Investigating Cybercrime in Nigeria

Mufutau Temitayo Lamidi
University of Ibadan, Nigeria

INTRODUCTION

Information communication technology (ICT) is a means by which relevant online information is managed effectively to achieve desired results. It involves the use of various electronic gadgets such as computers (desktop and laptop), tablets, iPad and other phone types as tools to access, manage or handle different forms of information on the Internet and derive from it the advantages it offers. Given the several advantages of ICT to national development, Nigeria, among other countries, has keyed in into it to partake of the benefits ICT offers. With a population of 186,987,563, Nigeria's Internet penetration is estimated to be 52.02% (African Union Commission & Symantec, 2016: 81). The Internet is gaining popularity by the day as is gains adherents with more people using it for their various needs. However, the advances in ICT have been both a blessing and a curse to Nigerians. It has improved people's lives in different areas, ranging from information dissemination to social networking, advertising, marketing, Internet banking and money transfer, among others. It has made conducting businesses by some professionals, especially in banking and finance, journalism and entertainment sectors, more effective. Particularly, it has enhanced government's cashless policy, which discourages citizens from carrying huge cash around town whether for business transactions or to purchase commodities in markets. Despite its several advantages, it also has disadvantages, principally, in cyber-attacks. Nwogwugwu & Uzoechina (2015) observe that although crimes (especially economic crimes) predated globalization, globalization and ICT that have promoted Nigeria's economy globally have become useful tools in the hands of economic offenders to commit crimes and launder proceeds of their illicit acts.

Reports are rife in newspapers, online forums and blogs about incidents of cyber-attack in Nigeria. This study investigates different cyber-attacks which are usually subtle and felt largely by the generality of Nigerians. The aim is to examine its nature in order to offer advice towards stemming its tide.

BACKGROUND

Cybercrime is described as "crimes committed on the internet using the computer as either a tool or a targeted victim." (Kamini, 2011: 240). The computer is a tool when it is used against a victim such as in theft, pornography and online gambling; and the computer is a target when its programme, software or structure is deliberately destroyed/vandalised.

Cybercrime can be targeted at organisations, individuals or the society at large. For organisations, governments, firms, companies or groups of individuals are usually targets. In this wise, there is unauthorised access to/control of computer system, possession of unauthorised information, cyber terrorism against government organisation and distribution of pirated software (Kamini, 2011). For instance, Symantec (2016: 81-82) reports that Nigeria has faced a daily increasing challenge in vulnerability User Datagram Protocols, UDP, up to 25%; botnet drones, 20%; web defacement of government websites, 3%

DOI: 10.4018/978-1-5225-9715-5.ch069

increase, weekly average; and phishing, 4% daily average. Hence, it is no surprise that Nigeria has ranked third in four consecutive years (2006, 2007, 2008 and 2009) on the list of world cybercrime perpetrator countries (Dagaci et al., 2014).

For individuals, their person or property is the target. Individuals often get harassed through e-mail, cyber stalking, dissemination of obscene materials, defamation, indecent exposure, e-mail spoofing, cheating and fraud. Their properties may be vandalised, viruses may be introduced into their systems, and there may also be intellectual property thefts, Netrespass Internet time theft and unauthorised control/access over their computer systems.

For the society at large, cybercriminals target anyone and everyone indiscriminately. In this category are cybercrimes such as (child) pornography, polluting the youth through indecent exposure, trafficking, financial crimes, sale of illegal articles, online gambling and forgery.

Cybercrime has been studied from different perspectives. Studies such as Ayofe and Osunade (2009) and Dagaci et al. (2014) view Cybercrime from a generalist point of view. Kamini (2011) and Toyo (2017) actually investigated it as a phenomenon, especially in their country or state of abode, and Aribake (2015) and Ojeka et al. (2017) studied it from a professional angle. In addition, while Okeshola & Adeta (2013) and Omodunbi et al. (2016) studied cybercrime from a sociological perspective, Nwogwugwu & Uzoechina (2015) looked at it from an economic perspective, Chawki (2009) from a legal perspective, and Boniface & Michael (2014) from a technological perspective.

Against the backdrop of Nigeria being ranked third on the list of world cybercrime perpetrator countries for four consecutive years, Dagaci et al. (2014) examine the major causes, forms, rate of victim, economic cost to Nigeria and alternative strategies of reducing the menace. Ayofe and Osunade (2009) also define the concept of cybercrime and identify reasons for it, how it can be eradicated, those involved and the reasons for involvement. They suggest how to detect criminal mails and proffer solutions to checking the increasing rate of cybercrimes and criminals.

Kamini (2011) is one of the studies that examine the effect of cybercrime in India. It discusses the types of cybercrime, the mode and manner of its application as well as the legal frame operating against cybercrime in India. It finally suggests what individuals and corporate bodies can do to prevent cyber-attack. Another study is Toyo (2017), which focuses on Abraka in Delta State of Nigeria. The study examines the causes and types of cybercrime prevalent in Abraka, the players and the impact on the society. It identifies causes of cybercrimes as urbanisation, quest for wealth, weak implementation of cybercrime laws and ill-equipped security agencies as well as negative role models. It observes that yahoo attack and hacking are the most prominent cybercrimes in Abraka; and cyber-attacks often result in financial losses, mistrust of youths, carnal abuse and government's abandonment of rural communities. It suggests some control measures like establishment of national institutions, awareness and training, upholding ethical and moral standards, using computer forensics and anti-virus, and establishment of laws to control the menace.

Okeshola & Adeta (2013) and Omodunbi et al. (2016) also discuss cybercrime from the perspective of education and society. The researchers drew data from tertiary institutions in Zaria and Ekiti State. They identified different reasons why cybercrime thrives and proffered suggestions to curb its menace. The noted that youths, especially males, are the major players in cybercrime. Okeshola & Adeta, for instance, identified some of the motivational factors as