


2-2019

Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria

Follow this and additional works at: <https://vc.bridgew.edu/ijcic>

 Part of the [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Mohammed, Kabiru H.; Mohammed, Yusuf D.; and Solanke, Abiodun A. (2019) "Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria," *International Journal of Cybersecurity Intelligence & Cybercrime*: 2(1), 56-63.

Available at: <https://vc.bridgew.edu/ijcic/vol2/iss1/5>

Copyright © 2019 Kabiru H. Mohammed, Yusuf D. Mohammed, and Abiodun A. Solanke

K. Mohammed., Y. Mohammed., & A. Solanke. (2019). *International Journal of Cybersecurity Intelligence and Cybercrime*, 2 (1), 56-63.

Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria

Kabiru H. Mohammed*, Usmanu Danfodiyo University, Nigeria

Yusuf D. Mohammed, Usmanu Danfodiyo University, Nigeria

Abiodun A. Solanke, Usmanu Danfodiyo University, Nigeria

Key Words; legislation, investigation, prosecution, cybercrime, digital Forensics, digital divide

Abstract:

The advancement of Information and Communication Technologies (ICT) opens new avenues and ways for cyber-criminals to commit crime. The primary goal of this paper is to raise awareness regarding gaps that exist with regards to Nigeria's capabilities to adequately legislate, investigate and prosecute cases of cybercrimes. The major source of cybercrime legislation in Nigeria is an act of the National Assembly which is majorly a symbolic legislation rather than a full and active legislation. In perusing these avenues of inquiry, the authors seek to identify systemic impediments which hinder law enforcement agencies, prosecutors, and investigators from properly carrying out their duties as expected.

Introduction

The recent development in Information Communication Technology (ICT) has made changes in every aspect of our life. These changes are clearly reflected in cyberspace-related areas. The positive influence of cyberspace on knowledge, trade and businesses, and communication is undoubtable. However, there is a dark side of cyberspace, which deteriorates its peaceful usage, that is cybercrime (Harbawi & Varol, 2016). Cybercrime describes a range of circumstances in which technology is involved in the commission of crime. It presents numerous and constantly evolving challenges to government and law enforcement (Jonathan, 2011). At this juncture, it is necessary to briefly distinguish between a computer crime and a cybercrime, the rationale being that more oftentimes than not, the two concepts are regarded as one and the same, when in fact they are only similar, but are definitely different. Computer crimes are those criminal acts perpetrated with the use of a computer; stated in other words, computer crimes include crimes committed against the computer hardware, the materials contained

*Corresponding author

Kabiru H. Mohammed, Management Information System, Usmanu Danfodiyo University, Sokoto, Nigeria.

Email: kabiru.mohammed@udusok.edu.ng

Reproduction, posting, transmission or other distribution or use of the article or any material therein, in any medium as permitted by written agreement of the International Journal of Cybersecurity Intelligence and Cybercrime, requires credit to the Journal as follows: "This Article originally appeared in International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), 2019 Vol. 2, Iss. 1, pp. 56-63" and notify the Journal of such publication.

© 2019 IJCIC 2578-3289/2019/02

or associated with the computer which includes the software and data. Typical examples of computer crimes include but are not limited to embezzlement, fraud, financial scams and hacking (Ajayi, 2016).

Cybercrime is an umbrella term used to describe two distinct but closely related criminal activities: cyber-dependent and cyber-enabled crimes. The former are offences that can only be committed by using a computer, computer networks, or another form of ICT. These acts include the spreading of viruses and other malicious software, and distributed denial of service (DDoS) attacks. Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud and the latter, cyber-enabled crimes, are traditional crimes that are increased in their scale or reach by the use of computers, computer networks or another form of ICT. This includes but is not limited to fraud (including mass-marketing frauds, phishing e-mails and other scams; online banking and e-commerce frauds); theft (including theft of personal information and identification-related data); and sexual offending against children (including grooming, and the possession, creation and / or distribution of sexual imagery) (McGuire & Dowling, 2013).

Due to the dichotomies in jurisdictions and issues addressing the same concept in legal literature, cybercrimes, to date, have no globally accepted definition that could possibly encapsulate all the facets of this novel brand of crime. Therefore, the definitional problem of cybercrime subsists, but one thing that is certain is that most definitions of cybercrime make reference to the Internet. For the sake of overcoming the lacuna, cybercrime has been defined as crime committed over the Internet which might include hacking, defamation, copyright infringement and fraud (Ajayi, 2016).

According to Palmer (2001), digital forensics is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal; or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

It is necessary to point out that a lacuna exists in the capabilities of a typical West African nation, like Nigeria, to adequately handle and manage legislation, investigation and prosecution of cybercrime related cases and also to properly provide ethics of conduct on digital investigations and hence the need to bridge the gap among security professionals, law enforcement, and prosecutors.

Background

Nigeria is a West African nation that is made up of multiple and diverse ethnic groups, which by default, creates its own challenging social problems. After several pressing calls from business and civil society, Legislators enacted the Cybercrime Act 2015 that created, among other provisions, laws related to the use and misuse of computer or electronic devices. But to date, yet to be identified is any breakthrough case that the Act has helped to conclude. This might not be unconnected to the lack of expertise required for law enforcement agencies and other stakeholders to convincingly prosecute offenders. So many times, court proceedings have had to rely on previous judgments to adjudicate on computer crime offences. This was the practice before the amendment of the Nigerian Evidence Act of 2011 which now provides the admissibility of digital evidence. Of the greatest impediments against global efforts towards stemming the menace of cybercrime remains the anonymous nature of the identity of cybercriminals.

It is instructive to note that even where there are legislations on cybercrimes, the provisions of the said extant laws are not severe enough to deter cybercriminals from their illegal acts (Ajayi, 2016). One can envisage the huge gap between the vast involvement in the digital world and the legislation

process. Upgrading the judicial system is not as fast as easy as its technological opponent, and this is in fact causing a struggle in following-up with up-to-date cybercriminal activities and techniques. Also, a considerable number of law enforcement personnel do not really have the interest in technology; some of whom do not even care to surf the Web. Unfortunately, cybercriminals have advanced levels equal to, if not surpassing the skills of law-abiding technology professionals. These criminals may use a variety of methods and tools to reach their goals and perhaps leave little of null tracking behind (Harbawi & Varol, 2016).

It has been an established fact that cybercrime cases in Nigeria are mainly prosecuted by the Economic and Financial Crimes Commission (herein referred to as ‘the EFCC’) using documentary evidence collected during ‘search and seizure’ raids carried out by law enforcement agents. With the way cybercrime evidence is collected in Nigeria, all options must therefore be duly explored during digital evidence acquisition from collection, through processing, to preservation to ensure that when tendered in court, the suspect(s) related to the crime is/are undeniably and positively linked to the evidence for admissibility purposes during legal proceedings (Ajetunmobi, Uwadia, & Oladeji, 2015).

Review of related Literature

Research has been conducted on the gap that exists on the issue of cybercrime with regards to legislation, investigation and prosecution of cybercriminals. The menace of cybercrimes has been discussed by many scholars and writers in different fora with various perspectives with the view to curtailing the challenges that affect not only Nigeria but indeed the world. The current picture of cybercrime legislation is dynamic, indicating ongoing legal reform and increasing recognition that cybercrime requires a legal response across multiple areas: being it criminal, civil, and administrative. The technological developments associated with cybercrime mean that while traditional laws can be applied to some extent, legislation must also grapple with new concepts and objects, such as intangible ‘computer data,’ not traditionally addressed by law (UNoDC, 2013).

With escalations in reports of serious cybercrime, one would expect to see a corresponding increase in conviction rates. However, this has not been the case with many investigations and prosecutions failing to get off the ground. The chief causes of this outcome may be attributed to trans-jurisdictional barriers, subterfuge, and the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology-aided crime (Brown, 2015).

Cybercrime has been on the agenda of the Nigerian Government for many years. Investigations – in particular of fraud-related cybercrime have been carried out in particular by the Economic and Financial Crime Commission (EFCC). Though, the Government adopted the National Cybersecurity Policy and Strategy otherwise known as “The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015” (“Status regarding Budapest Convention”, 2018). With the Cybercrime Act in place, Omotubora (2016) argued that, the omission or failure to criminalize bare unauthorized access or ‘Basic Hacking’ into computer systems is inimical to the overall effectiveness of the provisions of the law dealing with authorized access. Omotubora (2016) also contends that it is unnecessary and counter-productive for the law to include a finite list of further offences that a hacker may intend to commit.

Gaps between the laws used for prosecution of cybercriminals and enforcement procedures in the Cybercrime Act, 2015 are often exploited by defense counsels when evidences tendered are found to be tainted and inconclusive to be admissible for successful prosecution of cases (Ajetunmobi, Uwadia, & Oladeji, 2015). When cybercriminals are apprehended, they have unfettered access to renowned private attorneys who charge very high legal fees. This is not a problem to the cybercriminals as they

can readily afford to pay high professional fees to the best lawyers who specialize in cybercrime practice (Ajayi, 2016).

One could concede that the Nigerian Legislation on Cybercrime Act is more symbolic in the sense that it was served as a reassurance to the citizens that lawmakers are “getting tough” on the menace of cybercrime issues quickly and easily, while that is not the case. Similarly, presentation of digital evidence in legal proceedings is another important issue. Because lawyers and judges may have limited technical knowledge, the presentation of digital evidence must be done in a clear, easily understandable manner (Liles, Rogers, & Hoebich, 2009). Broucek and Turner (2002) note that most legal professionals have a limited understanding of technology and tend to lack confidence in the ability of technical specialists to produce evidence that is admissible in a court of law. To fairly and justly evaluate the merit of digital evidence, judges should have some understanding of the underlying technologies and applications from which digital evidence is derived, such as computers, the Internet, and email services (Kessler, 2011).

Another serious challenge that is worth mentioning is the issues raised by Brungs and Jamieson (2005) concerning best practices, testing of digital forensic tools, and expert witnesses. Numerous digital forensic techniques are used by investigators and examiners; however, no best practice guides are currently available. Also, there currently are no published error rates or testing results for digital forensic tools (Liles, Rogers, & Hoebich, 2009). Standards used to check the validity of scientific evidence may vary as per the field of forensic examination (Humera, Aman, & Oludare, 2018). The Daubert criteria are currently recognized as the benchmarks for scientific evidence which are (i) testing (ii) error rates (iii) peer review and (iv) acceptability used in legal proceedings for evaluating the admissibility of scientific facts and testimony including digital evidence (Humera, Aman, & Oludare, 2018).

The qualifications and skills of expert witnesses is also a serious issue. Meyers and Rogers (2004) question whether one can be considered an expert based on the ability to use a tool or software package, but without the ability to clearly define how the tool works or without reviewing the source code. In many cases, forensic experts may apply a particular tool not because it is the most effective tool but because it is available, cheap, and the expert is familiar with it, (Precilla, Dimpe & Okuthe, 2017). This could lead to unreliable results in the long run. Since digital evidence is used to make judgments in courts, if forensic experts produce unreliable results, there will be negative effects on parties in terms of faulty criminal convictions, improper civil judgment, and lost opportunity because a forensic investigator risks loss of integrity if doubt can be introduced into the accuracy of the tools used (Precilla, Dimpe & Okuthe, 2017).

A court could become more familiarized with digital evidence vulnerabilities, and start scrutinizing the trustworthiness of evidence from computer systems and investigative methods (Cole et al., 2015). Laws and legislation regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cyber criminals in different countries. The long and permeable borders of African countries compound the problem of detection (Cassim, 2011). The current legislation on cybercrime in Nigeria needs to be reviewed to meet the standards in developed countries (Busari, 2017). Nigeria was a country sorely challenged by weak forensic capacity, but now has a state-owned high-powered DNA Forensic Laboratory Centre which was described as the first in the whole of West Africa, known as the Lagos State DNA Forensic Centre (LSDFC) in addition to the EFCC’s own Digital Forensic Lab equipped by the UK government.

Legislation on Cybercrime in Nigeria

Over the years, the Nigerian government has enacted far-reaching laws aimed at curbing the menace of cybercrime and punishing the perpetrators of these crimes. The current legislation in this area is the Cybercrime Act, 2015, which is an enactment of the National Assembly. The Act is considered to be a symbolic legislation that serves as a reassurance function to the public that lawmakers are “getting tough” on a particular problem very quickly and easily, when that may not be the case (Marion, 2010). Questions arise as to if the Cybercrime Act, 2015 will be effective enough in solving the problem, take for instance the Act clearly stated that all cybercafés should be duly registered “...as a business concern with Computer Professionals’ Registration Council in addition to a business name registration with the Corporate Affairs Commission. Cybercafés shall maintain a register of users through a sign-in register. This register shall be available to law enforcement personnel whenever needed.”(Nigerian Cybercrime Act, 2015). But to date, one can authoritatively say that most cybercafés in the country are operating without a license.

Recommendations

As digital evidence grows in both volume and importance in criminal and civil courts, judges need to fairly and justly evaluate the merits of the offered evidence. To do so, judges need a general understanding of the underlying technologies and applications from which digital evidence is derived. Due to the relative newness of the computer forensics field, there have been few studies on the use of digital forensic evidence and none about judges’ relationships with digital evidence. Similarly, gaps identified among security professionals, Law enforcement, and prosecutors need to be bridged. Below are some recommendations for the Nigerian government to improve the current situation regarding stakeholders’ handling of cybercrime issues.

1. Cooperation, awareness, and enlightenment campaigns:

The existence of a suitable legal framework is not enough to fight criminality, such as cybercrime. An effective implementation based on the practice of the legal framework is also crucial. This can be achieved by:

- a. The creation or improvement of mechanisms against cybercrime and the activation of all stakeholders affected by cybercrimes in combating this phenomenon.
- b. Increasing government and public awareness of the risks that the country faces, and by increasing regional and global cooperation in combating cybercrime.
- c. The government should also increase cooperation with Internet Service Providers (ISPs), as well as increase awareness by raising campaigns about the dangers of the Internet and online security (Dushi, 2014).

2. Computer technology curriculum:

Most law enforcement actors are not equipped with the necessary technological knowledge, whereas Internet criminals are experts in computer technology. To combat these crimes, it is necessary to educate and develop human resources as one of the most reliable strategies. In addition, universities, schools of higher education, and academic institutions should open special courses designed to allow future generations of judges, prosecutors, and lawyers to be trained in this difficult, but very relevant and important area (Dushi, 2017).

3. Strengthening the existing institutions:

There should be an identification of key institutions in the field of cyber security. Those institutions

must have sufficient staffing, with a variety of specialists, both from the legal and information technology (IT) fields, who must be constantly trained (Dushi, 2017).

4. Capacity building programs for stakeholders:

There must be an improvement in the operational capacity and response of law enforcement authorities against cyber-attacks. In this context, it is necessary to increase the number of experts in the field of investigating and prosecuting cybercrime. This is possible by frequently organizing specialized trainings and sending relevant officials abroad for specialization training. The specialization of experts in the field of cybercrime as well as increasing their knowledge of domestic and international legislation in the field, and on the methods and ways of implementing this legislation in the most adequate and effective ways can be achieved through these trainings (Dushi, 2017).

5. Forensic expert qualification:

The reviewer of a forensic expert report should scrutinize the qualifications of a forensic examiner to avoid the unfortunate scenario wherein an unqualified forensic examiner produces a flawed or unreliable report. While no uniform set of standards exists to gauge the competency of a digital forensic examiner, reviewers should consider the most appropriate combination of certification, education, and real-world experience, given the case at hand (Garrie & Morrissy, 2014).

6. Engagement of decision-makers:

It is essential that decision-makers in government and organizations understand risks and options, agree on strategic priorities, provide political backing and allocate resources to measures on cybercrime.

7. Establishing reporting channels for individuals and public and private sector organizations:

Reports may trigger law enforcement investigations, provide intelligence for a better understanding of the scope, threat, and trends of cybercrime, and allow for collating data to detect patterns of organized criminality (Alexander, 2013).

Conclusion

There is broad consensus between practitioners and researchers that cybercrime investigations are hindered by insufficient knowledge and a skill gap of law enforcement officers as well as the relevant actors in the judiciary. This paper discussed ways on how to bridge the gap that exists among legislators, investigators, and prosecutors in Nigeria, and suggested recommendations to address the menace of cybercrime threats.

As digital evidence grows in both volume and importance in criminal and civil courts, judges need to fairly and justly evaluate the merits of the offered evidence. To do so, judges need a general understanding of the underlying technologies and applications from which digital evidence is derived. In order to meet the needs of stakeholders in a concerted, complementary and sustainable manner, awareness must be created among the key stakeholders (i.e., legislators and law enforcement officers).

References

- Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(1), 1-12.
- Ajetunmobi, R., Uwadia, C., & Oladeji, F. (2015). *Computer forensics guidelines: A requirement for fighting cyber crime in Nigeria now?* Accessed on September 22, 2018 retrieved from <http://196.45.48.50/opendoc.php?sno=30415&doctype=pdf&docname=Computer%20Forensic%20Guideli>

nes:\%20A\%20Requirement\%20for\%20fighting\%20Cyber\%20Crime\%20in\%20Nigeria\%20now?

- Alexander, S. (2013). Capacity building on cybercrime – discussion paper, Data Protection and Cybercrime Division, Council of Europe, Strasbourg www.coe.int/cybercrime.
- Brown, C.S.D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9(1), doi: 10.5281/zenodo.22387
- Busari, K. (2017, October 31). “Nigeria’s Cybercrime Act needs review – Senate Committee” Premium Times accessed on 24th September, 2018 retrieved from: <https://www.premiumtimesng.com/news/more-news/247851-nigerias-cybercrime-act-needs-review-senate-committee.html>
- Broucek V., & Turner P. (2002). Bridging the divide: Rising awareness of forensic issues amongst systems administrators, presented at the Third International System Administration and Networking Conference.
- Brungs, A., & Jamieson, R. (2005). Identification of legal issues for computer forensics. *Information Systems Management*, 22(2), pp. 57–66
- Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. *CILSA* 44(1):123-138
- Cole, K.A. (2015). Gupta, Shruti; Gurugubelli, Dheeraj; and Rogers, Marcus K., “A Review of Recent Case Law Related to Digital Forensics: The Current Issues.” *Annual ADFSL Conference on Digital Forensics, Security and Law*. <https://commons.erau.edu/adfsl/2015/wednesday/2>
- Dushi, D., (2017). Law enforcement and investigation of cybercrime in Albania. *European Scientific Journal* accessed on 24th August, 2018 retrieved from: <https://ejournal.org/index.php/esj/article/download/9228/8769>
- Explanatory Memorandum on Cybercrimes (Prohibition, Prevention, Etc) Act, 2015, retrieved from https://www.cert.gov.ng/file/docs/CyberCrime_Prohibition_Prevention_etc_Act_2015.pdf
- Garrie, D.B., & Morrissy J.D. (2014). Digital forensic evidence in the courtroom: Understanding content and quality. *Northwestern Journal of Technology and Intellectual Property*, 12(2) retrieved from: <http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss2/5>
- Harbawi, M., & Varol, A. (2016). The role of digital forensics in combating cybercrimes: 4th International Symposium on Digital Forensics and Security (ISDF2016), 25-27, Little Rock, AR doi: 10.1109/ISDFS.2016.7473532.
- Humera A., Aman B. J., & Oludare, I. A. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems*, 14(2): 346–376 doi: 10.3745/JIPS.03.0095
- Jonathan, C. (2011). Cybercrime, *Commonwealth Law Bulletin*, 37:4, 671-680, doi:10.1080/03050718.2011.621277
- Kessler, G. C. (2011). Judges’ awareness, understanding, and application of digital evidence. *Journal of Digital Forensics, Security and Law*, 6(1). Retrieved from <http://commons.erau.edu/db-security-studies/25>

- Liles, S., Rogers, M., & Hoebich M. (2009). A Survey of the legal issues facing digital forensic experts. In: Peterson G., Shenoi S. (eds) *Advances in Digital Forensics V. Digital Forensics 2009*. IFIP Advances in Information and Communication Technology, Vol 306. Springer, Berlin, Heidelberg
- Marion N.E., (2010). The Council of Europe's Cyber Crime Treaty: An exercise in symbolic legislation. *International Journal of Cyber Criminology*. Vol. 4 Issue 1/2, p699-712. 14p.
- Meyers, M., & Rogers, M. (2004). Computer forensics: The need for standardization and certification. *International Journal of Digital Evidence*, 3(2).
- McGuire, M., & Dowling., S. (2013). Cyber-crime: A review of the evidence summary of key findings and implications. Home Office Research Report 75, Home Office, United Kingdom, October. 30p.
- Nigeria: Status regarding Budapest Convention (2018): accessed on 22nd September, 2018 available at https://www.coe.int/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/nigeria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print\&_101_INSTANCE_hFPA5fbKjyCJ_languageId=hu_HU
- Omotubora A., (2016). Comparative perspective on cybercrime legislation in Nigeria and the UK – a case for revisiting the “Hacking” offences under the Nigerian Cybercrime Act 2015. *European Journal of Law and Technology*, Vol 7, No 3
- Palmer, G. (2001). A road map for digital forensic research. *Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS)*, New York.
- Precilla, M. D., & Okuthe, P. K. (2017). ‘Impact of Using Unreliable Digital Forensic Tools.’ *Proceedings of the World Congress on Engineering and Computer Science 2017 Vol I WCECS 2017*, San Francisco, USA
- United Nations Office of Drugs and Crime: Comprehensive Study on Cybercrime (2013). Accessed on 10th September, 2018. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf