic Transaction Bill into law. The primary objective of the ETA is to secure the cyber space as a means of mitigating crime incidence that may affect the ability of the citizens to create worth.

The Act is divided into twelve groups of clauses. These are electronic transactions, electronic government services, the certifying agency, consumer protection, protected computers and critical database, Domain name registry, and appeal tribunal. Other clauses relate to the industry forum, the liability of service providers and intermediaries, cyber inspectors, cyber offences, and miscellaneous matters.

The law enforcement is dealt with in the tenth group of the clauses and the Act empowers security agencies in the course of the execution of court warrants to seize a computer, electronic record, programme, information document or thing if they reasonably believe that an offence has been or is about to be committed, (ETA 2008, Act 772, clause 98). The law enforcement agencies may also request the preservation of evidence by providers of wire or electronic communication services or remote computing services pending the issuance of a Court Order, (ETA 2008, Act 772, clause 100). The Courts are empowered, upon application of a law enforcement agency, to order an electronic communication service provider to disclose the contents of an electronic communication, that is in transit, held, maintained or that has been in electronic storage in an electronic communications system, if the disclosure is relevant for the investigative purposes in the interest of national security, (ETA 2008, Act 772, clause 101). However, the scope of the enforcement of the Act is limited by the area of jurisdiction as it's contained in clause 142 (2):

That this Act applies if, for the offence in question:

(a) The accused was in the country at the material time;
(b) The electronic payment medium, computer or electronic record was issued in or located or stored in the country at the material time;
(c) The electronic payment medium was issued by a financial institution in the country; or
(d) The offence occurred within the country, on board in Ghanaian registered ship or aircraft or on a voyage or flight to or from this country at the time that the offence was committed, whether paragraph (a), (b) or (c) applies.

Traditionally, the legal jurisdiction involves territories with the scope of country being defined by the limit of its boundaries. This territorial notion is ineffective to prosecute cybercriminals. Determining where cybercrime is committed can be difficult since the perpetrators and the victim can be located in different countries. The offenders may also utilize computer systems in different countries to attack their victims.

Another pitfall of the Act is that punishment is not clearly stated as in the drug trafficking law and this allows judges to exercise their discretional powers to make pronouncement on cyber offences. For instance, under the Narcotics Drugs Law (P. N. D. C. L 236), Section 2(2) states that "a person found guilty of narcotic offence is liable on conviction to a term of imprisonment of not less than ten years". Additionally, properties acquired by scammers by fraudulent means are not seized or confiscated unlike the Drugs Law, Section 11 to 14 which stipulated that properties acquired by drug traffickers should be seized. Obviously this law provides a vent for the criminal as the weight of the punishment does not commensurate with the nature of the cybercrime.

Therefore, it is not surprising that the Ministry of Communications (2014), concluded in their final draft report on Cyber Security Policy that 'even though the ETA has provisions for law enforcers to fight against cybercrime, however, this is not adequate and does not address fully all aspects of cyber security challenges especially the multi stakeholders approach' (Ministry of Communication final draft on Cyber Security in Ghana, 2014: 6). This accession has also been reechoed recently by the National Cyber Security Advisor that the law has been in existent for more than 10 years and certain gaps ought to be tightened to better position the country to deal with the increasing cases of cybercrime (Daily Graphic, 5/12/18, page 45).

6.2.2 National Information Technology Agency Act (NITA), 2008 (Act 771)

The National Information Technology Agency is a Ghanaian public institution established by Act 771 in 2008, as the ICT policy implementing arm of the Ministry of Communications. Its mandate is to regulate and monitor the activities of companies in the electronic industry of ensuring quality information delivery and standard of

efficiency. The agency is further empowered to give accreditation to individuals who want to conduct legitimate business online. Under this Act, the functions and responsibilities of the agency are captured in clause 3 which stipulates that the Agency shall;

(a) Perform the functions of the certifying Agency established under the ETA, 2008 (Act 772).
(b) Issue licenses and ensure fair competition among license holders in the cyber space.
(c) Monitor, enforce and ensure effective compliance with the conditions contained in licenses and tariffs; (National Information Technology Agency Act, NITA 2008:3).
(d) Maintain registers for approval given for equipment used under the ETA, 2008 (772)
(e) Establish quality of service indicators and reporting requirements that apply to the license holders under the ETA.

It's interesting to note that fake websites are being created everyday by the internet hackers and duped innocent people without NITA detection or apprehension. This could be attributed to the inadequate skilled manpower or technical enabling environment to track the perpetrators.

6.2.3 Data Protection Act (DPA), 2012 (Act 843)

The Data Protection Act is one of the key legislations to improve legal certainty and transparency in the cyberspace. The Data Protection Act 2012 (Act 843) was passed by parliament in 2012, to protect privacy of individual and personal data (Data Protection Act 843, 2012:5). The Minister of Communications on Thursday, November 18th, 2014 inaugurated an 11-member governing board of the Data Protection Commission (DPC) chaired by the Supreme Court Judge, Justice Date-Bah to regulate the processing of personal information on the internet (Daily Graphic, 25/04/15, page 3). The Commission has the power under the clause 3 of the Act to:

a. implement and monitor compliance by individuals who utilize the electronic industry
b. make the administrative arrangements it considers appropriate for the discharge of its duties;
c. investigate any complaint under this Act and determine it in the manner the Commission considers fair; and
d. keep and maintain the Data Protection Register.

The privacy fortified the human dignity and guaranteed other key rights such as freedom of association, speech as enshrined under Article 18(2) of the 1992 Constitution of Ghana. The information and communication technologies are being used by numerous anti-social elements in aiding their illegal activities. Daily Graphic (14/11/2014, page 32) explained that data in the wrong hands have caused untimely death and jeopardized many lives. Therefore, it is imperative that strong provisions are made to protect people against the abuse by those institutions that keep their information on the internet such as schools, hospitals and governmental organizations. The intended purposes of the Data Protection Commission are yet to be fulfilled because data are still collating from the various institutions that controlled individual's information online.

6.2.4 Criminal Offences Act, 1960 (Act, 29)

The growing Internet penetration in Ghana had opened up the country into new online trading platforms, which had empowered the average Ghanaian to transact various business operations. Even though the online portal serves as a medium of exchange for goods and services, most transactions take place offline. As a result, some Sections of the Criminal Offences Act (29/30) are recaptured in the Electronic Transactions Act (Act 772) to prefer charges against cybercrime suspects. These Sections include: 20, 21, 23, 122, 124, 133, 137, and many others.

Crimes committed under these Sections of the Criminal Offences Act 29/60 which have been reiterated in the Electronic Transactions Act (Act 772) are bailable offences and carry lesser punishment which cannot deter fraudsters from committing such offences. Besides, Danquah & Longe (2011) were of the view that the criminal code under which cybercrime suspects are currently charged has existed under the fraud laws established in 1960 which gives room for defense lawyers to often win and acquit their client because some of the facts do not support the prosecutor's evidential claims.

This conclusion connotes with the Routine Activity theory proposed by Lawrence Cohen & Marcus Felson in 1979 which emphasis that crime can occur when there is no strong guardianship or deterrent measures like the police patrols or effective laws to deter potential offender from being perpetuating the act.

7.0 Methodology

In this study, the design used was exploratory research design. The design made room for the concepts and issues to be unearth by the researcher. The study made use of qualitative method. The purpose of the study was to explore how the existing laws are reacting to address cybercrime activities in Ghana. To fulfill this mission, the researcher tried to explore in all angles of the research by preparing interview guides to elicit the relevant information from the respondents.

A total of nine (9) respondents participated in the study. The number consists of 8 Police personnel drawn from four Units at the Criminal Investigations Department (CID) headquarters who are specialized in handling internet fraud cases, and a Circuit Court judge. The CID departments contacted were: Commercial Crime Unit (CCU), Documentation and Visa Fraud Section (DVS), Intelligent Unit (IU), Legal and Prosecution Unit (LPU).

Two officers were selected from each unit. The four senior police officers heading these units were purposively selected to enrich the discussion. The assumption is that the higher the rank the more knowledge one can acquire on the job. Another four staff were randomly selected amongst the junior ranks to share their thought and experiences about this emerging crime.

The 2016 Annual Report of the Ghana Police Service highlight that the basic function of the Commercial Crime Unit (CCU) is to investigate all criminal cases related to commercial activities. The Documentation and Visa Fraud Unit (DVS) also deals with visa and documents fraud cases. Legal and Prosecution Unit (LPU) prosecute cases and offer legal advice to the various units concerning case docket and appropriate legal instruments prefer against culprits. The Intelligent Unit mounted surveillance, conducted crime analysis, gathering and disseminating criminal information to various embassies and other stakeholders. On preliminary visits to the Cocoa Affairs Court Directorate in Accra, the researcher contacted three judges and surprisingly, they all advised that "Court 8" judge who is an expert in cybercrime should rather be consulted. So the investigator had to settle on her to shed light on legal issues relating to cybercrime in Ghana.

Essentially, qualitative analysis involves a process of discovery that enables the researcher to remain close to the data and form an evidence-based understanding of the research issues. In the data analysis, each of the in-depth interviews was transcribed as soon as the information was gathered and developed them into codes. Ethical considerations such as privacy, anonymity and confidentiality of the participants were adhered to by using pseudonyms to protect the respondent's identity.

8.0 Presentation and discussion of findings

8.1 Responses and Challenges of Ghana Police Service towards Cybercrime

The Ghana Police service has, since its inception been in the frontline of the criminal justice system of Ghana. It is the most visible arm of government as the symbol of law and order, to the people. The Police Service is mandated by Article 200 of the 1992 Constitution of the Republic of Ghana, and the Police Service Act of 1970 (ACT 350). The Constitution mandates the Service to operate on democratic policing principles. Whenever the ordinary citizen suffers from injury or loss of property through crime, it becomes an incumbent upon the police to investigate and establish the prima facie of the case. The Police Service Act 350 provides in Section 1 (1) states that "it shall be the duty of the police service to prevent and detect crime, to apprehend offenders, and to maintain public order and safety of person and property".

This duty extends to the full range of prohibitions under the penal statutes. As cybercrime acts become ever more prevalent, Ghana Police Service as law enforcement agent increasingly face the question of what it means to 'prevent' and 'apprehend' in the context of crime with transnational element. Hence, the researcher developed interest to delve into the scope of the phenomenon from the police perspective. As reiterated earlier, four Units were contacted at the CID headquarters to shed light on the menace. The interview schedule was organized to find out the ordinary and legal meaning of cybercrime, the magnitude of cybercrime situation in Ghana, the demographic characteristics of actors (i.e. victims and the offenders), and how police is reacting to the problem.

During the interview, the head of the Commercial Crime Unit, made general observation which presupposes that the practice of cyber fraud is becoming severe and gaining grounds rapidly. He noted "it is becoming serious, formerly it was on small scale but now it is worse. Even people who are transferring money to buy goods outside Ghana get their monies being diverted into different accounts".

An attempt was made to find out how police officers understand cybercrime. Even though most of the respondents commented on the issue with different preambles, yet they all arrived at the conclusion that 'it is a crime committed via the use of internet and by extension making false representation'. As a result of the fluid meaning of the concept, further questions were posed to find out whether there is a legal definition that supports the officers' claims but the majority of the personnel acknowledged that there is no law in Ghana that clearly states what constitutes cybercrime, outlines its offenses and the punishments to commensurate with the crime

On the other hand, the head of the Legal and Prosecution Unit disagreed with that assertion. He argued;

> "Crime is crime; whether stealing, whether murder, whether cyber, they are all crime, and a crime is any act that offenses the laws of the state. We have the law passed in 2008, that is electronic transaction act, Act 772 and the various crimes that are committed by the use of internet have been defined in that act. So the police, when particular crime is committed by the use of internet we have clear definition of that crime in the act which gives the police power to investigate and prosecute such offenses in competent court of jurisdiction".

This answer allowed the investigator to probe further about the jurisdictional efficacy of the Act and he opined;

> "The law states that if the offense is committed by the use of computer, and it can be even an ATM card, mobile phone or any electronic device. It means

> that the person's 'mens rea' or the criminal intent for the commissioning of the act has been informed under the sovereign will of Ghana. And the role of service providers do not control over what customers are doing. The service providers open up the traffic for people, individuals buying their credit and connect to the cyber world and decide what they want to do. So the law enjoins us (police officers) that where there is need to access the information from service providers, we go for it. In the same vein, if the need arises to access information outside Ghana, we use The International Criminal Police Organization (INTERPOL) to get the response".

It was obvious from the discussion that there are some disagreements about the phenomenon as the police officers holding different views. Although the head of the Legal and Prosecution Unit tried to salvage the image of the police service on how they are responding to the issue, his approach is still skewed towards traditional means of international cooperation which may not be sufficiently timely to ensure access to extraterritorial volatile data retrieval because cybercrime can occur within milliseconds. The conversation was then shifted to the age demography of both offenders and the victims because some criminologists argued that age distribution of crime is invariant over broad range of other social conditions. Commenting on the age issue, the Director of Documentation and Visa Fraud Unit at the CID headquarters, explained;

> "What I know and from what I have investigated, they are young men between the ages of 18 to 30 and the majority of them are secondary school leavers, but at the highest level there are people who are working at the banks and other higher institutions using the internet to commit crime. The perpetuators can be grouped into two categories: that is technical and non-technical people. The technical people are the real hackers. They are the IT specialists as in people who have gone so much into IT like programmers, system administrators, computer security professionals; data based security administrators, and computer forensic. They can hack into an electronic payment system and transfer account from one data to another. The non-technical people are criminals in the real world who have fair idea about IT system and they use it to facilitate their heinous crimes. Now in Ghana, those we have mainly as the perpetrators of cybercrime are the non-technical people. People who normally fall victim of cybercrime in Ghana are the divorcees and they are mostly middle-aged women between 36 to 45 years. They are easily tricked by the cyber offenders on love relationships. You see, people at this age category simply don't think it could happen to them, and when it does, it takes them too long to lodge complaint. And in the end we find it difficult to adduce evidence to support their case".

Online dating has become an accepted practice in the modern times: indeed, many find it preferable to traditional dating as it allows you to select candidate and break the ice without any social engagement. This makes it an ideal hunting ground for internet scammers looking for a quick score and not in the usual dating sense.

Responding personnel opened their remarks about the complex nature of cybercrime, and enumerated some challenges that affected the investigation, apprehension and prosecution of cyber offender in Ghana. The officers acknowledged that the police organization is understaffed and this affects their effort to fight crime. The head of the Intelligent Unit observed; "in my opinion, the population is expanding at geometric progression as against slow expansion of police service and therefore the numbers of crimes are far outweighing the investigators". This concern also reiterated in the Ghana Police Service (2016) Annual Report where police-population ratio stood at 1:847 which remained far from achieving United Nations policing standard of 1:500 people.

Inadequate training or lack of technical know-how on the part of cybercrime investigators increases the level of sophistication. The traditional law enforcement methods have proven ineffective against the growing evidence of criminals using electronic devices to commit fraud. The head of the Legal and Prosecution Unit noted;

> "Equipping investigators with technique to detect, analyze and retrieve falsified documents from any digital device is the way forward but many crime officers are not trained; many do not even understand what cybercrime is or what constitutes cybercrime. Ghana Police College is a higher learning institution of the Ghana Police Service and ran courses designed to update senior corps but cybercrime is not part of their syllabus, recruit training is also not part of it. At the Detective school, I even forced my way to teach but the training itself is not enough. I stand for two hours and that is all. We need computers to study how the whole crime is perpetuated, that is, going into how computer is hacked, how information is properly protected, but we don't have

the equipment".

Other participants argued that 'you can have good investigators but if you do not have the necessary investigation tools to work with and adduce evidence to support your case, the offenders can be discharged unconditionally'. The conclusion remark by one of the junior officers is worth quoting;

> "We don't have the means to monitor what is going on within the internet cafés. People will sit down 24 hours browsing, and do all sorts of things without being detected. But on the other jurisdictions, they have a specialized unit that controls cyber information, and the Unit is connected into the Internet Service Providers portal to monitor what people are reading or twits over the internet space".

The final problem enumerated by the key informants was the difficulty of obtaining information from the telecom service providers. For example, one of the respondents explained;

> "The process of getting information from the telecommunication companies is very cumbersome: first, the investigator has to file an Ex-parte motion in court to declare his intention to access information from the Telco's: secondly, the investigator has to swear an affidavit in support of the motion thereof, and lastly, the court will order for the disclosure of information. In each process it can take you some weeks before you get a response", he added.

The complexity of cyber security threat requires unparalleled response from the law enforcement agencies because data can be altered within few seconds, and sometimes service providers do not store computer data for longer periods. The Article 100 (2) of Electronic Transaction, Act 772 states that "where an order from the Court is not obtained and served for fourteen days after the receipt of the written request, the electronic communication provider is not under any obligation to preserve the evidence". As a result, this conventional policing method of accessing information cannot be an effective mechanism to deal with this contemporary criminal threat.

8.2 Cybercrime and Legal Mechanisms

Law is a dynamic tool that enables the state to respond to new societal and security challenges, such as cybercrime. A discussion with some officers of the Ghana Police Service further revealed that when such cybercriminals are apprehended and processed to court, there are no sufficient legal bases to prosecute them as the legal system is not up to date to convict the scammers, and this contributes to the prevalence of the menace. The head of the Police Intelligent Unit remarked;

> "This is an intelligent led operation and after we worked hard to present our docket before court, the judges still rely on the conventional procedural trial; that is the Complainant, the Prosecutor, and the Accused. So if one of the stakeholders is not around, nor represented, the judge will strike out the case, and from my experience, most of the cybercrime acts involve transnational element where either the accused or the accuser will be at different sovereign state and it has been a major setback to combat the internet fraud".

On the contrary, the Director in charge Legal and Prosecution debunked this assertion and explained that the Act 772 defined the various crimes that are committed by the use of internet. Although he did not quote the exact section to support his claim, he further gave a general statement that the law further allowed the police to prosecute offender in the absence of the victim or the complainant. These contradictory views expressed by the officers influenced the researcher's decision to carve it as one of the focal points for the discussion. In order to achieve this specific objective, Circuit Court Judge was consulted to throw more light on Electronic Transaction Act (Act 772), as an instrument for promoting legal certainty in the cyber ecosystem of Ghana. But as mentioned earlier, the investigator had to settle for speaking to the "Circuit Court 8" Judge at Cocoa Affairs Court Directorate because of her expertise on internet fraud.

The synopses for the discussion were the criminalization of the cyber offences; admissibility of electronic evidence in the cybercrime proceedings, and jurisdictional issues. Commenting on the issue, she expressed concern that 'criminals are now exploiting the internet to the detriment of the public and that if cybercrimes are allowed to continue, it would erode the public confidence in the online commercial activities such as trading, e-banking and other services, which would have serious consequences on the Ghanaian economy. Thus, it is high time we tighten up our laws to control the scourge', she emphasized.

8.2.1 The criminalization of cybercrime

The technological advancements associated with cybercrime means that while traditional laws can still be applied to some extent, the legislators must also be contended with the new concepts which were not traditionally addressed by the law. For instance, while the existing criminal law focused on physical objects of crime such as stealing, rape, murder and burglary; cyber law on the other hand are largely characterized by an intangible 'computer data' which also requires the introduction of specific offences, definition and concept to protect it legal integrity.

However, all these legal tussle would be understood on the Jerome and Hall criminal principle of 'nullum

crimen sine lege' (no crime without law) which requires that;

> No one shall be held guilty of any penal offence on account of any act or omission which did not constitute any penal offence at the time when it was committed nor shall a heavier penalty be imposed than the one that was applicable at the time the penal offence was committed (cf. Ofori-Amankwah, 2012:10).

It means that what constitutes any criminal offences must be clearly defined by law. This notion encouraged the researcher to enquire from the judge about the criminalization aspect of the Act 772 and she noted;

> "Yes, we have the Act 772 which basically regulates the transactions that occur in the electronic space and the offences are stated under Section 107 to 137 of the Act. The only section utilized by the Police as far as this Court is concerned, is Section 102 (2), which states that "a provider of an electronic communication service shall disclose a record or other information related to a subscriber or customer to a law enforcement agency on receipt of Court order for the disclosure". But that does not mean the evidence gathered from the service provider is attainable in court. Section 106 of the same Act makes it clear that "Where a Court varies; evidence obtained solely on the basis of electronic wired transfer is inadmissible in civil, criminals or administrative proceedings". So the prosecutors need to furnish with us [judges] supportive documents to substantiate their case.

8.2.2 Electronic evidence in cybercrime proceedings

In criminal cases, the burden of producing evidence is the means by which the facts relevant to the guilty or innocent of an individual at the trial are established. Therefore, the prosecutor has a duty to present sufficient evidence to support his claim beyond reasonable doubt. Electronic evidence is becoming central not only to the investigation and prosecution of cybercrime, but increasingly to crime in general as a result of the growing usage and application of communication technologies. During the study, some police officers pointed out, 'even where the evidence was adduced, the courts sometimes gave little weight to the electronic evidence, due in part to the lack of knowledge about the intangible nature of the electronic evidence'. Thus, a clarification was sought from the judge whether electronic evidence is admissible in court and she argued;

> "In the Act 772, Section 7, allowed the admissibility of electronic evidence and set parameters or the criteria for assessing the weight of the evidence in terms of reliability, integrity, original source and any other information that the court consider relevant. However, due to the lack of computer forensics laboratory, it is difficult for investigators to collect such digital evidence. In addition, some judges too need basic understanding of cybercrime in order to appreciate the electronic evidence".

Fighting crime is a joint effort between police and the judiciary. The court has a legal authority to punish the offender through fines or imprisonment to serve as deterrence to others. And so, if some judges 'do not have basic tenants of cybercrime'; it weakens the police determination to cramp down the perpetrators.

8.2.3 Jurisdictional issue in cybercrime

According to the Black's Law Dictionary (8th edition), jurisdiction is the practical authority granted to formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and, by implication, to administer justice within the defined area of responsibility. Every country has jurisdiction over people within its territory. Conversely, no State can exercise authority over persons outside its boundaries unless international treaties. In the context of the internet, cyberspace has no geographical boundaries. It establishes immediate and long-distance communications with anyone who can have access to any website. As internet does not tend to make geographical locations clear, the cyber citizens remain in physical jurisdictions and are subject to laws independent of their presence. Therefore, any related activities on the internet may expose the person to a risk of being sued in any country where another internet user may establish a claim. Accordingly, in each case, a determination should be made as to where an online activity will subject the user to jurisdiction in a distant country.

As such, a single transaction may involve the laws of at least three jurisdictions: the laws of the State in which the user resides; the laws of the State where the server hosting the transaction is located may apply; and the laws of the State which the person or transaction takes place. So an internet user in Ghana conducting a transaction with another internet user in USA through a server in South Africa could theoretically be subjected to the laws of all the three countries as they related to the transaction at hand. With this scenario, a question was posed to the judge about the jurisdictional integrity of Act, 772 and the key informant acknowledged;

> "Under Section 142 of the Act grants extra territorial powers but it is very difficult to enforce. The reality is that Ghana is yet to subscribe to any cybercrime convention that can facilitate extradition. So the window opportunity for the investigators is to explore the conventional treaties like INTERPOL to reach out the party concern"

She made further observation about the Criminal Offences Act (Act 29);

> "Criminal Offences Act, 1960 (Act, 29) actually deal with physical criminal behavior like theft, and a lot of sections have been modified to suit cybercrime offences. But the Sections give us [the Judges] a lot of discretionary powers without categorically defined how the case should be addressed.

In her concluding remarks, she is calling for specific cyber laws like the UK Computer Misuse Act which outline the various offences under clear subheadings to deal with the issue".

9.0 Conclusion

The discussions have revealed that cybercrime perpetrators are in two groups; that is technical and non-technical people. The non-technical people mainly employ social engineering tactics to defraud their client. The findings further highlighted that Ghana Police Service has been mandated to fight cybercrime in Ghana. However, the organization efforts are being limited by factors such as inadequate computer crime investigators, lack of ultramodern equipment, and lack of cooperation from the Internet Service Providers to adduce electronic evidence.

The Electronic Transaction Act of 2008, (Act 772) also needs to be reviewed to accommodate the new challenges that have emerged in the cyber environment such as a succinct definition of cyber offences, the admissibility of electronic evidence in court, and the explicit provisions on the extradition of individuals involving in cybercrime proceedings.

10. 0 Recommendations

1. In order to empower national law enforcement agencies to properly prosecute cybercriminals, the government should establish a progressive capacity building programmes for officers to acquire new ICT skills and effective ways of enforcing cyber laws. The training objectives must be abreast with the current trends in cybercrime investigation techniques, adducing and the storage of electronic evidence in courts.
2. The Government in collaboration with the Attorney General's department should set up a periodic process of reviewing and enhancing Ghana's laws relating to cyberspace to address the dynamics of cyber security threats.
3. Government of Ghana should further accede to international cybercrime conventions and protocols to fast track the rendition and extradition of offenders among member states to minimize the incidence of internet fraud.

References

Abbey, E., E (2015). "Inauguration of 11-member governing board of the data protection commission". *Daily Graphic*, April 25, pp. 22

Baudrillard, J. (1995). '*Simulacra and Simulations'*. Michigan: University of Michigan Press.

Bauman, Z. (2000). *Liquid Modernity*. UK: Polity Press

Black Law Dictionary (2004). (8th Ed.). US: West Publishing Co.

Castells, M. (2000). *The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I.* Oxford: Blackwell Publishing Ltd.

Castells, M. (2000). *The Power of Identity, The Information Age: Economy, Society and Culture, Vol. II*. Oxford: Blackwell Publishing Ltd

Cohen, L., & Felson, M. (1979). *Social Change and Crime Rate Trends. A Routine Theory Approach.* America Sociological Review, 44, 588-608

Criminal Offences Act, 1960 (Act, 29)

Data Protection Act (DPA), 2012 (Act 843)

Danquah, P., & Longe, B. (2011). Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact 11(3) 169-182.*

Donkor, B. K, T. (2017). "KNUST gets digital forensic laboratory". *Daily Graphic, October 25, pp.41.*

Electronic Transactions Act (ETA), 2008 (Act 772)

Ghana Narcotics Drugs Law *(P. N. D. C. L 236)*

Ghana Police Service: *2016 Annual Report.*

Ghana Police Service Act, 1970 (Act 350)

Harvey, D. (1990). *The Condition of Postmodernity*. Oxford: Blackwell Publishing Ltd.

Jones, D. (1993) "Banks move to cut currency dealing costs",*Financial Technology International Bulletin,* 10(6):1-3

Mensah, M. (2014). "Gvt Sets Up Data Processing Commission". *Daily Graphic, November 14, pp. 32*

Ministry of Communications (2014). Ghana National Cyber Security Policy and Strategy: *Final Draft*

National Information Technology Agency Act (NITA), 2008 (Act 771)

Ngnenbe, T. (2017). "Judiciary staff train in cyber security". *Daily Graphic, December 7, pp.69.*

Ngnenbe, T. (2018). "Electronic Transaction Act to be reviewed next year". *Daily Graphic, December 5, pp.45.*

Ofori-Amankwah, E. H. (2012). *Outline of Criminal Law Lecture*. Accra: 2WENTY 3THIRD SOLUTION

Olayemi, J. (2014). "Combating the Menace of Cybercrime". *International Journal of Computer Science and Mobile Computing, Vol.3, Issues 6, pp.980-991*

Ritzer, G. (1996). *Postmodern Social Theory*. New York: McGraw-Hill Publishing

Smith, B. (2011). *"Cybercrime and the Youth in Ghana: A Study of the Sakawa Conundrum in Accra and Agona Swedru Communities"*. A Thesis presented to the Department of Sociology, University of Ghana, Legon.

Smith, R., Grabosky P., & Urbas G (2004). *Cyber Criminals on Trial. Cambridge* (UK): Cambridge UP.

Snail, S. (2009). 'Cyber Crime In South Africa-Hacking, cracking, and other unlawful online Activities'. *Journal of Information, Law & Technology (JILT)*

Suman, S., Srivastava, N., & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent Innovation Trends in Computing and Communication, 2 (2), 334-337*

The 1992 Constitution of the Republic of Ghana.

Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in light of routine activity theory. *European Journal of Criminology, 2(4), 407-427*