CYBERCRIME AND DIGITAL EVIDENCE: THE NIGERIA POLICE FORCE IN PERSPECTIVE

*Olusoji Abraham Obideyi**

I. INTRODUCTION

Cybercrime refers to various forms of attacks against computers, digital devices and network systems which connect the cyberspace, whereas cyberspace is the interactive domain of digital networks that is essential for the effective running and operations of critical infrastructure sectors such as health, transportation, finance, energy, agriculture and food processing, including security. Cybercrime is notably a big challenge in Nigeria and all over the world, notwithstanding the criminal justice systems in existence. For any successful apprehension and prosecution of cybercrime in the society, a professional approach to finding, preserving, collecting, analysing and utilizing digital evidence is crucial.

Cybercrime is an act that violates the law, and it is perpetrated using Information and Communications Technology (ICT) to facilitate a crime or target networks, systems, data, websites and/or technology. Europol differentiates cybercrime into *cyber-dependent* and *cyber-enabled* crimes. The key distinction between these categories of cybercrimes is the role of ICT in the offence. When an ICT device is the target of the offence, the cybercrime negatively affects the confidentiality, integrity and/or availability of computer data or systems.[1]

The International Criminal Police Organization (INTERPOL) in Nigeria, among other security outfits within Nigeria, regularly churns out data on the trends of cybercrimes within Nigeria. These crime measurement tools and victimization surveys vary based on the types of cybercrime data collected and analysed, and the methods used in collecting and analysing the data.

Cybersecurity businesses and other private organizations that focus on security, business risk and/or threat analysis around the world publish cybercrime and/or cybersecurity trends reports based on historical cybersecurity incidents, and their types, frequency and impact. With the advent of new technologies – the Internet of things, drones, robots, self-driving cars and lots more – new cybercrime trends will definitely be unmasked.

A. Categories of Cybercrimes in Nigeria

There are diverse classifications and categorizations of cybercrime globally, for example, Maitanmi et al. (2013) classified cybercrimes into three main categories namely: Target Cybercrime (computer as target), Tool Cybercrime (computer as tool of cybercrime) and Computer Incidental (computer playing minor role in the crime).[2] However, the most common categorization of cybercrimes, and of course which was adopted by this paper, is as follows:

i. Cybercrime against people (individuals): These are activities targeted against individuals, their persons and property, and they include harassment via e-mails, cyberstalking, distribution of obscene materials, defamation, unauthorized control or access over a computer system, indecent exposure, e-mail spoofing, cheating and fraud, computer vandalism, transmitting viruses, net-trespass, intellectual property crimes, and internet time thefts.

ii. Cybercrime against Property: These are activities targeted against computer/digital infrastructures

* Staff Officer-TO-IGP (ICT/TS), IGP Secretariat, The Nigeria Police Force, Nigeria.

[1] https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html

[2] https://www.researchgate.net/publication/327111080_Impact_of_Cyber_Crimes_on_Nigerian_Economy

such as routers, communication masts and base stations (or BTS), database systems and corporate digital facilities. These crimes include DDOS attacks, hacking, virus transmission, cyber and typo squatting, computer vandalism, copyright infringement and IPR violations.

B. Cybercrime against Government[3]

Nigeria 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*, which 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 in the Courts of Law. 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 for the admissibility of digital evidence. Out of all the hurdles against global works on stemming the threat of cybercrime remains the mysterious character of the identity of cybercriminals as noted by Ajayi (2016).[4]

It is instructive to note that even where there is legislation on cybercrime, the provisions of the said extant laws are not severe enough to deter cybercriminals from their illegal acts.[5] Also, a considerable number of law enforcement personnel do not really have an 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.

It is an established fact that cybercrime cases in Nigeria are mainly prosecuted by the Nigeria Police Cybercrime Units and the Economic and Financial Crimes Commission (EFCC) using documentary evidence collected during search and seizure raids carried out by the law enforcement agents. With the way cybercrime evidence is bring 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.

II. EFFECTS OF CYBERCRIMES AND GLOBALIZATION TO NIGERIA

Cybercrimes have inflicted severe consequences and loss to national economies in many respects. Governments world over, therefore, have engaged this monster in a serious fight in a bid to eradicate it. Serious and coordinated efforts have been made by governments, individuals and organizations on many continents of the world, including America, Asia, Europe and Africa, but the fight in Nigeria seems uncoordinated because the root causes of cybercrimes have not been unearthed or tackled. Consequently, the crimes seem to still be booming notwithstanding the pockets of efforts made by the government.

A. Effects of Cybercrimes on the Nigerian Economy

i. *Capital flight and loss of foreign investments:* capital which was supposed to have come to Nigeria is diverted to other African countries as a result of lack of confidence on Nigeria as a result of prevalent cybercrimes in the country.

ii. *Bad national image and reputation:* This creates lack of confidence in Nigeria and on Nigerians. Foreigners avoid dealing with Nigerians like lepers and this leads to lack of direct foreign investments. Also, many legitimate Nigerian online entrepreneurs are denied the opportunity to do business with nationals of other countries.

[3] Governments, firms, companies, and corporate bodies. These include hacking, accessing confidential information, cyber warfare, cyber terrorism against governments and corporations, operation/use of pirated software, espionage and so on.
[4] https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210
[5] Ibid.

iii. *Rejection of certain countries by e-commerce communities or platforms:* This is one of the most visible and biggest challenges to genuine legitimate business personalities in Nigeria. Several e-commerce platforms or e-payment providers such as PayPal, eBay, MoneyGram, prohibit Nigeria, and some countries notorious to be safe havens for cybercriminals, from the use of their payment gateways.

iv. *Loss of revenue by banks, private individuals, government organizations to the activities of cybercriminals, especially in Nigeria:* This destroys confidence in the system and creates unnecessary fear in people having anything to do with online transactions.

B. Challenges in Cybercrime Investigation

With escalations in reports of serious cybercrimes, 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.[6]

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 Nigeria Police Cybercrime Unit, Economic and Financial Crime Commission (EFCC). The Federal Government of Nigeria adopted the National Cybersecurity Policy and Strategy otherwise known as "*The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015*".

Gaps between the laws used for prosecution of cybercriminals and enforcement procedures in the Cybercrime Act, 2015 are often exploited by defence counsels when evidence tendered are found to be tainted and inconclusive to be admissible for successful prosecution of cases. When cybercriminals are apprehended, they have unfettered access to renowned private attorneys who charge very high legal fees. This is not a problem for the cybercriminals as they can readily afford to pay high professional fees to the best lawyers who specialize in cybercrime practice.

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. It is noted 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. Judges should have some understanding of the underlying technologies and applications from which digital evidence are derived in order to justly evaluate the merit of such evidence.[7]

Other serious challenges that are worth mentioning are the issues 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.

Laws and legislation regulating cyberspace tend to result in few prosecutions due to the jurisdictional difficulties and additional resources required in tracking down cybercriminals in different countries. The current legislation on cybercrime in Nigeria needs to be reviewed to meet the standards in developed countries. Nigeria was a country sorely challenged by weak forensic capacity, but it 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 Digital Forensic Lab equipped by the UK government.

[6] 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

[7] 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

III. RECOMMENDATIONS

Having examined the various aforementioned concepts on this subject matter, below are some suggestions to ameliorate the already exacerbated situation on cybercrimes in Nigeria:

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, among other things, cooperation among investigative agencies and digital forensic laboratories (e.g. sharing information about procedures for preservation and collection of digital evidence, cooperation to obtain the results of analysis promptly, etc.).

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 very vital area.

3. *Capacity-building programmes for stakeholders*: There must be an improvement in the operational capacity and response of law enforcement authorities against cyberattacks. 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.

4. *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.

5. *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.

IV. CONCLUSION

There is broad consensus 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 highlighted cybercrime trends in Nigeria, enumerates the effects of cybercrime and globalization on the economy of the nation, the challenges encountered by actors in criminal justice response to cybercrimes and other related offences. It concluded by discussing ways on how to bridge the gap that exists among legislators, investigators, and prosecutors in Nigeria, and furnished recommendations to address the peril of cybercrime threats.

Certainly, 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).