Unmasking Cyber Crime Issues in the Nigerian Cyber Space for effective Preventive Measures

Gulleng, Daskyes Yohanna[1]

Department of Sociology

University of Jos

Abstract

The complex nature of the Nigerian cyberspace has made it more difficult for unsuspecting members of the public to avoid being victims. This is partly because majority of Nigerians are ignorant of the changing dynamics of cybercrime and security. This article was an attempt at unmasking the mask behind cybersecurity issues in Nigeria to help reduce the rate of victimisation. It looked at the challenges faced by the security agencies in their effort at policing the criminal cyberspace which include lack of security awareness, expertise of the policing agencies as well as lack of proper legal framework. The paper recommended that securing the Nigerian cyberspace requires a multidimensinoal approach that involves the collaboration of players across various disciplines. It also advocated for a security culture where every member of the society is aware and willing to share information that would help security agencies to properly respond to any suspecting cybersecurity threat.

Key words: Cyber space, Cybercrime, Cybersecurity, Security, Victimisation,

Démasquer La Cybercriminalité Dans Le Cyber Espace Nigérian Pour Des Mesures Efficaces De Prévention

Résumé:

La nature complexe du cyberespace nigérian a rendu plus difficile aux membres du public pour éviter d'être victimes. C'est en partie parce que majorité des Nigérians sont ignorants de l'évolution de la dynamique de la cybercriminalité et la sécurité. Cet article est une tentative de démasquer le masque derrière les questions de cybersécurité au Nigeria pour aider à réduire le taux de victimisation. Il a examiné les défis auxquels sont confrontés les organismes de sécurité dans leurs efforts à l'ordre le cyberespace criminel qui comprennent le manque de sensibilisation aux

[1] Address for Correspondence: Dr. Gulleng, Daskyes Yohanna, Department of Sociology, University of Jos Email: dgullengs@yahoo.com, gullengd@unijos.edu.ng

questions de sécurité, de l'expertise des agences de police ainsi que l'absence de cadre juridique approprié. L'étude a recommandé que l'obtention de la Nigerian le cyberespace nécessite une multidimensinoal approche qui implique la collaboration d'intervenants de diverses disciplines. Il a également plaidé pour une culture de sécurité où chaque membre de la société n'est au courant et prêt à partager de l'information qui aidera les organismes de sécurité pour réagir correctement à tout soupçonner la cybersécurité menace.

Mots clés : Cyber Espace, La Cybercriminalité, La Cybersécurité, La Sécurité, La Victimisation,

Introduction

The continuous dominance of the internet in today's modern world is seen as part of the globalization process that is collapsing boundaries, dissolving group identities and is supposedly sweeping away old realities (Yar,2006). Similarly, the use of the cyber space is opening opportunities for people to make new discoveries on how to move their businesses online and to expand frontiers of knowledge. The internet provides tremendous opportunity for individuals and organisations to generate collect and utilize colossal amount of data which was earlier non-existent. Banks, financial organizations and enterprises are capitalizing on the unprecedented opportunities presented by this wave of digitisation to transform their business models. As observed by Cameron (2015), the world has been digitized to the extent where things that used to be real and tangible are now machine-generated or they only exist as bits and bytes. This development has also opened access to information that supports democracy, as it opens platforms for more participation and allows the flow of information which hitherto was under the control of state authorities.

While it is true that the cyberspace creates opportunities for legitimate social, economic and political activities, criminals and deviants take advantage of this to offend the 'collective conscience' of the society; a situation criminologists regard as 'opportunity structures' (Grabosky, 2003; Newman and Clarke, 2003, Yar, 2006). Attacks against businesses, financial institutions and nation states have become part of our daily lives as cases of online fraud and hacking hit headlines with such regularity. This paper explores issues relating to cybercrime and cyber security as they affect social, political and economic development in Nigerian. It also analyses challenges of policing the Nigerian cyberspace in terms of enforcement, legislation, investigation and prosecution. The paper further seeks to provide a roadmap for a more secured Nigerian cyberspace in view of the fact that Information Technology has become part of our daily lives.

Conceptual Review

Cyber crime

Different interpretations and understanding have been shared by experts within the cyber security circle including criminologists, sociologists, the police, legal and computer technology experts and other related security agencies on what cybercrime means. According to Kshetri

(2010), cybercrime is increasingly becoming more elusive in view of the confusion surrounding which definition to adopt. The way out of this dilemma however is not to see cybercrime as a single phenomenon but as a range of illicit activities whose 'common denominator' is the central role played by networks of information and communication technology (ICT) in their commission (Yar, 2006).

A more acceptable definition which takes into consideration these varying perspectives has been offered by Thomas and Loader (2000, p.3). They conceptualised cybercrime as those 'computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.' This definition is broader as it captures the connection between crime and deviance which are both recurrent features of contemporary developments around the internet and the cyberspace. Meanwhile, Cameron (2015) has attempted to frame the fundamental characteristics of cybercrime to include:

a. The conduct is facilitated by information and communications technology;
b. The conduct is motivated by intent to commit harm against a person or organization;
c. The perpetrated or intended harm encompasses conduct amounting to interference or damage to either tangible or intangible property owned by a person or organization; and
d. The conduct concerned is criminalized within either the jurisdiction of the victim or the jurisdiction of the accused.

Cyberspace

The usage of the term cyberspace is traceable to the work of Williams Gibson (1982, p.51) who argued that cyberspace is:

> A consensual hallucination experienced daily by billions of legitimate operators in every nation. It is a graphic representation of data abstracted from the banks of every computer in the human system. It is also an unthinkable complexity of lines of lights ranged in the non-space of the mind, clusters and constellation of data like city lights receding

This underscores the fact that the social-interactional features of the cyberspace environment involves primarily the collapse of space, time, barriers, many-to-many connectivity, and the anonymity and changeability of online identity that make possible new forms and patterns of illicit activity (Cameron, 2015).

Typologies of Cyber Crime

Cybercrimes have been classified along a number of different lines. One commonplace approach is to distinguish between 'computer assisted crimes' and computer focused crimes. Computer assisted crimes are those crimes that pre-date the internet, but which take on a new life in cyberspace (e.g. fraud, theft, money laundering, sexual harassment, hate speech, pornography).

Computer-focused crimes are those which have emerged in tandem with the establishment of the internet, and could not exist in isolation of it; such as hacking, viral attacks and website defacement (Furnell, 2002, Lilley, 2002). Similar to this classification is the one adopted by policing bodies such as the UK's National Hi-Tech Crime Unit, which distinguishes between 'old crimes, new tools' and 'new crimes, new tools' (NHTCU, 2004). While the above distinction is helpful, it may be rather limited for criminological purposes, as it focuses on the technology at the expense of the nature of social relationships that exist between offenders and their targets or victims.

Another alternative to the categorisation of typologies of cybercrime is drawn from criminal law which Wall (2001, p.3–7) sub-divided into four as follows:

1. Cyber-trespass. This involves crossing boundaries into other people's property and/or causing damage, e.g. hacking, defacement, viruses.

2. Cyber-deceptions and thefts. This includes stealing (money, property), e.g. credit card fraud, intellectual property violations or what is called piracy.

3. Cyber-pornography. This has to do with breaching laws on obscenity, nudity and decency.

4. Cyber-violence. This is common with crimes relating to psychological harm or acts that incite physical harm against others, thereby breaching laws relating to the protection of the person, e.g. hate speech, stalking.

5. Crimes against the state. This involves activities that breach laws protecting the integrity of the nation and its infrastructure (e.g. terrorism, espionage and disclosure of official secrets). Such a classification is helpful, as it allows us to relate cybercrime to existing conceptions of prohibited and harmful acts.

These classifications could further be subdivided according to the object or target of the offence as they are important in helping criminologists understand the forms in which they operate (Yar, 2006). While cyber trespass and cyber deception could be seen as crimes against property, pornography covers crimes against morality and cyber violence relates to crimes against the person.

The Problem

In Nigeria, the use of technology continues to rise with increasing access to computers and mobile device ownership growing exponentially. More and more people are now making use of the social media than before. The rate at which banks, financial institutions and other related organizations share data through online networks has increased. Millions of computerised machines in form of tablets, smartphones, ATM machines, security installations, environmental control systems and much more are all linked together, increasing inter-dependencies and loss of direct control of data security.

This growing access however comes with new risks and vulnerabilities that could undermine individual, group and corporate security. Chief among these is the global rise of cybercrime and professional cyber criminals (Symatec, 2016), mostly driven by a wide range of motivations such as pure financial gain, to raising the profile of an ideology, to espionage or terrorism as well as for economic and political reasons. The case of Russia and the 2016 election of the United States of America is an indication that cybercrime does not respect societal level of development. The unique characteristics of the internet which include offence dominance, difficulty in attribution of attacks, development of cyber weapons by states and the use of non-state actors to camouflage their actions are making cyberspace more and more vulnerable (Symatec, 2016, Cameron, 2015). This is because the internet enables them to manipulate and reinvent their social identity by giving false information about their personalities which are often times different form their 'real world' identities (Yar,2006, Ndubueze, 2016). More so, inappropriate cyber data has made it difficult to track cyber criminals and bringing them to justice.

Despite the fact that cybercrimes and threats of attacks are very real and the impact debilitating, knowledge of the activities of cybercriminals and cyber security is left at the mercy of what the media presents. Researchers within the field of criminology and security related agencies have little or no knowledge of the techniques and strategies of cybercriminals in Nigeria. Worthy of note also is the fact that literature on cybercrime is mostly dominated by foreign authors including those written about Nigeria. This is an indication that cybercrime and cyber security is under-researched in Nigeria even when the risks are everywhere. This paper is therefore is a wakeup call for criminologists' and security experts to espouse the issues with the desire to come to terms with the reality of the dangers of cybercrime.

Policing the Nigerian Cyberspace and Issues of its Safety

Globally, Cyber Security is linked to national security as it involves issues relating to public safety and developments within the economic, political or social spheres of any society (Muller, 2015). Addressing the security of the cyberspace of any country requires setting the rules of acceptable behaviour in the cyber world, curbing terrorist activities, enhancing the respect of human rights in cyberspace, or bringing cyber criminals to justice. Also, criminologists who have sociological orientation analyse cyberspace within the socio- economic, structural and environmental context in which such crimes occur. This is with the general belief that the structure of the society and the environment has a profound impact on how social interactions can take place (both licit and illicit), and so transforms the potential scope and scale of offending (Yar, 2006). In other words, the security of the cyberspace of a country is a reflection of the way governance is organized along social, economic, political and cultural lines. Thus, whether we become more vulnerable to cybercrime potential predators who can reach us almost instantaneously with ease depends to a very large extent on how strong our institutions are and how prepared the security architecture is.

In Nigeria, the primary agencies charged with the responsibility of protecting cybercrimes are the Economic and Financial Crime Commission (EFCC), the Independent Corrupt Practice and other related offences Commission (ICPC), State Security Service (SSS), and the Nigerian Police (Symatec, 2016). All these agencies play prominent roles in the fight against the new trend of social vice. The Nigerian Cyber Crime Act which was signed into law in 2015 also provides a unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. The act also ensures the protection of critical national information infrastructure, and promotes cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

Regardless of these however, the safety of the Nigerian cyberspace in the context of these complexities is not certain. This is due to the lack of security awareness or knowledge of the risks associated with cybercrimes and specialised training for the law enforcement agencies. These constitute the largest impediments to cyber security improvements. According to Olowu (2009), the approach of the Nigerian security agencies towards cyber criminality has not shifted from the military culture of repression. Nigeria police and other crime control agencies traditionally operate within local boundaries, focusing attention and resources on crimes occurring within their domains while cybercrime, is an inherently de-territorialized phenomenon. The sophisticated nature of the internet creates a range of entirely new demands upon the police which question their traditional local dominance and could in fact marginalise them completely (Wall, 2011). Cybercrime does not only produce problems for the police because internet-related offending takes place within a global context whereas crime tends to be nationally defined, but policing the internet is also a complex affair by the very nature of the traditional policing and security in place (Johnson & Shearing, 2003). This has made the Nigerian cyberspace more vulnerable as the security agencies are not well equipped with the required modern techniques to secure it.

Another issue relating to the security of the Nigerian cyberspace is the fact that the internet is dominated mostly by young people who are mostly unemployed. The high level of unemployment in Nigeria is a problem that is increasing daily. According to the National Bureau of Statistics (2016), the national unemployment rate increased to 13.9% compared to 10.4% in 2015. The statistics reveals that the unemployment rate is very high among youth, most of whom are university graduates with computer and internet competency. This combines to create a new generation of local hackers and cyber-criminals. According to Olowu (2009), although they do not have deep programming knowledge like experienced hackers who can create their own malware or viruses, they take advantage of many websites available for free that help them understand the basics behind hacking techniques with links to underground hacking sites and even free tools to use. Addressing the problem of cyber security in a country dominated by unemployed youth requires an approach different from traditional policing. It is about strengthening institutions that would absorb the teaming unemployed youth who automatically constitute fertile grounds for the growth and promotion of cybercrime.

Barriers to Providing Cyber security in Nigeria

Providing adequate security for the Nigerian cyberspace is faced with lots of challenges. First among the challenges is the fact that there is a significant lack of security awareness among users, whether by the general public or organisations and enterprises. Comparing security awareness in Africa to Europe or the US, one would see far less effort being made to raise awareness among users (Symatec, 2016). Poor security awareness means that investments to fight cybercrimes are minimal, leaving businesses vulnerable to fraudsters or online attacks. Nigeria is in dire need of strong ICT security policies rooted in awareness training, targeting users, employees and law enforcers to understand the risks and prevent attacks (Ribadu, 2007; Mazzitelli, 2007).

Lack of appropriate expertise also presents barriers to the effective policing of cybercrime. Investigation of such crimes will often require specialized technical knowledge and skills, and there is at present little indication that the police have the appropriate training and competence (Symatec, 2016, Mercke, 2012). Moreover, research indicates that many police do not view the investigation of computer-related crime as falling within the normal parameters of their responsibilities, undermining attempts to put such policing on a systematic footing (Hyde, 1999).

Although Nigeria has provided the legal framework, there are no deliberate steps at enforcing such laws. According to Symatec (2016), even where appropriate legal measures have been put in place, many countries (especially in the developing world, Nigeria inclusive) simply lack the resources needed to enforce them (Drahos and Braithwaite, 2002). In countries facing urgent economic problems, with states that may be attempting to impose order under conditions of considerable social and political instability, the enforcement of internet laws will likely come very low on the list of priorities, if it appears at all.

The United Nations Economic Commission for Africa (2014) further identified the following as challenges to providing cyber security in developing countries in the midst of prevailing cybercrime which could also be a reflection of the is happening in Nigeria.

These challenges are:

- Low level of security provisions sufficient to prevent and control technological and informational risks.

- Lack of technical know-how in terms of cyber security and inability to monitor and defend national networks, making African countries vulnerable to cyber espionage, as well as to incidences of cyber terrorism. However, awareness building is difficult if cyber security is not a government priority. A comprehensive understanding within governments is needed of the necessity of securing cyberspace and the technological challenges required. Otherwise, implementation of cyber security becomes difficult.

• Inability to develop the necessary cyber security legal frameworks to fight cybercrime. A survey of 21 countries conducted by ECA(2014) found that while many countries had proposed legislations, the level of deployment of security systems in both the private and the public sectors to combat cyber-crime was low. According to Muller (2015), a legal framework that reaches too broadly and is too ambitious is difficult to uphold; however, a framework that does not include enough is no solution either.

• Cyber-security concerns are broader in scope than national security concerns. Yet, few major significant cyber security initiatives in Africa have been implemented. As ICTs are hailed as the end-all to the many pressing problems of Africa, cyber security is a critical issue that needs to be dealt more comprehensively.

• There is a need to build an information society that respects values, rights and freedoms and guarantees equal access to information, while encouraging the creation of authentic knowledge and that can build confidence and trust in the use of ICTs in Africa.

• Generally limited levels of awareness of ICT-related security issues by stakeholders, such as ICT regulators, law enforcement agencies, the judiciary, information technology professionals and users. Muller (2015) further identified the following as challenges for developing nations (Nigeria inclusive).

Prospects for Effective Cyber Crime Prevention in Nigeria

Providing Cyber security requires multi-dimensional approach involving many disciplines and fields. The contributions of criminologists, sociologists, political scientists, economists, the legal profession and experts in cyber technology are needed. No government can fight cybercrime or secure its cyberspace in isolation. Nations have to take appropriate steps in their respective jurisdictions to create necessary laws, promote the implementation of reasonable security practices, incident management, and information sharing mechanisms, and continuously educate both corporate and home users about cyber security. The step taken by the Nigerian Government in enacting the Cyber Crime prohibition and Prevention Act 2015 is in the right direction. However, when it comes to tracking cyber criminals, it is not only the existence of laws dealing with cybercrimes but the political will to invest in research and man power training and appropriate cyber forensics data collection which are essential to bring criminals to justice.

On the background of these issues, Nigeria possesses considerable responsibility for making cyber security a reality. The government should not merely promote and encourage research and development in security but also promote a security culture and demand compliance with minimum security standards (security should be built into products and services), while strengthening law enforcement in respect of cybercrime. At the strategic level, it is necessary to ensure prevention, reporting, information sharing and alert management. It is also necessary to raise awareness of best practices in risk management and security. Another important requirement is for the government to key into the global platform for the coordination and harmonization of legal systems across nation states where information sharing works best in the fight against cyber criminality. At the same time, it is essential to provide education, information and training in information processing and communication technologies, not merely as security and deterrent measures but as part of a security culture and cyber code of conduct.

The security culture must be such that players are given the means to learn to manage the technological, operational and information risks that threaten them in connection with the use of new technologies. In this context, Nigeria must encourage reporting of instances of cybercrime and ensure that there is trust between the various players of the economy who mostly operate in the private sector and the legal and law enforcement authorities identified above. Surveillance, detection and information centres for IT and criminal risks must be made operational in order to provide prevention, necessary for the control of those risks.

Nigeria should have a clearly defined development policy that is all encompassing for the information society reflecting its own values and norms. This is so central in view of the prevailing socioeconomic realities the country is faced with. It should be noted that to contain cybercrime in a global, centralized and coordinated manner, a response is needed at the political, economic, legal and technological level. In the case of Nigeria, addressing the problem of unemployment is one of the very crucial ways in which cybercrime could be addressed. When the youth are engaged, the tendency for them to explore the negative opportunities provided by the internet would be less.

References

Cameron S., D., B. (2015). Investigating and Prosecuting Cyber Crime:Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9 (1), 55-119.

Drahos, P. with Braithwaite, J. (2002) *Information Feudalism: Who Owns the Knowledge Economy?* London: Earthscan.

Furnell, S. (2002) *Cybercrime: Vandalizing the Information Society*. London:Addison-Wesley.

Gercke, M (2012). (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. International Telecommunications Union available at www.itu.int/ITU-D/cyb/cybersecurity/legislation.html.

Gibson, W. (1984). *Neuromancer*. New York: Acc.

Grabosky, P. (2003) ‘Cyberterrorism’, at http://www.alrc.gov.au/reform/summaries/82.htm.

Hyde, S. (1999). A Few Coppers Change. *The Journal of Information, Law and Technology (JILT)*, 2, at http://www.law.warwick.ac.uk/jilt/99–2/hyde.html.

Kshetri, N (2005). Pattern of Global Cyber War and Crime: A Conceptual Framework, *Journal of International Management*, 11(4), 541-562.

Lewis, B., C. (2004), Prevention of Computer Crime amidst International Anarchy, *American Criminal Law Review*, 41, 1353.

Lilley, P. (2002) *Hacked, Attacked and Abused: Digital Crime Exposed*. London: Kogan Page.

Mazzitelli, AL (2007). Transnational Organised Crime in West Africa: The additional Challenge. *International Affairs*, 83(6), 1071-1090.

Muller, L.P (2015). Cyber Security Capacity Building in Developing Countries: A Policy Brief. Norwegian Institute of International Affairs.

Ndubueze, P.N. (2016). Cyber Criminology and the Quest for Social Order in the Nigerian Cyberspace. *The Nigerian Journal of Sociology and Anthropology*, 14(1), 32-48.

Newman, G. and Clarke, R. (2003) *Superhighway Robbery: Preventing e-commerce Crime*. Cullompton: Willan Press.

NHTCU National Hi-Tech Crime Unit (2004) 'What is Hi-Tech Crime?', available at http:// www.nhtcu.org./nqcontent.cfm?a_id=12334&tt=nhtcu.

Olowu, D (2009). Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa. *Journal of Information, Law & Technology*.

Ribadu, N (2007). Cyber-crime and Commercial Fraud: A Nigerian Perspective. A paper presented at the Congress Celebrating the Fortieth Annual Session of the UNCITRAL, Vienna, Austria, 9-12 July 2007.

Shearing, C., & Ericson, R. (1991). Culture as figurative action. *British Journal of Sociology*, 42(4), 481–506.

Symatec (2016). Cyber Crimes and Cyber Security Trends in Africa. Symatec, available at Symantec Worldwide: http://www.symantec.com/

The United Nations Economic Commission for Africa (2014). Tackling the Challenges of cyber security in Africa. A Policy Brief.

Thomas, D. and Loader, B. (2000) 'Introduction – Cybercrime: Law Enforcement, Security and Surveillance in the Information Age', in D. Thomas and B Loader (eds), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age.*

Wall, D.S.(2011). Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. *Police Practice & Research: An International Journal*, 8(2):183 205.

Wall, D.S. (2001). Cybercrimes and the Internet. In D.S.Wall(ed). *Crime and the Internet.* London. Routledge.1-17

Yar, M (2006). *Cyber Crime and Society*. London: SAGE Publications