Volume. 18, No. 1

ISSN 0189 0255
2015

The Nigerian Law Journal

CONTENTS

The Nigeria Police and Problems of Cybercrime Investigation: Need for Adequate Training	Ikenga K.E. Oraegbunam	1
The Role of the Police in Free and Fair Democratic Elections in Nigeria: The Legal Framework	Prof. Adedokun A. Adeyemi	29
The Imperative of Imposing Penal Sanctions for the Willful Transmission of the Ebola Virus and Other Infectious Diseases in Nigeria	Osinibi, Olusegun Michael	52
Law, Development and the Nigerian Oil and Gas Refineries	Idowu Adegbite	72
An Overview of the Arms Trade Treaty 2014	Daniel U. Nnam Esq Ugwuozo C. Walter Esq	107
Compensation for Victims of Crime in the Nigerian Criminal Justice System: The Need to the Need	Elizabeth Ama Oji	120
Dynamics and Challenges of Internal Displacement In Nigeria: A Critical look at the Law	Awhefeada, Ufuoma V. (Mrs.)	149
Intellectual Property: Basis and Impediments to Effective Protection	Chioma O. Nwabachili Chudi C. Nwabachili	171
An Overview of the Same Sex Marriage (Prohibition) Act, 2013	L.O.C. Chukwu	183
Case Review		
Automated Teller Machine (ATM): A Review of *Sunday Chris Ugwu v. First Bank of Nigeria Plc*, Suit No. E/484/2009	Herbert A. C. Umezuruike	203

THE NIGERIAN LAW JOURNAL
Vol. 18, No. 1, 2015

EDITORIAL BOARD
Professor Felicia N. Monye: Editor-in-Chief, Faculty of Law, University of Nigeria, Enugu Campus
Professor Oluyemisi Bamgbose., Faculty of Law, University of Ibadan, Ibadan
Professor Ambrose O. O. Ekpu, Dean, Faculty of Law, Ambrose Alli University, Ekpoma.
Professor Mohammed L. Ahmadu, Faculty of Law, Usman Danfodiyo University, Sokoto
Idowu Adegbite , Associate Prof. and Ag., Dean , Faculty of Law , Olabisi Onabanjo University , Ago - Iwoye , Ogun State.
Dr. Bunmi Akaakar, Faculty of Law, Rivers State University of Science and Technology, Port Harcourt.
Dr. Yusufu Y. Dadem, Deputy Director General and Head of Campus, Nigerian Law School, Kano Campus, Bagauda
Dr. Timothy F. Yerima, Associate Professor and Acting Dean, Faculty of Law, Kogi State Unversity Anyigba
Dr. Yusuf Mohammed, Faculty of Law, University of Maiduguri, Maiduguri

This Journal should be cited as (2015), Vol. 18, No. 1, Nig. L. J.

Published in 2015 by
The Nigerian Association of Law Teachers,
The Secretariat,
The Nigerian Association of Law Teachers,
C/o Professor Felicia N. Monye
Faculty of Law, University of Nigeria, Enugu Campus, Nigeria
Phone: 234 803 4529597
E-mail: nigerianlawjournal@gmail.com

ISSN 0189 0255

© 2015 The Faculties of Law of Nigerian Universities, the Nigerian Law School, and the Nigerian Institute of Advanced Legal Studies
All rights reserved.

Printed by: Chenglo Ltd,
No. 6 Plot 1123 ECA Moneke Crescent
Corridor Layout Enugu
E-mail: chengloltd@yahoo.com
Phone: 234 803 7032 855

CONTENTS

Articles

The Nigeria Police and Problems of Cybercrime Investigation: Need for Adequate Training
Ikenga K.E. Oraegbunam 1

The Role of the Police in Free and Fair Democratic Elections in Nigeria: The Legal Framework
Professor Adedokun A. Adeyemi 29

The Imperative of Imposing Penal Sanctions for the Willful Transmission of the Ebola Virus and Other Infectious Diseases in Nigeria
Osinibi, Olusegun Michael 52

Law, Development and the Nigerian Oil and Gas Refineries
Idowu Adegbite 72

An Overview of the Arms Trade Treaty 2014
Daniel U. Nnam *Esq*
Ugwuozor C. Walter *Esq.* 107

Compensation for Victims of Crime in the Nigerian Criminal Justice System: The Need to the Need
Elizabeth Ama Oji 120

Dynamics and Challenges of Internal Displacement In Nigeria: A Critical look at the Law
Awhefeada, Ufuoma V. (Mrs.) 149

Intellectual Property: Basis and Impediments to Effective Protection
Chioma O. Nwabachili
Chudi C. Nwabachili 171

An Overview of the Same Sex Marriage (Prohibition) Act, 2013
L.O.C. Chukwu 183

Case Review

Automated Teller Machine (ATM):
A Review of *Sunday Chris Ugwu v. First Bank of Nigeria Plc*,
Suit No. E/484/2009
Herbert A. C. Umezuruike 203

Call for Papers 211

THE NIGERIA POLICE AND PROBLEMS OF CYBERCRIME INVESTIGATION: NEED FOR ADEQUATE TRAINING

By
Ikenga K.E. Oraegbunam*

Abstract

Cyber criminality presents unique problems of investigation for prosecution due to the global nature of the Internet. On the Internet where territorial boundaries disappear, criminals can operate from any part of the globe. Thus, the transnational nature of cyberspace poses significant difficulties for law enforcement and prosecution, which ordinarily must take place within national borders. Unfortunately, an adequate global uniformity or harmony needed for fighting cybercrime is not available even as anti-cybercrime laws are still lacking in many developing nations including Nigeria. Added to this is the near anonymity of the offenders. Hence, it is discovered that while computer technology will continue to be used in not only novel but also many traditional crimes, the nature and particular features of these crimes will pose new and unique challenges for investigators. To reduce the rate of cybercrimes in Nigeria, therefore, this study advocates for the establishment of computer forensic department within the Police and adequate training and retraining of those who man proposed the unit. The paper also recommends that those who are knowledgeable in the affairs of computer technology should be enlisted in the recruitment process of the Police.

Key Words: Nigeria Police, Cybercrime, Investigation, Training, Jurisprudence

* PhD (Law), PhD (Rel. & Soc.), PhD (Phil.), MEd, BL, Senior Lecturer, Department of International Law & Jurisprudence, Faculty of Law, and Deputy Director, Special Projects, Nnamdi Azikiwe University, P.M.B 5025 Awka, Anambra State, Nigeria. E-mail: ikengaken@gmail.com. Phone: +2348034711211.

1. Introduction

The Constitution of the Federal Republic of Nigeria 1999 (as amended) establishes a Police Force for the Federation.[1] Police matters are exclusively of federal legislative competence such that the Police institution is to be organised and administered in accordance with the provisions of an Act of the National Assembly.[2] The law which provides for such organisation and administration is the Police Act.[3] Thus, the Nigeria Police shall have such powers and duties the exercise of which is subject to the Act as consistent with the Constitution.[4] The Police and its powers and duties are therefore ultimately subordinated to the rule of law.[5] Accordingly, the Police is vested with the power to arrest any offending citizen;[6] to detain and search his person;[7] search his property;[8] take his finger print;[9] and conduct prosecutions in courts of law.[10] These powers are quite expansive, but they must be exercised within the law.[11]

Be that as it may, one of the inherent duties of the Police in common law jurisdictions (among which is Nigeria) is investigation. This is in line with the Anglo-Saxon adversarial justice system wherein the executive arm of government as represented by the Police conducts investigations in relevant situations to establish a

1 Section 214 (1) of 1999 Constitution (as amended): "There shall be a police force for Nigeria, which shall be known as the Nigerian Police Force, and subject to the provisions of this section no other police force shall be established for the federation or any part thereof". See also section 3 of Police Act.

2 See generally S. Nchi, *Separation of Powers under the Nigerian Constitution*, Jos: Greenworld Publishing Company, 2000, p. 88.

3 Cap P19, Laws of the Federation of Nigeria 2004. See also Criminal Procedure Act, Cap C 41, Laws of the Federation of Nigeria 2004, sections 3-11; Sheriffs and Civil Processes Act, Cap S 6, Laws of the Federation of Nigeria 2004, sections 7-15.

4 The Constitution, of the Federal Republic of Nigeria 1999 (as amended), section 214 (2) (b). See also section 1(3) of the Constitution.

5 Ibid.

6 The Police Act, sections 24-27.

7 Ibid, section 29.

8 Ibid, section 28.

9 Ibid, section 30.

10 Ibid, section 23.

11 For instance, section 35 (2) (3) & (4) of 1999 Constitution imposes some limitations on the exercise of Police powers by ensuring that the Police follow certain due process of law especially as relates to their powers of arrest and detention of citizens.

prima facie case prior to prosecution.[12] While investigation may be easy in relation to conventional crimes, it is hard to undertake in combating cyber criminality. The reasons are obvious. Digital information or data consisting in 'zeros' and 'ones' are the form in which the emerging Internet society carries out its activities, whether through software applications, email, data feeds or the Web. More still, the global economy and interaction have become increasingly dependent on the processing and transmission of such data across networks to support its infrastructure and carry out many of its functions. Unfortunately, this advent of the Internet and the proliferation of digital regime have also created new opportunities for those who engage in criminal and other illegal activities. Apart from a dramatic increase in the incidence of crimes, there is also an evolution of new varieties in criminality. Certainly, old forms of crimes such as fraud, gambling, piracy, forgery, cheating, terrorism, criminal defamation, stealing, and the like, receive more boost and fillip as a result of the speed, convenience and worldwide coverage of the Internet. In addition to these old crimes in *new wine skins*, are yet new types of offences such as electronic mail scams, cyber stalking, page jacking, salami attacks, Internet time theft, electronic mail bombing and spoofing, unauthorised access to computer systems or network, and so on, that are created and aided by same qualities. The result is that cyber criminality constitutes an obstacle to growth of information technology. It is also a hindrance to economic development and an impediment to good social relations and value orientation. Cyber criminality blurs Nigeria's international image. It is an instrument for breach of fundamental rights. It can invade automated data system and attack cryptology. It is also a device for an assault on the person of an individual and for incursions on his property especially intellectual property.

No doubt, when cybercrimes are committed, the ability of the Police to investigate and prosecute the perpetrators will be driven, in part, by the availability and accessibility of relevant data or information to the investigators, whether in the context of intelligence gathering, evidential retrieval or subsequent analysis and presentation in court. The snag is that such data may be held on systems controlled by the suspect, a victim or a third party service provider, particularly a communications service provider. Other indices that can constitute *obex* to smooth investigation of cybercrimes include the speed at

12 This is unlike in inquisitorial tradition where the powers of investigation reside in the adjudicating judge.

which offences can be committed, high cost of investigation, and the potential for deliberate exploitation of sovereignty issues and cross-jurisdictional differences by criminals and organised crime outfits. Similar to this is the volatility or transient nature of evidence, including frequent lack of collateral or forensic evidence. Unfortunately, as at the present, those committing cybercrimes in Nigeria appear to be smarter than investigation agencies.

This paper examines the problems and some fundamentals of digital forensic investigation only through which deep and reliable evidence for prosecution of cybercrime cases would be gathered. It is apt to note, however, that this study is concerned with the problems raised by data for law enforcement agencies investigating network-based crimes. It begins with a review of the field of computer and network forensics. Besides, as a study in law, it is neither within its scope nor indeed within the competence of the writer to engage in a detailed examination and critical analysis of the various forensic techniques employed in computer and cybercrime investigations. The study is limited to giving attention to the two key elements of the activity, namely, identifying the suspect(s) and obtaining data related to the suspect's activities. Ultimately, it enquires into the readiness or otherwise of the Nigeria Police to investigate cybercrimes with a view to combating the menace at least in view of the country's Vision 20:2020. Finally, certain relevant recommendations are made towards the end of the paper.

2. Idea of Criminal Investigation

Before examining the nature and process of digital forensics and investigation which constitute the domain of cyber criminality, it may be apt to first consider the meaning and the trajectory of criminal investigation generally. Such a study would be helpful in determining the extent of the peculiarity and uniqueness of the investigation of computer crimes and cybercrimes.

Criminal investigation embodies everything done by an authorised agency or person, within the law, for the purpose of determining what crime has been committed, who committed the crime, where the crime was committed, why the crime was committed, when the crime was committed and how the crime was committed with a view to bringing the offender to book. It should be noted that the aim of bringing an offender to book after investigation mainly differentiates criminal investigation from any other type of investigation. Criminal investigation has been defined as a "lawful search for people and things to reconstruct the circumstances of an

illegal act, apprehend or determine the guilty party, and aid in the state's prosecution of the offender".[13]

Criminal investigation is usually a detailed and systematised examination or search to achieve any or all of the above stated goals and resolve all the relevant issues raised by them or any of them. From the foregoing, three distinguishable aspects of criminal investigation stand out as follows: discovering what crime has been committed from alleged or available facts; identifying the person that committed the crime; and collecting sufficient evidence to show or prove the guilt of the offender in court. In his attempt to find answers to any of or all the foregoing question(s), a criminal investigator is expected to follow laid down rules and procedures; otherwise adverse legal consequences may follow.

Momodu highlights the questions[14] which an investigator should find answers to in the course of criminal investigation. The first question is to ascertain what crime was committed. Crimes are generally reported by victim(s) or witnesses of the crimes. The fact given of a crime reported by a victim or witness is, in most cases, enough to give an investigator an idea of what crime has been committed. However, an investigator is expected to take active steps to discover the actual crime that has been committed. It is also necessary to know who committed the crime. Perhaps, the identification of the offender is one of the most difficult questions in criminal investigation. Criminals rarely confess to having committed any crime. Yet, circumstantial evidence as the next alternative is fraught with the problem of accuracy. Moreover, the secrecy with and in which crimes are committed may make eye witness of criminal activities impossible.[15] Yet experts can process physical or trace evidence for tendering in court and an accused person may be convicted when such evidence is supported by credible expert witness testimony[16]. Furthermore, a suspect could be identified by the

---

13 R. Bohm & K. Haley, *Introduction to Criminal Justice*, 3rd ed. Cambridge University Press, Cambridge, 2002, p.206.

14 B. Momodu, *Law and Practice of Criminal Investigation and Prosecution in Nigeria*, Stirling-Horden Publishers Nig. Ltd., Lagos, 2007, pp.2-7.

15 This was judicially acknowledged by the Supreme Court in *Emeka v State* (2001) 14 NWLR 666.

16 Although the court would normally accept unchallenged and uncontradicted evidence of an expert, yet it is not bound to do so. It is only when expert witness is credible that it would be accepted by the court. Therefore, in trying to discover the author of a crime, absolute reliance should not be placed on result of forensic analysis or expert witness testimony as court may refuse to rely on it for whatever legal reason, the investigator should also

method he is known to operate, known as the *modus operandi*.[17] This approach is based on the fact that criminals tend to repeat a method that usually brings complete success to their exploits. An investigator must therefore be careful at the scene of crime to look out for characteristic behaviour and procedure to compare with methods and patterns of known criminals. Another way an offender may be identified is through identification parade.[18]

More still, the question of where a crime was committed is important and must be resolved during investigation as it forms one of the particulars by which notice of the commission of an offence may sufficiently be given to a suspect if he is eventually taken to court.[19] The place of the commission of an offence is also important as it may determine which court may assume jurisdiction in the matter.[20] It is therefore necessary for investigation to reveal the place where the offence was committed. Quite another issue is to know why the offence was committed. Although generally the motive by which a person is induced to do an act or to form an intention is immaterial so far as regards criminal responsibility[21], yet it may be necessary for an investigator to unravel the motive of the offender to give a clue to the prosecutor of the possible defence the offender is likely to rely upon during prosecution. Also the investigator, knowing the motive, has been put on notice. That investigator would then have to gather evidence that would counter the speculated defence. Moreover, motive by which a crime was committed goes a long way in determining the pattern of investigation. When motive is not identified, the range of possible suspects is wide and that would certainly make investigation difficult.

look out for other evidence, where available, pointing to the guilt of the accused person (See *State v Ejiofor & Ors* (1983) 1 NCR, p.86).

17 *R v Mortimeri* (1936) 25 C. App. R 150; *R v Smith* (1914) All ER 202, (1915) 11 Cr. App. R 229; *R v Armstrong* (1922) All ER 153.

18 *The State v Aibangee* (1988) 3 NWLR (pt. 84) 548; *Eyisi v The State* (2001) 8 WRN 1 at 39; But see *Tajudeen Alabi v The State* (1993) 7 NWLR (pt. 307) 511, (1993) 9 SCNJ (pt.1) 109. See also *R v Turnbull* (1976) 3 All ER 549 at 551-552

19 Section 202 Criminal Procedure Code (CPC) cap 30, Laws of Northern Nigeria1963 (now adapted by the individual states of the old northern Nigeria); Section 152 (1) Criminal Procedure Act (CPA), cap C 41, Laws of the Federation of Nigeria 2004..

20 Section 134 CPC

21 See the 3rd paragraph of Section 24 of the Criminal Code. Criminal Code is the schedule to the Criminal Code Act, Cap C 38, Laws of the Federation of Nigeria 2004 (now adapted by the states of the old southern Nigeria).

Furthermore, the question as to when the crime was committed is quite salient. Like the place of the commission of a crime, the time of the commission of a crime is important as it forms one of the particulars by which notice of the commission of an offence may sufficiently be given to the suspect during arraignment.[22] Time of the commission of the offence is also important to determine whether by reason of time, the prosecution of the offence is statute barred. Finally, laws are by nature not retroactive; thus the time a crime was committed must be investigated to determine whether the purportedly breached law was in existence as at the time the alleged offence was committed.[23]

Lastly, it may be apt to demonstrate how the crime was committed. This is the final stage of the process of investigation which consists in the gathering or collection of evidence to show in the law court how a crime was committed. The investigator should be able to narrate the sequence of activities of the accused with the evidence he/she has gathered. It is not all types of evidence that the court would rely on against the accused person. The investigator is to gather only admissible and reliable evidence to be used in convincing the court that the accused committed the crime. If the court is not convinced, no matter how certain the investigator is about the fact that the accused committed the crime, the court would not convict him. In order to gather admissible evidence that the court would rely on to convict an accused person, there are rules and procedures laid down by law which must be adhered to in the conduct of criminal investigation. The discussion of these rules and procedures is however beyond the scope of this paper.

Summarily, the investigation process is generally divided into two parts: the preliminary investigation and the follow-up investigation[24] discussion of which is also beyond the scope of this

22 Section 202 CPC; Section 152(1) CPA.

23 Section 36(8) of the Constitution of the Federal Republic of Nigeria 1999 (as amended): "No person shall be held to be guilty of a criminal offence on account of any act or omission that did not, at the time it took place, constitute such an offence, and no penalty shall be imposed for any criminal offence heavier than the penalty in force at the time the offence was committed".

24 Preliminary investigation embodies the actions taken by the first officer to arrive at the scene of crime after its detection and reporting. During preliminary investigation an investigator is expected to take note of all notable information such as the time the offence was said to have been committed, and time of other significant happening before, during and after the commission of the offence, date of the commission of the offence and date the offence was reported if different from date of commission of the offence. A follow-up

work. Suffice it to note that the investigators' duties include tracking down suspects; getting witnesses to testify; collecting items of evidential value; analysing the evidence obtained; preserving the evidence; conducting interviews for witnesses; interrogating suspects; conducting searches, writing reports on cases investigated or under investigation; preparing case files; and testifying in court[25].

3. Nature and Process of Cybercrime Investigation

It is apt to delineate the meaning of cybercrime before discussing the nature and process of cybercrime investigation. In its most simplistic form, cybercrimes can be described as criminal actions committed on cyberspace. They are of two major categories: crimes committed solely with the aid of the Internet, which were unknown to criminal laws prior to the advent of the Internet. Examples of such will include dissemination of viruses and other malicious codes. The second category relates to crimes which became enhanced through the aid of the Internet. These criminal activities were committed traditionally, but have been introduced to the cyberspace and their operations have been aided by Internet's anonymity and inventiveness. An Example here is online fraud.[26] It is about this second category that the term 'cybercrime' has been described as a misnomer. Hence, the concept of cybercrime is seen as not radically different from that of conventional crime. It is argued that both include conduct, whether act or omission, which causes breach of rules of law and counter-balanced by the sanction of the state[27].

However, cybercrimes may be said to be of those species of which the conventional crime is, and where either the computer is an object or subject of conduct constituting the crime. "Any criminal activity that uses computer either as an instrumentality, target or means for perpetuating further crimes comes within the ambit of cybercrime."[28] It is a criminal activity done using computers and the Internet. This includes anything from downloading illegal music files

investigation is every aspect of investigation conducted after a preliminary report based on preliminary investigation carried out up to the stage when the case is referred for prosecution (See Swanson, Chamelin, and Territo, *Criminal Investigation*, 8th Edition, McGraw Hill, London, 2003, p.30).

25 B. Momodu, *Op. cit.*, p.16.

26 D. Ashaolu, "Combating Cybercrimes in Nigeria 1",*McAsh's Thoughts*, December 24, 2011.

27 http://www.crime-research.org/articles/joseph06/2. Last visited on 26-07-12.

28 S.36 (12) of the Nigerian Constitution provides that no person shall be penalised for an offence that is not defined in a legislation enacted by the law making body.

to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting business information on the Internet.[29]

Cybercrime encompasses any criminal act dealing with computers and networks. It includes traditional crimes conducted through the Internet. For example, hate crimes, telemarketing and Internet fraud, identity theft and credit card account theft are considered to be cybercrimes when the illegal activities are committed through the use of a computer and the Internet.[30] Thus, it is a crime committed on the Internet by using the computer as either a tool or a target[31]. The general definition of cybercrime may be "unlawful acts wherein the computer is either a tool or a target or both".[32] The computer may be a tool in the following kinds of activity - financial crimes, sale of illegal articles, intellectual property crimes, pornography, e-mail spoofing, cyber stalking and forgery. The computer can also be a target for unlawful acts in the cases of unauthorised access to a computer, e-mail bombing, data dialing, logic bombs, Trojan attacks, and web jacking.

There is no gainsaying that prosecution of a suspect in respect of any of the above criminal conduct requires thorough investigation. Yet, the investigation of cybercrime and the gathering of appropriate evidence for a criminal prosecution via, for instance, the science of 'forensic computing', 'digital forensic' or 'cyber-forensic' is by no means an easy task. This is primarily due to the intangible and often transient nature of data, especially in networked environment. The technology renders the process of investigation and recording of data for evidence extremely vulnerable to defence claims of errors, technical malfunction, prejudicial interference or fabrication. Such claims may lead to a ruling from the court against the admissibility of such evidence.[33]

It goes without saying that the task of investigation is all the more difficult when crimes are committed in cyberspace. The response to the question of what and where cyberspace is still forms a conundrum. How then would an investigator identify the author of

29 D. Pawan, *The Internet: Legal Dimensions*, Research Study, University of California, 1990.

30 www.techtei-ms.com/../c/c. Last visited on 12- 04-11.

31 Sbc.webopedia.com/../cybercrime-crime.html. Last visited on 11-08-11.

32 http://www.crime-research.org/articles/joseph06/2. Last visited on 26-07-12.

33 I. Walden, *Computer Crimes and Digital Investigation*, Oxford University Press, New York, 2007, Chapter 6.

an offence committed within such an unclear, unspecified, and hardly determinate *locus criminis*? One of the important aids in the identification of the author of a crime is forensic science. In puzzling criminal situations where identification of the offender(s) appears unlikely, forensic science has unravelled the perpetrator of a crime. Momodu succinctly puts it:

> When a crime is committed, the scene of the crime is rich with trace evidence that could be analysed. Forensic experts can analyse trace evidence found at crime scene and with it pin down a particular individual to a specific place and/or time and link him to the crime in issue. Trace evidence can be identified by class or individual characteristics, physical matches and mathematical probability. Finger prints (whether visible or latent) found at crime scene may link an offender to a crime. With the development of Automated Fingerprint Identification System (AFIS), thousands of sets of stored fingerprints can now more easily be stored for a match with those of a suspect. Proper document examination by an expert, who examines the handwriting, typewriting, ink, paper, typography etc., may also link an offender to a crime. Again, firearm examination using ballistic techniques by an expert who examines the type of weapon, the specific weapon used to fire a bullet, the distance between the weapon and the target and whether a suspect fired a weapon in the first place, may also link a suspect to a crime. Moreover, blood, semen and other body fluids which are usually spilled after a violent crime may be analysed, individualised, and therefore may be used to link an alleged offender to a crime. Hairs, fibres, even inorganic substances such as paint, glass found at the scene of crime may also be used to prove a case against a suspect, as they can be subjected to analysis by an expert to discover traces that may indicate some of the characteristics of the suspect or his property[34].

Walden observes that law enforcement investigative techniques are generally subdivided into coercive and covert techniques, the former involving powers of search and seizure, the latter involving interception and surveillance[35]. In contrast to other forms of crime, the investigation of cybercrimes will more frequently involve the deployment of techniques falling into both categories of activity. Covert techniques are generally used at an earlier stage in the investigative process, for the gathering of intelligence as much as evidence, while coercive techniques are used primarily to gather evidence once the relevant ICT (Information and Communications Technology) resources have been identified. A particular technique used, or investigative power exercised, at different points in an investigation may therefore form part of either a covert or coercive investigative process. Law enforcement access to data about whom a person has called on phone or sent an email, for example, may be used to identify persons to be placed under surveillance, or post-arrest to establish evidential links between accused persons.[36]

It may be proper to note that, in practice, a criminal investigation can often interfere with the rights of others, whether the person is the subject of the investigation or a related third party. In a democratic society any such interference must be justifiable and proportionate to the needs of society to be protected[37]. However, the growth of network-based crimes has raised some unique and difficult issues in respect of the appropriate balance between the needs of those investigating and prosecuting such crimes, and the rights of network users to privacy.

There are also the interests of communications service provider (CSPs), the intermediaries that build and/or operate the networks and communications services through which data is communicated. Law enforcement agencies will be looking towards such intermediaries to assist them in the investigative process, either in terms of gathering data transmitted by the suspects themselves or providing data generated by the CSPs about the communication activities of suspects. Such assistance may be provided on either a

---

35 I. Walden, *Computer Crimes and Digital Investigation*, Oxford University Press, New York, 2007, p. 203.

36 *Ibid.*

37 Section 45 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended).

voluntary or mandatory basis, which also raises important legal issues for consideration.[38]

Be that as it nay, it is good to note that three main avenues for obtaining forensic data are discernible. First, data can be obtained from the suspect covertly through various forms of surveillance. Second, data can be gathered from a communications/Internet service provider, whether in the course of a covert investigation or otherwise. Third, data can be garnered coercively from the suspect, through the exercise of search and seizure powers. These are currently the primary sources of evidence in cybercrime investigations[39].

It is therefore necessary to briefly consider two key challenges in a digital investigation, namely, identifying the suspect and obtaining data relevant to the suspect's criminal activities. But before then, consideration is given to some of the problems that handling data creates for investigators. What then are some of the data problems in a cybercrime investigation? Data in the digital environment raises a range of problems for investigators, many of which require not only specialist technical skills, but also an appropriate procedural framework designed to tackle these problems. The first of these is the 'identity problem'. How does one establish an adequate forensic link between an item of data and the virtual identity of the person to whom the data relates; and then between the virtual identity and a real world person? Establishing identity is widely recognised as being one of two key problems in a cybercrime investigation that is likely to become worse over time.[40]

The second problem may be referred to as the 'location problem', although this really covers three distinct issues arising from where the data is to be found. Related to resolving the 'identity problem' is the obvious need to identify the physical location of the suspect. In a mobile phone context, for example, cell site analysis may determine whether the suspect in possession of an identified handset was present in the locality at the relevant time. Location also has jurisdictional implications, since cyberspace activities cross state borders requiring investigators to seek data residing outside their national jurisdiction and their legal competence.[41]

---

38 For the purpose of this discourse, a mandatory requirement for a CSP to provide assistance is not being classified as a coercive policing technique.

39 I.Walden, *Op. cit.*, p.204.

40 Ibid, 'Digital Evidence – the Emerging Specialties'.

41 See generally I. Walden, *Op.cit.*, chapter 5.

The third aspect of the location problem arises from the fact that forensic data may also be present within a network forming part of, or connected to, the Internet, and/or may be found on terminal equipment operating at the edges of the network. The law sometimes treats data obtained within a network differently from that same data when it is at the edges of a network. In addition, data may reside, or be at rest, on the ICT resources of the victim, the suspect or some third party, such as a CSP or online service provider (e.g. credit card company or search engine[42]). Alternatively, the same data may be obtained in the process of it being transmitted across a network, generally referred to as intercepted data. Specific rules of criminal procedure address law enforcement access to these different sources of evidence: data 'at rest' and data 'in transmission'. Indeed, such a situation has been recommended, in order to facilitate cybercrime investigations: "the legal distinction between searching computer systems and seizing data stored therein and intercepting data in the course of transmission should be clearly delineated and applied".[43]

More still, the nature of ICTs bestows upon data the duality of being notoriously vulnerable to loss and modification, as well as being surprisingly 'sticky'[44], at one and the same time. These characteristics may be referred to respectively as the 'integrity problem' and the 'stickiness problem'. The former meaning the process of obtaining forensic data is a significant technical challenge for investigators, since it may modify the source data or its related meta-data, thereby fatally undermining the evidential value of the forensic material. Indeed, the manner in which an investigator interacts with data creates further problems due to the confused treatment of intangible information.

On the other hand, the 'stickiness' of data is attributable, in part, to the multiple copies generated by the communications process, particularly in an Internet environment, as well as the manner in which data is held and removed on electronic storage media. While

---

42 Google, for example, is alleged to maintain cookies about the web-searching history of its users for substantial periods of time. See *The Observer*, 'Our internet secrets stored for decades', 2 October 2005.

43 Council of Europe Recommendation No R (95) 12, 'concerning problems of procedural law connected with information technology', at principle 1.

44 'Sticky' connotes the idea of inability to modify the data or even to retrieve the data for the purpose of evidence and/or prosecution. the 'stickiness' of data is attributable, in part, to the multiple copies generated by the communications process, particularly in an Internet environment, as well as the manner in which data is held and removed on electronic storage media.

the 'stickiness' of data will generally work to the advantage of an investigator, the availability of data may not enable a successful prosecution where the defendant is unaware of its existence. Conversely, the widely held perception that data held on an ICT resource is transient may work to the advantage of an accused, where he can raise doubt as to the existence or otherwise of relevant forensic data. In the English case of *Callfrrey,*[45] for example, the defence counsel was able to create sufficient doubt in the minds of the jury as to the existence of a Trojan horse virus on the defendant's private computer (PC) at the relevant time for the defendant to be acquitted, despite expert testimony to the contrary.

Related to the 'stickiness' problem is the 'analysis' problem created by the volume and nature of the data that an investigator may be required to handle in the course of an investigation. Modern data media, such as hard drives, DVDs and memory sticks are capable of storing vast amounts of data, while networks are capable of transmitting huge bit streams of data over channels and across nodes. Again, while an investigator may be able to obtain and preserve such data in a relatively straightforward manner, through the exercise of seizure or interception powers, the ability to access, manage and analyse it for subsequent presentation in court can present very significant problems, from the need to overcome protection mechanisms, to the availability of appropriate resource within any time limits imposed by law.[46]

Digital evidence may comprise the content of a transmission or, more frequently, the attributes of a communications activity, or 'meta-data', that identifies and describes the content of a transmission and its management by an ICT resource. The digitisation of information also means that traditionally distinct forms of data are represented in a common language i.e. - binary machine code. Taken together, these features create a 'data type' problem, where existing legal rules treat the obtaining of different types of forensic data differently; the law governing interception, for example, being only applicable to the obtaining of communications content. Distinguishing different types of data and determining the applicable procedural regime governing the obtaining of such data can be a significant challenge for investigators. No doubt, the inability to adequately address some or all of the data problems can have a direct impact on the prosecutorial process, especially evidential

45 Southhwark Crown Court, 17 October 2003.

46 E.g. *Magistrates' Courts Act* 1980, section 127; *Prosecution of Offences Act* 1985, section 22, and *Computer Misuse Act*, s 11(2), (3).

admissibility and the probative value of any forensic data.[47] This section considers both the technical challenges and the legal rules that relate to these data problems.

One veritable aspect of data problems borders on traceability. This is real as one classic aphorism of the Internet age is that "On the Internet, nobody knows you are a dog'.[48] However, in the course of an investigation, the investigator will need to identify the person carrying out the illegal activity. The process of establishing a real world person's identity from their Internet-related identity creates a significant forensic and legal hurdle. Broadly speaking, there are two initial sources of forensic data to assist in the identification process: that created by a suspect's use of communications services; and the content of a person's communication activities. In the former case, attempts are made to identify the source, and often the recipient, of a communication, based on some form of unique identifier. The identifier will generally identify the terminal equipment from which the communication originated, such as a telephone number or PC, and may identify a specific user, such as an email address. However, where the terminal equipment resides in an environment where multiple persons have access, whether at home, the office or a public place, proving that a specific person was using the equipment or account at the relevant time is an obvious problem, and potential defence. Successfully completing this forensic trail to a real person, therefore, raises substantial challenges for investigators.

In the second scenario, investigators may be able to obtain various data elements that a suspect has disclosed in the course of his activities, which can be traced back to the suspect. Such content may be disclosed knowingly, but unwittingly, or inadvertently, such as 'cookies'.[49] In the English case, *Vallor,*[50] for example, the virus writer was identified through the posting he made to various Internet bulletin boards boasting about his activities, under the name of 'Gobo'. One common means of identification is through payment data, such as credit card details, used to access and purchase online

47 See generally I.K.E. Oraegbunam, *Jurisprudential Problems in Fighting Cybercriminality in Nigeria: Need for Panacea*, Ph.D. Dissertation in Law, Nnamdi Azikiwe University, Awka, Nigeria, 2012, Chapter 6.

48 New Yorker cartoon, 5 July 1993.

49 'Cookies' can be configured to include user names, passwords and other identification data.

50 *Vallor* [2004] 1 Cr App R (S) 319.

services. In the child abuse case *Landslide*[51] and subsequent 'Operation Ore' in the United Kingdom, for example, the primary source of identification evidence was credit card details given by subscribers.[52] Also, in the cyber-espionage case, *Haephrati*,[53] the suspects were traced, in part, through the use by one of the accused of his American Express credit card to open an email account used to send messages with a virus attached.[54] In June 2006, it was revealed that SWIFT, the international electronic funds transfer network based in Brussels, had transferred transactional financial data contained in millions of records to the US Government, as well as enabling the US authorities' direct access.[55] Indeed, such payment details may not only be valuable in the investigative stage, but may subsequently be used as a component of a crime prevention strategy, enabling a payment service provider to close an account used in the course of criminal conduct.[56]

While it is beyond the scope of this study to examine the full range of technical means available to identify persons in a cybercrime environment, it is valuable to briefly examine some of the complexities that arise when an investigator needs to resolve an IP address to an individual. When utilising any Internet-based service, such as email, the originator and recipient of a message require an IP address, a unique number that identifies the relevant resources.[57] That IP address is then logically linked to the originator's pseudonym and domain name, for instance, ikengaken@gmail.com. However, while the IP address is unique, the person to whom it is linked will usually vary. Internet Service Providers (ISPs) and corporate networks will

51 Reported in I. Walden, Op. cit., p.170. US Department of Justice Press Release, 'Thomas Reedy Sentenced to Life Imprisonment in Child Porn Case', 6 August 2001. See also *US v Reedy*, 304 F 3d 358, 60 Fed R Evid Serv 133 (5th Cir (Tex) 26 August 2002).

52 Reported in I. Walden, Op. cit., p.170.See BBC News, 'Operation Ore: Can the UK cope?', 13 January 2003. Available at http://news.bbc.co.uk. Accessed on 16/07/14.

53 Reported in I. Walden, *Op. cit.*, p.170.

54 See Government Opening Note in *The Government of Israel v Michael and Ruth Haephrati*, drafted by John Hardy, Counsel, delivered at Bow Street Magistrates' Court, 26 August 2005, at para 10.

55 *New York Times*, 23 June 2006.

56 E.g. the *Data Protection (Processing of Sensitive Personal Data) Order* 2006 (SI No 2068).

57 In IPv4, uses 32 bit addresses written in dot. decimal notation comprising four octets, eg 38.111.64.2. The new IPv6 uses 128 bit addresses written as eight groups of hexadecimal digits, eg 1002:0db8:0770:003c:0546:0000:1428:57ab. See generally http://en.wikipedia.org.

generally, for reasons of efficiency, dynamically assign an IP address to a user each time they log onto a service or at the commencement of each communication session.

Identification in a cyberspace environment may therefore be a four-staged process.[58] First, it is necessary to identify the IP address that needs to be resolved to a machine or person. These will generally be found on logs generated by the specific application utilised by the suspect, such as the web or mail server of the victim or an intermediary ISP.[59] The recorded sourced IP address may, however, have been 'spoofed', where a false source IP address is inserted in the packet headers. While 'spoofing' may be carried out at an individual user level, it may also be done on a commercial level, as a service offered to users wanting to use the Internet anonymously, sometimes referred to as a 'darknet' service.[60]

Second, one has to establish the entity, such as an ISP, to whom the IP address has been assigned. This can be relatively straightforward, for example using *'who is'* software to interrogate one of the regional or local registry databases, detailing IP address allocation.[61] However, since the registries may not have a requirement to verify such information, a large proportion of it is often inaccurate, either because false information was supplied in the first instance, or because the information is not kept up to date. An alternative or supplement to registry lookup is to use a 'trace route' application to follow the route of the packets across the Internet.[62] In either case, if accurate, an IP address holder will be found. Generally, this will be a service provider or organisation, although an individual may be identifiable if he has a fixed IP address, then the registry may effectively identify the owner of the machine.

58 R. Clayton, "Anonymity and Traceability in Cyberspace", *University of Cambridge, Computer Laboratory, TechnicalReport*,UCAM-CL-TR-653, November 2005. Available at http://www.cl.cam.ac.uk/TechReports/UCAM-Cl-TR-653.html. Accessed on 16/07/14. See also LINX, "Best Current Practice – Traceability", May 1999, available from http://www.linx.net. Accessed on 16/07/14.

59 Ibid., p 28.

60 http://www.anonymizer.com; https://www.relakks.com/. Accessed on 16/07/14.

61 B. Nikkel, 'Domain Name Forensics: A Systematic Approach to Investigating an Internet Presence'. *Digital Investigation* (2004) 1, pp.247-55.

62 See http://www.webopedia.com/TERM/T/traceroute.html Accessed on 16/07/14.

Where blocks of IP addresses belong to a service provider or organisation, the third stage will be to approach the IP holder to match the target IP address to a specific user at the relevant time.[63] This may be achieved by studying one or more historic logs, such as a RADIUS log for dial-up account authorisation, which will generally record the start and end of a session; or the log of a DHCP system, for dynamically allocated IP addresses.[64] Such a process will clearly not be possible where the IP holder provides an anonymous public service such as a cyber café; or the user has logged on to an unsecured wireless network, or, most commonly, the IP holder does not maintain or retain a complete or sufficiently detailed log of IP address allocation.

The final stage is to obtain the subscriber's account details, such as home address, from the ISP's administrative records. As with the third stage, the existence of administrative records will depend, in part, on the nature of the connection being provided, as well as the method of payment for the service (e.g. direct debit). For 'free' Internet services, the key identification data may consist of the 'calling line identity' (CLI) number of the user's line.[65] As 3G mobile telephones increasingly become a standard access device for the Internet, administrative records may not exist for a large proportion of subscribers using 'pay-as-you-go' services.

The above illustrates that the ability to trace a person from their IP address is dependent on the input of different entities and the existence of various logs and records. As will be alluded to later in this paper, the forensic value of such logs and records has recently prompted some governments in some foreign countries to impose data retention requirements on ISPs operating at stages 3 and 4, in order to preserve the identification data, rather than depend on the vagaries of individual ISP practices and procedures.

Having considered the complexities involved in tracing and identifying a suspect, the next forensic challenge concerns the capability of law enforcement agencies to appropriately obtain the required intelligence or evidential data. The digital forensic process for obtaining data generally involves a number of different stages; (a) identifying what data may be available and where it may reside; (b)

63 Determining time can itself be difficult, due to machine errors and time values (e.g time zones and daylight saving).

64 See generally A. Cormack, "Log files", *JANET Guidance Note* GD/NOTE/008, June 2004. Available at http://www.ja.net/services/publications / technical-guides/gn-logfiles.pdf. Accessed on 16/07/14.

65 The CLI may identify a line or a private switch within an organization.

preserving such data in a manner that minimises interference with the original data; (c) analysis of the data for intelligence and evidential purpose; and (d) presentation of the data and evidence derived from it in a court of law.[66] There are also certain widely accepted rules or principles that govern each of these processes. The ACPO (Association of Chief Police Officers) Guide, for example, promulgates standard forensic practices for obtaining data on the basis of four key principles:

> **Principle 1: No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.**
>
> **Principle 2: In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.**
>
> Principle 3: An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
>
> Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

Be that as it may, forensic data, as noted above, may be obtained from numerous sources, victim, suspect or third party; either in the course of its transmission or when residing on a source-controlled resource, media or device. There are pertinent technical features concerning the different ICT resources from which digital evidence may be obtained. It should also be borne in mind that every incidence of cybercrime, as for any other crime, will have a unique life-cycle,

66 R. McKemmish, "What is Forensic Computing?" (No. 118), Australian Institute of Criminology, June 1999.

from first detection and reporting to any eventual proceedings.[67] Data may be held on a huge variety of types of data media. Such media vary in respect of their mobility and ease of use, from the fixed hard drive on a computer, to tapes and removable USB[68] flash drives. However, all such storage media are today becoming cheaper, have greater storage capability, and operate at greater speeds, all of which directly feed into the 'analysis' problems in terms of the volumes of data potentially involved in the forensic process. Most media have a basic four-way functionality, in terms of enabling data to be written, read, modified and deleted from the media; while some, such as CD-Rs have been developed to only enable data to be written and read. The latter have been designed to address the integrity problem for individual and commercial users, but would also be beneficial from an investigatory perspective.

Digital media store data in different ways at a physical level, such as magnetic particles and laser-created pits, as well as at a logical level, in terms of partitions, drives and sectors. The way in which a device logically handles the data it processes has direct implication for any subsequent forensic analysis. Microsoft's FAT and NTFS files systems and Unix's FFS system, for example, utilise space on the storage media in very different ways, which require the use of different analytical techniques to examine data stored by such systems. However, under all files systems, data is not necessarily stored in a contiguous manner, but rather will often be fragmented across the media, in blocks, which are only logically associated through addressing information[69].

The deletion of data from digital media may take different forms. The deletion of files in standard desktop applications will generally only result in the removal of the addressing information associated with each block of data, which logically links the various blocks comprising the contents of the file; or the files are simply treated as deleted and are renamed in another directory, such as the 'Recycle Bin' or 'Trash'. As such, the data remains on the media, and is potentially recoverable, until it has been either completely overwritten by new data, or been deleted by other means. This residual physical representation of erased data is sometimes referred

67 See Information Assurance Advisory Council, Directors and Corporate Advisors' Guide to Digital Investigations and Evidence, September 2005, at Section 3.

68 Meaning 'Universal Serial Bus'. 'Firewire' is the version used by Apple Macintosh.

69 I. Walden, *Op. cit.*, p.212.

to as 'data remanence',[70] and is one cause of the 'stickiness' data problem.

As well as the organisation of files in terms of the characteristics of the digital media, the operating system and applications that utilise the media also use systems for identifying and organising the data they operate upon, in terms of file names, extensions, folders and directories. Such systems will often maintain a wide range of valuable forensic details about the attributes of a data file, in terms of its size and usage. Usage data, such as the date and time at which actions were carried out on a data file,[71] is obviously an extremely valuable forensic source, but is also highly vulnerable to claims of inaccuracy, modification and interference. As such, it will often require some form of corroboration using other data sources, including the contents of the data file, such as a date placed in a digital photograph or the actual commission of the offence.

To address the 'integrity' problem, an investigator needs to be able to obtain the data in a manner that is complete, yet minimises the interference with the target data. Such data may simply be printed and copied, although this may create evidential vulnerabilities. Therefore, for most types of digital media, the most common technique used to obtain forensic data is that of 'imaging'.[72] Imaging involves the acquisition and creation of a complete bit stream image of the digital media, such as hard drive or smart card, in a non-invasive manner and including those areas which are not occupied by data elements. The imaging process itself will obviously generate data, such as cryptographic hash function, that may be required at a later stage to verify the authenticity and integrity of the acquisition process and any subsequent copies. A number of copies of the image are generally created, a master copy for evidential purposes, a copy on which the analysis is carried out, and a third that is provided to the suspect for his own verification and analysis purposes.[73] The images are widely accepted as an accurate representation of the original digital media, and the use of such images never appears to have been

70 See http://en.wikipedia.org. Last visited on 12/05/14.

71 The three primary date systems are creation date, last modified date and last accessed date.

72 See, e.g., Encase (http://www.encase.com) used by the majority of law enforcement agencies especially in the UK; but see also Vogon (http://www.vogon.co.uk) and I look (http://www.ilook-forensics.org). All accessed on 03/12/14.

73 See generally P. Sommer, 'Digital Footprints: Assessing Computer Evidence', *Criminal Law Review*, Special edition, December 1998, pp.34-46.

successfully challenged before the courts. Another advantage of 'imaging' is that it can allow the original digital media to be returned to the owner, such as a business, who can then continue to use the resource, thereby minimising the degree of collateral disruption and interference caused to a victim or innocent third party.

One critical element of the process of forensic analysis is the capability to map the events recorded on the various devices from which data is derived to real time, in terms of establishing an accurate chronology of the events relating to the criminal conduct. Most of the ICTs that operate within a network and at its edges will time record; yet such multiplicity, coupled with their susceptibility to inaccuracy, makes mapping events in cyberspace to the real world a considerable forensic challenge. This problem is obviously exacerbated by the transnational context and different time-zones within which such networks operate[74]. The nature of networks, such as the Internet, means that forensic and evidential data are often present in foreign jurisdictions, which situation raises complex jurisdictional issues when law enforcement agencies need to obtain such remote material.

4. Nigeria Police, Police Act, and Cybercrime Investigation: The Way Forward

The Police Act makes provisions for the organisation, discipline, powers and duties of the police, the special constabulary and the traffic wardens. Its commencement date was 1 April 1945, that is to say, exactly seven decades ago. Although the first generation computers (1937-1953) were just being built, the idea of an Internet system was not yet conceived. Thus, commission of crimes through a networked computer structure could not have been imagined by the makers of the Police Act. Hence, the Act seems to be one of those colonial relics that struggle for relevance in an era when crimes are being committed with technological sophistication and electronic precision and finesse. Yet the Police is a very fundamental institution or agency in a society which exists to maintain rule of law and order. Whether or not such an agency is of a state or a federation is immaterial. In Nigeria, in spite of the cacophonic debates on whether there is a need for state police, the 1999 Constitution despite sundry amendments still insists, at least for now, on a single police force for the entire Federation:

74 Ibid.

Although the Police Act lags behind the computer ways of committing crimes, the duties of the Police as provided by the Act are still relevant. Section 4 of the Act provides thus:

> The Police shall be employed for the prevention and detection of crime, the apprehension of offenders, the preservation of law and order, the protection of life and property, and the due enforcement of all laws and regulations with which they are directly charged, and shall perform such military duties within or without Nigeria as may be required of them by, or under the authority of, this or any other Act.

It is observed that on the face of it, this provision is wide and omnibus enough to cover the general duties of the Police and the essence of policing in a civilised society. Similarly, the powers of the Police are clearly stated in Part IV[75] of the Act, and which powers include that of conduct of prosecutions before any court (though subject to the powers of the Attorney-General[76]), arrest, search, detention, and of taking finger prints. However, in the light of combating cybercrimes, it is unlikely that the Nigeria Police is powerful enough to exercise these powers and fulfill its duties as provided for by the Act. For instance, the power of "any police officer to conduct in person all prosecutions before any court" in Nigeria as stated in section 23 of the Act melts away as a result of the dearth of technical know-how in collecting evidence via cyber-forensics and presentation of the collected data in court for the purpose of securing conviction. Again, the Police in relation to the power of arrest, with or without warrant,[77] is rendered *incapax* due to lack of training in tracing cybercriminals whose dastardly acts are often marked with anonymity or at best with pseudonymity. This is also true of the police power of search that is marred by general lack of computer appreciation and literacy which will make it impossible to navigate through applications in search of information. In the same vein, the Act which provides that *"it shall be lawful for any police officer to take, for the purposes of identification,... finger print impressions of all persons who may from time to time be in lawful*

75 Police Act, Section 23 to 30.
76 See sections 174 and 211of 1999 Constitution (as amended).
77 Ibid., sections 24 and 25. See also section 10 of the CPA.

custody"[78] does not advert to whether the members of the Nigeria Police have the requisite skills to exercise such power.

No doubt, the lack of adequate training of the Police and other law enforcement officers, prosecutors, and the judiciary, will often exacerbate the problems of investigation and prosecution of cybercrimes in Nigeria. Unlike in Nigeria, in more developed countries, substantial efforts have been made over recent years to address this training need, with the establishment of specialised facilities and courses,[79] supplemented by training courses offered by the vendors of forensic applications and services.[80] In addition, in many jurisdictions, computer forensics has become a recognised academic discipline, leading to a range of qualifications at higher education institutions.[81] In the United States of America, the Department of Justice has issued guidance on law and practice in the field: 'Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations'.[82] Such guidance becomes a de facto benchmark against which the practices of law enforcement officers and other investigators are likely to be evaluated. In addition, more formal forensic standards are being developed and promulgated in the field, which are designed to bolster the use of digital evidence.[83]

Surely, one would not be surprised at the general epistemological paucity of the Nigeria Police in fighting cybercrimes if one takes a cursory look at Article 55 (1) of the Nigeria Police Regulations[84] which provides for the twelve-month training curriculum for a cadet officer: On appointment, a cadet officer may

78 Police Act ,Section 30 (1).

79 eg in July 2005, the Entrex National Specialist Law Enforcement Centre (NSLEC) and the National Centre for Applied Learning Technologies (NCALT) launched a 'High Tech Crime First Responder E-Learning Programme' for police officers and staff. See http://www.centrex.police.uk. Last visited on 23-04-11.

80 eg http://www.sapphire.net.

81 eg the University of Glamorgan offers a BSc or HND in Computer Forensics; Canterbury Christchurch University College offers an MSc in Cybercrime Forensics, and Cranfield University has a Centre for Forensic Computing (http://www.dcmt.cranfiled.ac.uk/dois/cffc)

82 Available from http://www.cybercrime.gov/s&smanual2002.htm. Accessed on 23/04/14.

83 For instance, in the US, the National Institute of Standards and Technology (NIST) has published 'Guidelines on PDA Forensics' (November 2004). Available at http://csrc.nist.gov. Accessed on 23/04/14.

84 Nigeria Police Regulations, 1968.

be required to undergo a training course of twelve-month duration to include:

(a) six months basic training in law and foot drill;

(b) two weeks attachment for training in practical police work at a police station;

(c) one month leadership and citizenship training course at a recognised centre;

(d) one month first aid lay lecturers course;

(e) three months advanced training in law, foot drill, and the duties of his future substantive rank;

(f) a final period of attachment to a police formation for further training in practical police work, of a duration to be determined by the Inspector-General.

The above curriculum, no doubt, portrays a manifest inadvertence to the need for training in cybernetics. It is observed that this is a debilitating gap in police education especially now that every aspect of human life has been digitised and computerised. This lacuna is not an isolated case as same is observed in the training syllabus of the Special Constabulary[85], which is limited to physical training, foot drill, criminal law, criminal procedure, evidence, practical police work, musketry and revolver training, police discipline, and first aid.[86] Hence, this paper strongly recommends that the curriculum for police training be adequately rationalised and put into law to enable the members of the force to be duly empowered to fight electronic crimes.

There is therefore urgent need for Internet policing in Nigeria. Besides fighting cybercrime, other major duties of the Internet police would include censorship, propaganda, monitoring and manipulating

85 This arm of the police normally charged with the duty of combating serious crimes is not even popular in Nigeria in spite of the fact that it is provided for in the Police Act.

86 Article 14 (1) of Special Constabulary Regulation 1966.

the online public opinion. The practices in other countries may form lessons for Nigeria. For instance, in Canada, several attempts have been made to introduce tools that would allow law enforcement and security agencies monitor online communications without a warrant, the latest of which was bill C-30.[87] In Estonia, the Computer Emergency Response Team Estonia (CERT Estonia) established in 2006 is an organisation responsible for the management of security incidents in computer networks. Its task is to assist Estonian Internet users in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats. CERT Estonia deals with security incidents that occur in Estonian networks, are started there, or have been notified of by citizens or institutions either in Estonia or abroad.[88]

Similarly, in India, Cyber Crime Investigation Cell[89] is a wing of Mumbai Police, India, to deal with cybercrimes, and to enforce provisions of India's Information Technology Law, namely, The Information Technology Act, 2000, and various cybercrime-related provisions of criminal laws, including the Indian Penal Code. Cyber Crime Investigation Cell is a part of Crime Branch, Criminal Investigation Department of the Mumbai Police. Andhra Pradesh Cyber Crime Investigation Cell[90] is a wing of Hyderabad Police, India, to deal with Cybercrimes. In China, in 2005, departments of provincial and municipal governments in mainland China began creating teams of Internet commentators from propaganda and police departments and offering them classes in Marxism, propaganda techniques, and the Internet. They are reported to guide discussions on public bulletin boards away from politically sensitive topics by posting opinions anonymously or under false names. Chinese Internet police also erase anti-communist comments and post pro-government messages. In the Netherlands, the Dutch Police were reported to have set up an Internet Brigade to fight cybercrime. It will be allowed to

87 Parliament of Canada, "Legislative Summary of Bill C-30". http://www.parl.gc.ca/about/parliament/legislativesummaries/bills-is.asp? Accessed on 8/08/14.

88 "Estonian Informatics Centre - About CERT Estonia". Ria.ee. http://www.ria.ee/28201. Accessed on 24/06/14.

89 "Indian Cyber Crime Investigation Cell Official Website". Cybercellmumbai.com. http://www.cybercellmumbai.com/. Accessed on 8/08/14.

90 "Hyderabad Police Cyber Crime Investigation Cell Official Website". Hyderabadpolice.gov.in. http://www.hyderabadpolice.gov.in/. on 8/08/14.

infiltrate Internet newsgroups and discussion forums for intelligence gathering, to make pseudo-purchase and to provide services.[91]

The above countries are not isolated cases. In the United Kingdom, the Internet Watch Foundation (IWF) is the only recognised organisation therein operating an Internet 'Hotline' for the public and IT professionals to report their exposure to potentially illegal content online. It works in partnership with the Police, Government, the public, Internet service providers and the wider online industry. Again, in Malta, the Cyber Crime Unit is a specialised section within the Malta Police Force set-up in 2003.[92] Its primary role is to provide technical assistance in the detection and investigations of crimes wherein the computer is the target or the means used. The Cyber Crime Unit is made up of police officers who are trained in the investigation of crimes that take place over the Internet or through the use of a computer.[93] The Cyber Crime Unit's involvement is not limited to criminal acts commonly associated with technology itself - such as hacking - but extends to investigations of more traditional offences such as fraud, threats and other serious crimes. Indeed, the Cyber Crime Unit's assistance is sought regularly in order to preserve information found upon Internet websites, during searches carried out by police officers from a number of different sections of the Police Force, in the analysis of digital evidence seized in connection with investigations as well as in identifying persons who are committing crimes over the Internet.[94]

5. Conclusion

The principal duty of the Police is to fight crime and prevent it. Therefore, the Police must be equipped to perform the function successfully. Part of this is that they should be well trained and equipped. Police equipment is not restricted to firearms but should include modern gadgets such as computers, and communication gadgets that will enhance its performance. The emergence of cyber criminality constitutes a veritable challenge to the Police. It means that handling cybercrime should not be reserved to specialised national teams of cyber experts. Instead, cyber-cases have to be

91 Internet Brigade gets fit for fighting Cyber Crime, by Jelle van Buure, August 26, 2001, Heise Online. http://www.heise.de/tp/r4/artikel/9-9399/. 24/06/14.

92 http://www.police.gov.mt/en-us/cybercrimeunit.aspx<http://www.police.gov.mt/en-us/cybercrimeunit.aspx>Accessed on 8/08/14.

93 Ibid.

94 Ibid.

treated by basic police units. Knowledge and skills about cybercrime should thus exist throughout the police force. Every police officer should at least have some basic knowledge about cybercrime and how to settle everyday cyber cases.

Police officers not only come into contact with isolated cybercrime cases, but with a variety of connections between offline and online crimes. Increasingly, police officers have to deal with a cyber-aspect in traditional cases, for example, someone who is being stalked and whose e-mail account is hacked. New generations, who grow up in an era where computers and the Internet are indispensable, will increasingly have to deal with cybercrimes and traditional crimes such as threats and slander with a cyber-element. Consequently, the police in the full breadth of the organisation have to be able to deal with cybercrimes. There is no gainsaying that in Nigeria today, there is an urgent need for appropriate legal framework that would address the issues of cyber criminality. This is particularly necessary so as to address the deleterious consequences of cyber criminality in Nigeria. Be that as it may, just making an adequate law, though necessary, would not be sufficient condition for a successful fight against cybercrimes. Legislation must be accompanied by the ability to investigate and prosecute a suspect in deserving cases.