CHAPTER 14

Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable are Law Enforcement Agencies?

Dr. Muktar Bello & Dr. Marie Griffiths

University of Salford MANCHESTER
Salford Business School

MARCH 2020

ABSTRACT

The evolution of the Internet amidst a rapidly growing global economy has created a completely new environment in which traditional crime prospers. Equally the convergence of computing and communication has changed the way we live, communicate and commit crime. Cybercriminals in Nigeria commonly known as "419 scammers"; a word coined from the Nigerian criminal code that penalises people from obtaining money under false pretense cost the Nigerian consumer $13.5 billion dollars in losses in 2012. (Clarke, 2004, Sesan et al., 2012; Grabosky, 2001;)

Previous studies have focused on the causes and effects of cybercrime in Nigeria (Hassan et al., 2012; Adesina, 2017); laws penalising against misuse of computer (Olusola et. al., 2013b; Saulawa & Abubakar, 2014) and have focused relatively on financial cost and socio-economic effects of cybercrime (WITFOR, 2005; Sesan et. al., 2012). Even though some studies have tried to explore cybercrime from the perspective of law enforcement Agencies in the UAE and Jordan (Maghairah, 2009; Alkaabi, 2010), none has been done holistically from the view of law enforcement and members of the Cybercrime Advisory Council in Nigeria.

Adopting a classical criminological framework of Routine Activity Theory (RAT), this research examined particularly cyber-enabled crime of advance fee fraud in Nigeria within the scope RAT which argued that for crime to take place, three requirements must be present namely; a motivated offender, a suitable target and an absence of a capable guardian. The research examined the factors that motivate an offender and what elements make a target (i.e. victim or computer) suitable for a crime. In the process, it considers the suitability of law enforcement officers and some members of the Cybercrime Advisory Council (CAC) as capable guardians and what factors limits their capabilities in mitigating the activities of cyber criminals.

The research has been framed on an interpretivist paradigm and relativist philosophical stand, with focus on an inductive qualitative approach involving semi-structured interviews and documentation. These involved policy makers, members of parliament, telecommunications and ICT regulators on one hand; and investigators, prosecutors, forensic analyst and media practitioners particularly from the Economic and Financial Crimes Commission (EFCC), which is a leading law enforcement agency in the fight against cybercrime. The multi-dimensional evidence explains the role played by each of the stakeholders, the measures and partnership deployed in tackling cybercrime, and the challenges and recommendations needed in the international effort to tackle cybercrime globally.

Findings suggest that the proliferation and lack of effective policing of the internet enabled by the greed of individuals and lack of enforcement and collaboration of relevant stakeholders have led to financial losses to victims. The findings further show how lack of proper education and awareness of individuals, and adequate training and provision of tools for law enforcement officers contributes to the high prevalence of cybercrime in Nigeria.

Evidence is provided that documents the way members of the Cybercrime Advisory Council and especially the EFCC have attempted to overcome these challenges through partnership, capacity building and enforcement of relevant laws and policies aimed at addressing the issue of cybercrime in Nigeria. The finding equally extends the criminological understanding of deviant behaviors and furthers the current discussion on the role of law enforcement in policing the Internet.

Keywords: Cybercrime, Policing, Routine Activity Theory

1.0 INTRODUCTION

According to the UNODC (2013), as the usage of the internet increases globally, especially in developing countries, the number of targets and offenders increases daily. Also, it is difficult to estimate how many users of the internet are using it for illegal activities. Cybercrime, according to Wall (2017) cannot be eradicated and there is no way to 'turn these technologies off'. He further argued that more laws to address the issue of cybercrime is not the answers as most existing computer misuse laws in all jurisdictions are not properly enforced. Alternatively, using technology as a counter-measure is not the appropriate response as it is sometimes used to restrict the freedom of others. However, cybercrime could only be managed in a way the risks and harm are reduced to the barest minimum. In order to tackle cybercrime, law enforcement, government and the private sector as the 'capable guardians' would need to collectively respond adequately to the ever-evolving nature of technology based crimes (Wall, 2017).

2.0 PROBLEM STATEMENT

Undeniably, the policing of crime using the traditional Nigerian police has many limitations (Owen, 2014), and the integrity of the Nigerian police force has been eroded by its failure to perform its constitutional responsibilities to the society (Nwachukwu, 2012). Due to that, cybercrime has had a negative impact to the economy and reputation of the country as a haven of criminals. The problem of cybercrime in Nigeria is further compounded by the increased usage of the internet for fraudulent activities (UNODC, 2013) and the lack of cyber user awareness, which makes internet users vulnerable to be exploited by criminals online (Kortjan and Solms, 2014).

Even though, the Nigerian government have developed appropriate legal and institutional frameworks in securing the Nigerian cyberspace (Adomi and Igun, 2008), policing the cyberspace would require governments and legal systems to continuously adapt to new technologies and strategies in tackling cybercrime (Grabosky, 2001). Currently, there is a need for the Nigerian government to work together in strengthening the legal frameworks for cybersecurity, and also enforcing existing laws in order to reduce the impact of cybercrime in the society (Olusola, M., Samson, O., Semiu, A., Yinka, A. 2013b; Hassan, A.B., Lass, F.D., Makinde, J., 2012)

3.0 RESEARCH OBJECTIVE

1. To examine the current measures used by Law Enforcement Agencies in Nigeria in tackling cybercrime through review of relevant literature and interview of members of the Cybercrime Advisory Council in Nigeria.

4.0 RESEARCH QUESTION

1. Are Law Enforcement Agencies (LEA) in Nigeria capable guardians in tackling cybercrime explored in relation to Routine Activity Theory?

5.0 LITERATURE REVIEW

5.1 Cybercrime in Nigeria

The arrival of the internet and computers has opened many opportunities for the young and old in the global community to have access to the world from their homes, offices and cyber cafes. The coming of smart phones has made internet access easier and faster (Saulawa and Abubakar, 2014; Clough, 2010). Unlike in the past when the ability to commit computer related crimes was largely limited to those with the access and skill sets; nowadays, technology is easily accessible, thus, making it available to both offenders and victims (Clough, 2010)..

Sub-Saharan African (SSA) is the last continent to embrace the internet and mobile technologies. Internet penetration in Sub-Saharan Africa has been on the increase with most countries depending on privately owned internet access points such as cybercafés' for their daily internet activities (Longe, Ngwa, Wada and Mbarika, 2009).

Cybercrime has been one of the eluding issues in the online global transactions in Nigeria because of the endemic nature of computer related frauds and crimes. Due to the integration of digital technology across the globe, the economy of most nations across the globe is accessible through the use of information and communication technology (Abubakar and Saulawa, 2014).

Cybercrime has been a key agenda for the Nigerian Government for many decades. Investigations that are fraud related have been carried out by the Economic and Financial Crimes Commission (EFCC). Though the admissibility of electronic evidence was amended in the Evidence Act 2011 through the parliament, the lack of a proper legal framework on cybercrime

has made criminal justice measures ineffective until 2015 when the Government adopted the National Cybersecurity Policy and Strategy through an inter-ministerial committee headed by the Office of the National Security Adviser (Council of Europe, 2017).

5.2 Cybercrime Advisory Council (CAC)

The Cybercrime Act (2015) establishes the Cybercrime Advisory Council which is referred to as the 'Council'. The Council shall consist of a representative each of the ministries and agencies listed under the First Schedule of this Act'.

5.2.1 Functions and Powers of the Council

The functions and powers of the Cybercrime Advisory Council is contained in Section 43 (1) of the Cybercrime Act (2015). The functions are as follows:

a) To create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and promotion of cyber security in Nigeria;
b) To formulate and provide general policy guidelines for the implementation of the provision of this Act;
c) To advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues;
d) To establish a program to award grants to institutions of higher education to establish cyber security research centres to support the development of new cyber security defence, techniques and processes in the real-world environment and;
e) To promote Graduate Traineeships in cyber security and computer and network security research and development (Cybercrimes Act, 2015).

5.3 Limitations to Tackling Cybercrime

Cybercrime has evolved over the years with recent development in ICT resulting in newer cybercrime methods. However, advances in ICT have greatly expanded the capabilities of law enforcement agencies in adopting new methods of investigating cybercrime. Even though criminals may use new tools to prevent LEAs from conducting their work, it is important for police to expand their technical capabilities (ITU, 2012).

5.3.1 Technology and Training

Chukkol (cited in Barnard, 2014) states that Nigeria has seen a transition in how crimes are evolving at a greater speed with criminals embracing ICT to commit crimes. Smith (2003) argues that the investigation of cross-border cybercrime requires the adequate technical and forensic skills and knowledge. Other areas enumerated by Smith (2003) that need improving include:

a. Formulation of training programs and the development of investigative software tools
b. International training programmes should be developed and expertise shared between different nations.
c. The level of funding required for training and up-grading Equipments is inadequate.
d. Need for greater information sharing between investigators both within the public and private sectors.

5.3.2 Laws and Jurisdiction

Adequate and proper legislation is the bedrock for the investigation and prosecution of cybercrime. However, law-makers must continuously respond to ICT and internet development so as to measure the effectiveness of existing laws and provisions (ITU, 2012). With the exception of Europe and America that have sufficient investigative powers to prosecute cybercrime, the rest of the world has insufficient investigative powers (UNODC, 2013).

According to the ITU Report (2012), challenges in drafting national criminal laws to prosecute new forms of cybercrime takes time and some countries are yet to make the necessary adjustments.

Smith (2003) states that the harmonization of laws and the adoption of international conventions on cybercrime will make prosecution easier and will greatly improve the mutual assistance and extradition of criminals between countries.

5.3.3 Education and Awareness

Dix (2017) argued it is important for all digital users to practice basic cybersecurity hygiene to improve their own protection. He states that, about 80 percent of exploitable vulnerabilities online are due to ‘poor or non-existent cyber hygiene. Odumesi (2015) maintains, cyber risk increases without the proper precautions to protect personally identifiable information on the cyberspace. He further stated that, Nigerian online users are highly vulnerable to cyber-attacks because the lack of cybersecurity awareness had made it easy for cybercriminals to operate.

6.0 THEORETICAL FRAMEWORK

6.1 Routine Activity Theory

Within the scope of classical and choice theory, the perception of the available opportunities to commit crime was considered as an essential element (McQuade 2006). Cohen and Felson (1979) argued that for crime to take place, three requirements needed to be present namely, a motivated offender, a suitable target and an absence of a capable guardian. The RAT approach to crime causation is ecological and the accessibility, location and presence or absence of certain characteristics or people is what proves to be predictive of criminal behaviour (Kigerl, 2012; Cohen and Felson, 1979).

Akers and Sellers (2004), stated that a motivated offender must be someone who is willing to commit a crime and for whom the opportunity was present to allow the crime to be committed. A suitable target is the one the motivated offender values such as credit card information and that target also be visible, accessible and able to be illegally obtained by the offender (Clarke and Felson, 1998). Finally, the capable guardian must be absent; a capable guardian such as encryption, anti-virus or law enforcement officer is any person or thing that obstructs the motivated offender from acquiring the target (Cohen and Felson, 1979).

6.2 Absence of a Capable Guardian

Over the years, capable guardianship has evolved from knights of feudalism to the private security services of modern times which vastly outnumber sworn police officers in many developed economies (Grabosky 2001:248). Guardianship refers to 'the capability of persons and objects to prevent crime from occurring' (Tseloni, Farrell, Pease and Wittebrood, 2004). Routine activity theorists argue that the mere presence of a guardian in proximity to the suitable target is a crucial deterrent. Where the capable guardian is a person, he/she acts as someone 'whose mere presence serves as a gentle reminder that someone is looking' (Yar, 2005). The policing of crime in both terrestrial and cyberspace has become a 'pluralistic endeavour' as responsibilities for the control of cybercrime will be similarly shared between law enforcement officers, information security specialists and individual users. The first line of defence as it has always been with the terrestrial space is self-defence (Grabosky, 2001).

A guardian can be anyone or anything that creates a protection on the target victim. The motivated offender is discouraged from committing an offense when they know that the target has a guardian. Therefore, capable guardians as elements of crime can be controlled, modelled or changed to prevent crime (Lopez, 2014). Also, Tseloni et al. (2007:74) referred to guardianship as 'the capability of persons and objects to prevent crime from occurring'. However, Cohen and Felson (2008:3) stated that the capable guardian 'was not to seen to be a policemen or security guard in most cases'. This was a deliberate attempt to distance routine activity theory from the rest of criminology because it is entrenched to the criminal justice system as central to crime explanation. Cohen and Felson (2008) further argued that the most likely persons to prevent a crime is not a police officer but rather friends, neighbours and owners of a targeted property. They state that the absence of a suitable guardian is important, as an offender must find a suitable target in the absence of a guardian before a crime can occur. Although there may be direct intervention, Yar (2005) argued that routine activity theorist view 'the simple presence of a guardian in proximity to the potential target as a crucial deterrent'. In understanding the concept of guardianship in the cyber world, Yar (2005) contended that it depends on the guardians presence together with the suitable target at the time when the 'motivated offender converges upon it'. However, Felson (1998:53) stated that the problem faced by guardianship is more intensified in the cyberspace than in the terrestrial world because in the terrestrial space, the police 'are very unlikely to be on the spot when a crime occurs' while in the cyberspace it is only when informal guardianship has failed that a formal assistance of LEAs are sought. In summary, RAT concept of guardianship as argued by Yar (2005) is applicable to cyberspace even when the 'structural properties of the environment amplifies the limitations upon a establishing' a cyberspace guardianship.

This theory is considered appropriate when applied to cybercrime in Nigeria, because it extends the criminological understanding of deviant behaviours and the applicability of motivated offenders, suitable target and guardianship with the scope of the research.

7.0 METHODOLOGY

The research has been framed on an interpretivist paradigm and relativist philosophical stand, with focus on an inductive qualitative approach involving semi-structured interviews and documentation. These involved policy makers, members of parliament, telecommunications and ICT regulators on one hand; and investigators, prosecutors, forensic analyst and media practitioners particularly from the Economic and Financial Crimes Commission (EFCC), which is a leading law enforcement agency in the fight against cybercrime. The multi-dimensional evidence explains the role played by each of the stakeholders, the measures and partnership deployed in tackling cybercrime, and the challenges and recommendations needed in the international effort to tackle cybercrime globally. Table 1.1 showing demographics of the Research Participants

ORG	NAME OF ORGANISATION	SECTOR	NO	Role
A	**Economic and Financial Crimes Commission**	Law Enforcement	28	Enforcement of EFCC; AFF & Cybercrimes Act. Member of CAC
B	**Office of the National Security Adviser**	Presidency	1	National Coordinator of Cybercrimes Act. Member of CAC
C	**National Assembly – Senate Committee on ICT & Cybercrime**	Parliament	1	Making Laws – Oversight of all MDAs
D	**Nigerian Communications Commission**	Telecommunication	1	Telecoms Regulator. Member of CAC
E	**National Information Technology Development Agency**	Information Comm. Technology	1	ICT Regulator. Member of CAC

Table 1.1: Research Participants

7.1 Research Participants

Organisation A – Economic and Financial Crimes Commission (EFCC)

Organisation A is the leading law enforcement agency in the investigation of economic and financial crimes in Nigeria. The organisation has the powers to investigate advance fee fraud, a variant of cybercrime through the Advance Fee Fraud and Other Related Offences Act 2006 and investigate other forms of cybercrime through the Cybercrimes (Prohibition, Prevention) Act 2015. It is a key member of the Cybercrime Advisory Council in Nigeria.

Organisation B – Office of the National Security Advisor (ONSA)

Organisation B is the Office of the National Security Advisor under the National Security Advisor and acts as the overall coordinator of the Cybercrime Advisory Council. The ONSA is also the designated Nigerian Computer Emergency Response Team (ngCERT). The ONSA also serves as the National Forensic Lab of Nigeria. It initiated and coordinated the development of the National Cybersecurity Policy and Strategy of Nigeria.

Organisation C – National Assembly (Senate)

Organisation C is the National Assembly which houses the Senate and the House of Representatives. The National Assembly is one of the three arms of the Nigerian Government and it is solely responsible for making and amending laws. It also provides oversight functions of all Ministries, Departments and Agencies (MDAs) through its committee functions. The Senate Committee on ICT & Cybercrime are responsible for making input into ICT and Cybercrime Laws and provides oversight duties to MDAs that are mandated to tackle cybercrime in Nigeria.

Organisation D – Nigerian Communications Commission (NCC)

Organisation D regulates all mobile network operators (MNO) and internet service providers (ISPs) in Nigeria. It is responsible for providing guidelines, framework and enforcement of policies in the communications sector. It plays a key role in addressing the issue of cybercrime in Nigeria as it regulates all the ISPs and MNOs that manage all the communication platforms that are frequently used by criminals to commit crime online. It is a member of the Cybercrime Advisory Council (CAC).

Organisation E – National Information Technology Development Agency (NITDA)

Organisation E provides regulation, framework and guidelines for all Ministries, Department and Agencies (MDA) in the implementation of ICT in Nigeria. It is a member of the Cybercrime Advisory Council (CAC).

8.0 FINDINGS

The theme, 'Measure and Benefits of Measures by Law Enforcement and Members of the Cybercrime Advisory Council (CAC)', was analysed within the scope of what measures the organisations were using in tackling the issue of cybercrime. Also, participants were asked how beneficial the measures were in tackling cybercrime. Thirty-two (32) responded by mentioning different measures and approaches they were using to mitigate the activities of cybercriminals. Also, the benefits of the measures were analysed in order to understand how suitable the

measures were in tackling cybercrime. Eight (8) sub-themes emerged from the main themes. The emergent themes are:

1. Awareness Campaigns
2. Best Practices
3. Enforcement
4. Funding & Logistics
5. Partnership
6. Training and Manpower
7. Benefits of Measure

Figure 1.1 shows the theme and the emergent outcomes.

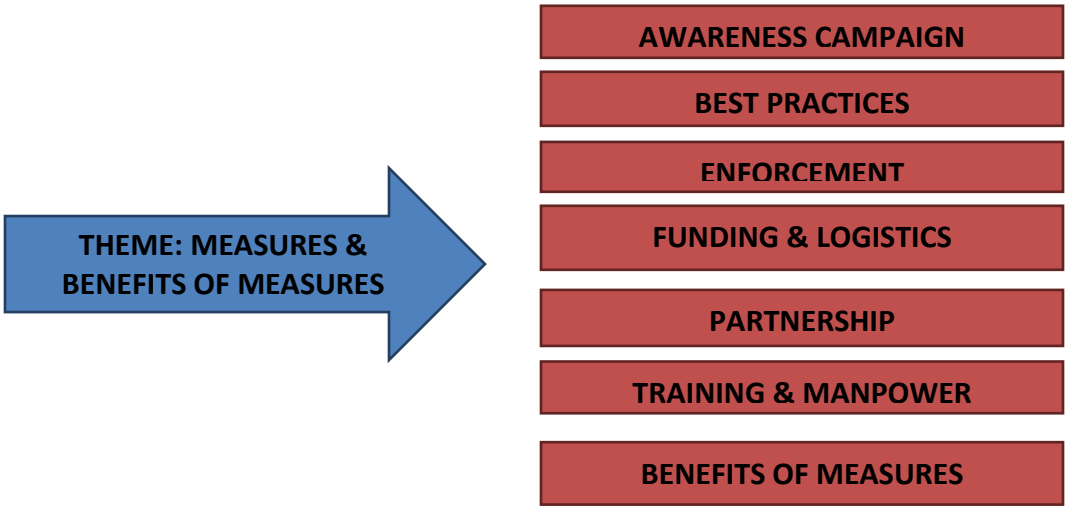

Figure 1.1: Theme: Measures, Benefits of Measures by LEAs, CAC & Sub-Themes

8.1 Awareness Campaign

Fourteen (14) participants stated that raising awareness of the general public about the dangers of cybercrime was one of the measures they were using to tackle the activities of cybercriminals. Participant 27 argued that:

> *The measures that are being taken right now in order to address the issue of cybercrime in Nigeria primarily are on awareness, sensitization campaign, re-orientation. Nigerians need to know more on how those internet fraudsters operate.* (Participant 27, Cybercrime Prosecutor)

8.2 Best Practices

Only one participant from the forensics unit stated that the measures they were using to curtail the activities of cybercrime was by adhering to international best practices in retrieving evidence

from digital devices which was vital for a successful investigation of cybercrime. The participant stated that:

> *We adhere to the international best practice such as ACPO guideline, we ensure that we maintain the integrity of every evidence we are working on. Chain of custody, we ensure that we properly establish a chain of custody and we don't temper with the integrity of any evidence because this evidence has to be presented in the court of law the way it is.* (Participant 11, Forensic Examiner).

8.3 Enforcement

The enforcement of cybercrime laws and other laws that criminalised the illegal use of computers to commit crime was one of the measures used by seven (7) participants in deterring criminals in committing crime. Participant 25, a lawyer with one of the organisations argued that:

> *We are enforcing the provision of the law, enforcing the provision of the Cybercrimes Prevention and Prohibition Act 2015.* (Participant 25, Cybercrime Prosecutor)

The Cybercrime Act 2015 was an important legal instrument that when properly enforced would assist in addressing the activities of cybercriminals. However, another participant argued that by opening up more offices and having a dedicated forensic unit in each of these new offices, it had reduced the backlog of cases.

8.4 Funding and Logistics

The provision of funds and tools to conduct proper cybercrime investigation was a measure used for the successful investigation of cybercriminals. Three (3) interviewees stated that funding and logistical support of tools was a major way they were able to counter the activities of cybercrime. One of the participants stated that:

> *We do some intelligence, social media. We try to source information from social media because some of these fraudsters and trace emails as well. We are using of email and domain tracing tools to help us as well.* (Participant 4, Cybercrime Investigator)

8.5 Partnership

The partnership between organisations in investigating cybercrime was one of the measures used in tackling cybercrime. Seven (7) interviewees agreed that, having partnerships with relevant stakeholders had been beneficial in investigating cybercrime. The participant argued that:

> *The cybercrime unit has been holding a lot of meetings with different agencies like Microsoft. Recently we had some people from Facebook that were here to enlighten us on new trends of the offences that are being conducted through Facebook. Some like Facebook lottery. And some other agencies too.* (Participant 21, ICT Team Lead)

Another participant made similar arguments by stating that due to the global nature of cybercrime, they collaborated with key stakeholders in proffering solutions to tackle cybercrime.

8.6 Training and Manpower

The training of staff and the recruitment of new staff was identified as one of the measures being undertaken to address cybercrime in Nigeria. These sub-themes were coded eight (8) times by different participants from different organisations. According to participant 10:

> *The Commission is making attempts to train more and more officers because the demand for digital forensic which provides digital evidence from cybercrime is huge. So the commission is currently training more and more people to increase the human capacity in investigating cybercrime. There is also an attempt to educate more and more officers on issues relating to cybercrime as well as also most judges are not well acquainted with cyber related crimes since they are intangible crimes so to speak, so the commission is making attempt to make sure more and more legal officers are educated.*(Participant 10, Forensic Examiner)

Participants 10's argument was centred on the training of staff in digital forensics and the education of judges to be able to understand cyber related crimes. Also, another participant argued that because of their experience in retrieving evidence from digital devices, they acted as training facilitators in educating staff from other departments and other organisations as well.

8.7 Benefits of Measures

The benefits of the measures used in tackling cybercrime varied from participant to participant. While some argued that it was effective, others said they could not know the benefits of the measures. However, in general thirty-two (32) responded stating that there was some form of benefit in deploying certain measures to investigate cybercrime. One of the participants argued that having more offices and more staff across the country had made the workload less, thus, reducing delays in investigating cybercrime. However, another participant from the Media department argued that they would not be able to know how beneficial the measures were until they got feedback from the public. Also, one of the participants, argued that no matter what measures were used against the cybercriminals, it was very difficult to keep up with the criminals because of the evolution of ICT.

9.0 DISCUSSIONS

Are Law Enforcement Agencies in Nigeria capable guardians in tackling cybercrime and explored in relation to Routine Activity Theory?

In order to discuss whether LEAs were capable guardians in preventing and investigating cybercrime, it was necessary to discuss the RAT element of absence of a capable guardian.

Finally, the challenges facing LEAs and the measures used by LEAs in tackling cybercrime was discussed in relation to the literature review.

9.1 Absence of a Capable Guardian

A guardian refers to anyone or anything that creates a protection for the target victim. The motivated offender is discouraged from committing an offense when they know that the target has a guardian. Therefore, capable guardians as elements of crime can be controlled, modelled or changed to prevent crime (Lopez, 2014). This research question is discussed from the viewpoint of stakeholders' role in tackling cybercrime and how the routine challenges they faced in the discharge of their duties limited them in being capable guardians in cyberspace. Figure 1.2 shows the challenges faced by LEAs and other stakeholders in tackling cybercrime.

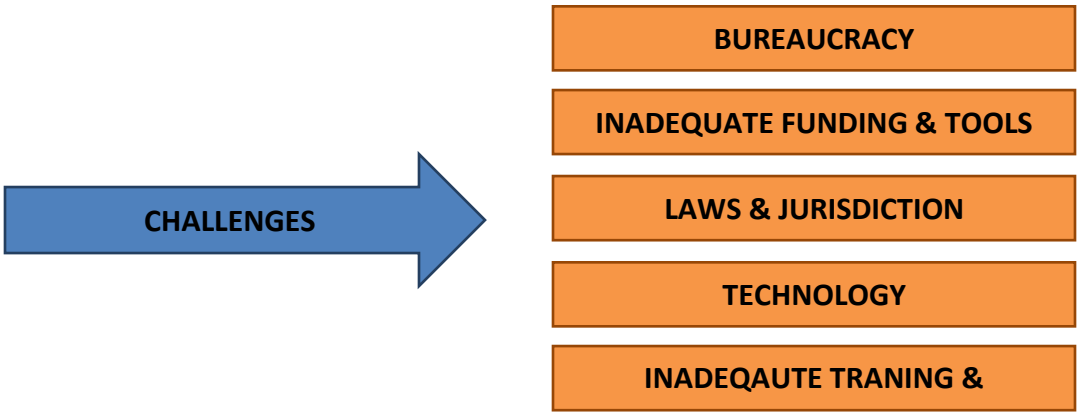

Figure 1.2: Challenges of Tackling Cybercrime (Capable Guardianship)

9.2 Bureaucracy

As shown in the research findings, bureaucratic bottlenecks within LEAs and other organisations hindered capable guardians such as the police in their endeavours for crime detection or prevention. Participants argued that bureaucracies in their organisation and other external large IT firms such as Google and Facebook made them incapable of protecting victims from cybercrime. This argument contradicts Yahaya's (2009) position that shows the Nigerian government as having a robust partnership especially with Microsoft with the aim of tackling cybercrime and software piracy in Nigeria. The findings also show that there is an issue in coordinating policies and practices in mitigating the activities of cybercrime. This finding contradicts Owens (2014) argument that places the blame on the traditional Nigerian police as having structural constraints which rendered it vulnerable to interference by the political elite, thus, limiting the police in effectively enforcing the law.

9.3 Laws and Jurisdiction

As shown by the research findings, the multiplicity of laws and different jurisdictions is a major challenge to stakeholders especially LEAs in tackling cybercrime globally. Participants argued that due to the transnational nature of cybercrime, it made it difficult to conduct a proper investigation without an existing legal instrument and agreement with other countries to back it up. This finding aligns with the UNODC (2013) argument that with the exception of Europe and America, most developing countries had insufficient powers to investigate and prosecute cybercrime. Furthermore, the finding aligns with Yar's (2007) argument of 'jurisdictional disparities' which could be problematic especially with policing or prosecuting deviant behaviours. The finding also shows that cooperation and collaboration between different countries on cybercrime issues is very challenging. The finding confirms Smith's (2013) argument that the harmonisation of laws and adoption of international conventions on cybercrime would make prosecution easier and improve the mutual assistance and extradition of criminals between countries. These findings also support Cohen and Felson's (1979) argument that lack of a capable guardian was a necessary condition for crime to take place. Yar's (2005) argument, that where the capable guardian was a person, their mere presence served as a gentle reminder that someone was looking. This aligns with the findings of the current study because the jurisdictional limitation of conventional police to deter crime from taking place was much more evident in cyberspace than in terrestrial space.

9.4 Technology

The finding from the research shows that the evolution of technology and the adoption of new technology to facilitate the commission of cybercrime by the criminals is a major challenge for stakeholders responsible for preventing, investigating or prosecuting cybercrime. This finding resonates with Chukkol (2014) who pointed out that Nigeria had witnessed the acceleration of crimes at a faster rate due to criminals embracing ICT to commit crimes. The finding also shows that some of the cybercrime investigators are playing 'catch up' in terms of their skillsets and training for investigating cybercrime. This finding aligns with Smith's (2003) argument that the investigation of cross-border cybercrime required adequate technical and forensic skills and knowledge. Also the finding aligns with Tiv's (2006) observation that the investigation of advance fee fraud required some computer knowledge which the criminals knew were beyond the skills of the traditional Nigerian Police Force. However, some of the findings especially from the 'Forensic Analyst' show that the affordability of storage devices makes the acquisition of

evidence from a digital artefact more difficult and time consuming because of low levels of qualified staff available to extract the information. This finding contradicts the ITU (2012) position which stated that even though the low cost of digital storage had increased, the number of digital sources of evidence, the digitisation and the use of such technologies had a great impact on procedures related to the collection of evidence and its use in court. The finding aligns with Cohen and Felson's (1979) argument that lack of a capable guardian was a necessary condition for crime to take place.

9.5 Inadequate Funding and Tools

The findings from the research show that inadequate funding for the procurement of tools and other logistical equipment needed to prevent and investigate cybercrime is a major challenge in fighting cybercrime. Some of the findings showed that the tools were either outdated or non-existent for investigating the ever evolving nature of cybercrime. This finding is in alignment with Smith (2013) who pointed out that the level of funding required for training and upgrading of equipment was inadequate. The finding also agrees with Dalton's (2012) assertions that cyber investigations were costly and that consequently, governments were reluctant to free up the funds. Also, the finding is in alignment with Cohen and Felson (1979) who pointed out that the lack of capable guardianship was a necessary condition for crime to take place in addition to the presence of a suitable target and a motivated offender.

9.6 Inadequate Training and Education

The findings of the research shows that inadequate training on the part of the investigators and lack of awareness on the part of the general public is a major challenge in tackling cybercrime. This aligns with Odumesi (2015) who pointed out that lack of cybersecurity training especially amongst LEAs had made it easy for fraudsters to operate in Nigeria leading to huge financial losses. The finding also aligns with Wall (1998) that public policing practices have been shaped by the time honored tradition of policing and could not respond to such rapid changes of ICT. The finding also shows that some of the lawyers and judges have inadequate knowledge about cybercrime, thus, making prosecution of cybercrime very difficult. This aligns with Buono's (2010) assertion that the current lack of adequate training on cybercrime for judges and prosecutors does not afford them the level of training required to deal with cybercrime and electronic evidence.

10. CONCLUSION

The policing of crime in both terrestrial and cyberspace has become a 'pluralistic endeavour' as responsibilities are shared between law enforcement officers, information security specialists and individual users (Grabosky, 2001). This study contributes to RAT, but expands the understanding of a capable guardian by including issues such as that inadequate funding and tools, training and education of law enforcement officers in Nigeria as rendering them unable to be capable guardians of potential victims of cybercriminal. Furthermore, the study contributes to RAT, by adding that the continuous evolution of technology has made law enforcement officers play 'catch up' to the criminals, while the borderless nature of cybercrime has made the application of laws and jurisdictions a cumbersome issue for policing cybercrime in Nigeria.

New insights from the current study regarding policy were raised in the research. The evidence suggested that the arrest and prosecution of criminals was not enough to serve as a deterrent to criminals. The issue of provision of education through specialised training of stakeholders involved in investigation, prosecution and prevention of cybercrime was greatly emphasised by the findings of the research. The improvement of the awareness level of individuals and the general public in protecting themselves was recommended.

REFERENCES

Abubakar, A.S (2009) *Investigating Fraud Schemes in Nigeria.* Paper presented at International Conference on Cooperation against Cybercrime. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2643

Adesina, O.S. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science* 13 (4)

Adesulu, D. (2017). Greed, cause of cybercrime – Don. *Vanguard News.* Retrieved 30 November, 2017 from https://www.vanguardngr.com/2017/06/greed-cause-cyber-crime-don/

Adomi, E., Igun, S. (2008) 'Combating cybercrime in Nigeria'. The Electronic Library 26 (5), 716-725

Alkaabi, A.O.S. (2010). *Combating Computer Crime: An International Perspective*. (PhD Thesis), Queensland University of Technology, Queensland. Retrieved from http://eprints.qut.edu.au/43400/

Barnard, J. (2014, 12 November). Global economy loses $445 to cybercriminals a year; now they are gunning for Africa's easy money. *Mail & Guardian.* Retrieved from http://mgafrica.com/article/2014-11-12-global-economy-loses-445bn-to-cyber-criminals-a-year-now-they-are-gunning-for-africas-easy-money

Clarke, R.V. (2004). Technology, Criminology and Crime Science. *European Journal on Criminal Policy and Research,* 10, 55-63.

Clarke, R.V., Felson, M. (2008). *Routine Activity and Rational Choice.* New Jersey: Transaction Publishers

Clarke, R.V., Felson, M. (1979). Opportunity makes the thief: Oractical theory for crime prevention. *Policing and Reducing Crime Unit: Research, Development and Statistics Directorate, 98, 1-36*

Clarke, R.V., Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 52, 170-183

Clough, J. (2010). *Principles of cybercrime.* Cambridge: Cambridge University Press

Cohen, L.E., Felson, M.K. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44(4), 588-608.*

Council of Europe. (2017). *Nigeria: Cybercrime policies and strategies.* Retrieved from https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/nigeria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=hu_HU

Cybercrime Prohibition, Prevention Act 2015.

Dalton, W. (2012). Cyber-crime policing completely inadequate, says ex-Scotland Yard detective. *IT Propotal.* Retrieved 15 November, 2017, from https://www.itproportal.com/2012/11/22/cyber-crime-policing-completely-inadequate-says-ex-scotland-yard-detective/

Dix, R.B. (2017). 5 Strategies for addressing cybercrime. *GCN.* Retrieved 10 March, 2017, from https://gcn.com/articles/2017/01/11/strategies-addressing-cybercrime.aspx

Felson, M. (1998). *Crime and everyday life,* 2nd Edn. Thousand Oaks, CA: Pine Forge Press.

Grabosky, P. (2001). Virtual criminality: Old Wine in New Bottle. *Social and Legal Studies,* 10(2), 243-249

Grabosky, P., Broadhurst, R. (2015). *The future of cyber-crime in Asia.* University of Hong King Press: Hong Kong

Hassan, A.B., Lass, F.D., Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. *ARPN Journal of Science and Technology,* 2(7), 626-631.

Internet Crime Complaint Center (2014). 2014 Internet Crime Report. Retrieved 23 July, 2016,from https://pdf.ic3.gov/2014_IC3Report.pdf

International Compliance Association ICA (2017). What is Financial Crime? Retrieved 28 December, 2017, from, https://www.int-comp.org/careers/a-career-in-financial-crime-prevention/what-is-financial-crime/

Internet World Stats (2017). Africa. Retrieved 2 January, 2018, from http://www.internetworldstats.com/africa.htm

ITU (2012). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved 20 July, 2016 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review,* 30(4), 470-486.

Kortjan, N., Solms, R.V. (2014). A conceptual framework for cyber-security awareness and education in Nigeria. *SACJ,* 52, 29-41

Longe, O., Mbarika, V., Ngwa, O., Wada, F. (2009). Crimincal Uses of Information and Communications Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact, Vol. 9 (3), 155-172*

Lopez, A. (2014). Routine Activity Theory of Crime. Retrieved 30 November, 2017, from http://lemoncenter.com/routine-activity-theory-elements-crime

Maghaireh, A.M.S. (2009). *Jordanian cybercrime investigations: a comparative analysis of search for and seizure of digital evidence.* (PhD Thesis), University of Wollongong. Retrieved from http://ro.uow.edu.au/cgi/viewcontent.cgi?article=4404&context=theses

McQuade, S.C. (2006). *Understanding and Managing Cybercrime.* New York: Allyn and Bacon.

Odumesi, J.O. (2006). Combating the menace of cybercrime: The Nigerian Approach (Project), Department of Sociology, University of Abuja. Nigeria

Olusola, M., Samson, O., Semiu, A., Yinka, A. (2013a). Impact of Cyber Crimes on Nigerian Economy. *The International Journal of Engineering and Science,* 2(4), 45-51.

Olusola, M., Samson, O., Semiu, A., Yinka, A. (2013b). Cyber Crimes and Cyber Laws in Nigeria. *The International Journal of Engineering and Science,* 2(4), 19-25

Saulawa, M.A., Abubakar, M.K. (2014). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013. *Journal of Law, Policy and Globalization, Vol. 32, 23- 33*

Sesan, G., Soremi, B., Oluwafemi, B. (2013). Economic Cost of Cybercrime in Nigeria. Retrieved 10 June, 2015, from https://pinigeria.org/downloads/research-reports/

Smith, R.G. (2003). *Investigating Cybercrime: Barriers and Solutions*. Paper presented at the Association of Certified Fraud Examiners, Pacific Rim Fraud Conference, Sydney. Retrieved from

Tive, C. (2006). *419 Scam: Exploits of the Nigerian Con Man.* New York: iUniverse Inc.

Tseloni, A., Wittebrood, K., Farrell, G., Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands: A cross-national comparative test of routine activities and lifestyle theories. *British Journal of Criminology, 44, 66-91*

UNODC (2013). Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Owen, O. (2014). The Nigerian Police Force: Predicaments and Possibilities. Retrieved 30 December, 2017, from, http://www.qeh.ox.ac.uk/sites/www.odid.ox.ac.uk/files/nrn-wp15.pdf

Wall, D.S. (1998). Catching Cybercriminals: Policing the Internet. *International Review of Law, Computers and Technology, 12:2, 201-218*

Wall, D.S. (2007). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice and Research*, 8:2, 183-205

WITFOR (2005) Social, Ethical and Legal Aspects. Retrieved 10July, 2015, from http://www.witfor.org/2005/themes/social-projrct3.htm

World Information Technology Forum (WITFOR) (2005). Social, Ethical and Legal Aspects. Retrieved 13 June, 2015, from http://www.witfor.org.bw/themes/social-projrct3.htm

Yahaya, F. (2009).EFCC, Microsoft tackle scammers, signs MoU. Retrieved 10 June, 2015, from, http://thenationonlineng.net/web2/articles/2031/1/EFCC-Microsoft-tackles-scammers-signs-MoU-/Page1.html

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4)407-427

Yar, M. (2006). *Cybercrime and Society.* London: SAGE