CURTAILING THE UPSURGE OF CYBERCRIMES AMONGST THE YOUTHS IN NIGERIA: THE SOCIO-PHILOSOPHICAL WAY FORWARD

PHILLIPS OLUBIYI
Department of General Studies, Federal Polytechnic, Ilaro, Ogun State, Nigeria
olubiyi.philips@federalpolyilaro.edu.ng

Abstract

Currently Nigeria is reportedly responsible for at least 9.3 billion dollars out of the total financial loss to rising phenomenon of cybercrimes. The internet's limitless expanse is referred to as cyber-space. Cyber-security refers to the set of policies put in place to secure the cyberspace. The term "cybercrime", refers to a group of organized crimes that target both cyberspace and cyber security. The Internet is one of the most rapidly developing sectors of technological infrastructure. The development and use of the internet over the last few decades has provided everyone with this possibility. Every day, Google, Wikipedia, and Bing, to name a few, provide answers to millions of inquiries. Cyberspace is a place that has almost anything that a person is searching for. With the breakthroughs in information accessibility and the benefits of the internet has come an increasingly and expanding set of disadvantages which is Cybercrimes. Cyber security has grown to become a global priority as threats to it have gotten more serious. The purpose of this paper is to investigate the definitions of cybercrime and cyber-security. The paper also attempted to outline the dangers of cybercrimes, identifies the causes of cybercrimes, and pro-offered solutions for eradicating cybercrimes especially in Nigeria.

Keywords: Cyber-Space, Cyber-Security, Global Cyber Security Awareness Culture

Introduction

The theme of cybercrime has been debated by many people, each with their own point of view, with most coming at it from different angles. Cybercrimes has progressed beyond traditional crimes and thereby posing a threat to the national security of all governments, including technologically advanced ones such as the United States. While the internet has eased various business activities like as sorting, summarizing, coding, editing and generating real-time processing mode for businesses, industries, governments, and non-profit organizations, the internet has also developed unforeseen negative effects including a variety of criminal activities, spamming, credit card fraud, ATM fraud, phishing, identity theft, as well as become a flourishing shelter for cyber miscreants to commit various heinous crimes (Strassmann, P. A. 2009).

Nigeria has a worldwide reputation. This is consistent with the fact that the country has come to realize the full potentials of the internet. However, Nigeria has also gained a global reputation for criminal activities, particularly financial scams aided by the use of the internet. Roseline (2012) argued that "Nigerian cyber thieves are constantly reinventing new techniques of committing a variety of cybercrimes, and the present strategies put in place by the concerned authorities and agencies of government to track these criminals are no longer adequate. The victims of cybercrimes also often exhibit increasing naivety and gullibility in the face of the fake opportunities presented by the internet con artists.

Statement of Problem and Objectives of study

This paper attempted to examine some of the gaps that still exist in the Federal government of Nigeria's cyber security architecture and policies with the aim of providing innovative strategies to fight against cyber aided financial losses, loss of Nigeria's reputation, and the Vulnerability of Nigeria's Information and Communication Technology (ICT) systems and networks. In addition, the paper also argued that inadequacy of cyber infrastructure, poor national databases, proliferation of cybercafés and the existing porosity of the internet in general still remains problematic for the country.

Literature Review

According to reports, Nigeria is accountable for at least $9.3 billion of the total financial losses caused by the rising phenomenon of cybercrime (Afon, 2016). This has drawn scammers and intruders of all stripes who are searching for

openings and prepared to attack their victims. In a larger sense, "cybercrime" refers to illegal activities done with the explicit purpose of extorting valuables from victims utilizing electronic equipment (computers), a communication network (the internet), and data before exploiting a victim's weakness. Aghatise (2006).

The purpose of cybercrime is to propagate malware, gather illegal data, and gain unauthorized access to a victim's computer in order to make money or steal sensitive data from the victim. Nigerian youths (aged 18 to 45) have profited from the rapid growth of the internet and technology by continuing to commit online fraud.

Due to the increased usage of cyberspace, the rate of cybercrimes has increased, posing a serious threat to global economy, national infrastructure, national security, governance, and technology. The goal of cybercrime is to engage criminal activities using a computer as a target or a tool, depending on the context of the vulnerability involved. There are many other methods, including ATD spoofing, identity theft, cyber-stalking, hacking, phishing, cyber-terrorism, online chat rooms, cyber-espionage, fraudulent electronic mail, etc.

Most Nigerian youth engage in cybercrime as a commercial opportunity driven by selfishness and selfish financial gain, as well as a result of unemployment, poverty, and weak government, as well as the track record of success in certain cybercrime cases. Since cybercrime is easy to learn and doesn't require any formal education, it intrigues individuals and has generated a lot of interest among young people from all walks of life. In addition, it is a crime committed by proxy or with less physical presence, and it also entails fewer resources compared to the damage they inflict L. Laura (1995).

A substantial section of Nigeria's social media and the internet ecosystem, where money, data, and transactions are exchanged, is taken up by cybercriminals who go by the names "yahoo-yahoo,""419 stars," and "yahoo plus." They have a well-known reputation and Live a luxurious lifestyle owing to the money they make from online scamming. They even go so far as to use online surfing and spiritual elements (magical rings, wrist incisions, etc.) to cast a spell on their victim and convince them to comply with their requests. Internet crime in Nigeria is heavily networked and socially organized; even as insiders and bank staff assist it by leaking sensitive customer data and enabling money transfers through domiciliary accounts, credit cards, and money gram.

Implications of Cybercrimes on Victims.

Psychological Implications:

Online victims of cyber-attacks typically experience emotional distress, which can lead to depression or acute stress disorder (ASD) (Schaeffer (2009). Based on examination of various literature, it has been observed that cyber terrorism (a sort of cyber-attack) raises anxiety in the victim's psyche, necessitating a rise in security improvements to avoid additional attacks and recover confidence (Strassmann, P. A. 2009). Most psychological victims of cyber-attacks believe they are to fault for the assault and choose not to engage anybody or manage the matter themselves. Isolation and drug misuse are two further consequences of the psychological effects of cyber attacks on their victims.

PhysicalImplications:

Cyber-attacks have progressed beyond attacks on data, information, and gadgets to attacks on physical structures. These physical attacks are aimed at critical infrastructure (such as power grids), medical facilities, and financial institutions. A literal example would be when a cyber-attack victim's location is monitored without his knowledge using his smartphone and Google Maps.

Educational Implications:

With the introduction of social media, the youth in Nigeria are becoming more conscious of cybercrime. This has significantly boosted the desire to participate in cybercrimes as a result of observing the affluent lifestyle displayed on social media, clubs, and other social occasions without realizing the risk underlying this money. Some young people go so far as to drop out of schools in order to join the cybercriminal pyramid.

Economical Implications:

The most prevalent negative consequences of cybercrimes includes Revenue losses, company interruption, profit pilferage, and welfare losses. In most circumstances, concerned stakeholders lack records of losses incurred or, to put it another way, conceal loss information. Every year, cybercrimes costs Nigerians millions to billions of naira, yet stakeholders prefer to see it as a necessary evil, a price to pay for business continuity, and a normal cost of doing business.

Strategies Adopted by Cyber Criminals in Nigeria

Next of kin Approach:

The Yahoo men use an old tactic in which they send emails to victims (referred to as Mugu) while posing as a person with a disability in need of assistance or a well-known businessman in the country. They take on many different forms, such as an oil tycoon who needs to export a large barrel of crude oil but needs millions of Naira to do so, or a banker of a deceased person who has a sizeable sum of money stashed away somewhere only he or she knows, necessitating the victim's participation as the next of kin.

After convincing the victim of the lie, he will be taken to see a number of significant lawyers and government officials who will be in charge of transferring the funds. At this point, they may invite the victims over to meet with their counterparts and extort money from them for logistics, but they do not get payment before the victims realize they have been tricked.

Romantic Relationships (Sweetheart Swindling) Approach

This tactic starts with making contact with the victim preferably a foreigner oftentimes through social media while using false identification, and then it progresses to creating an online romance or friendship with them. Once they acquire the victim's trust, they start to make demands, which increase over time until the victim is thoroughly taken advantage of (Roseline, O. Moses-kè 2012). **Other local methods**

Cybercriminals in Nigeria call their victims, posing as bank customer service representatives and asking them to revalidate their accounts. They do this by providing their victims with convincing information, such as the last four digits of their credit card, their email address, or any other information needed to carry out social engineering on the victim. They would take out every naira from that account if they were successful.

Methodology

This paper examined and synthesized significant facts about the issue under discussion using a theoretical and systematic analysis technique that included a review of previously published publications. It also applied a variety of secondary data sources, such as periodicals, newspapers, websites, and government records, to support its results, conclusions, and suggestions. The paper might possibly serve as a forerunner to more in-depth future studies.

Discussion and Findings

Computer crimes are more difficult to identify and investigate because of the speed and strength of current global information technology. Communications networks, for example, now cover the world, allowing a small personal computer to connect to locations in different hemispheres or continents with ease. This poses serious problems especially in terms of jurisdiction, evidence availability, investigative coordination, and the legal framework(s) that may be applied to criminal activities that occur.

New technologies give rise to new notions that lack legal equivalent or legitimacy. Viruses, on the other hand, use the resources of the infected system without the authorization of the owner. As a result, even a harmless infection might be misinterpreted as a system intrusion, electronic graffiti, or a harmless prank. However, the main argument is that the legal system, and hence the definition of computer crime, is reactive and unable to include new computational notions or actions.

Information has a number of unique and abstract features, such as the ability to remain in the owner's possession after being duplicated or stolen. The legal system has struggled with the ramifications of this in a computer-based framework throughout the previous decade. Traditional notions of copyright, patent rights, and theft have clearly been strained when applied to software and computer-based information, owing to the fact that existing concepts of theft and break-in, for example, relate to common notions of permanent deprivation or removal (theft) or physical damage (break-ins).

The ease and degree to which digital information may be altered and translated is a related attribute. That is, a piece of information (such as a program) can be represented in a wide range of informative formats. It can be represented as program text (source code), executable code (binaries), or it can be changed in a variety of ways, such as mathematically, encryptedly, or converted to, instance, a holographic picture or a piece of music. The music, picture, or encrypted text can be translated back to its original form as long as the method(s) of translation are known. As a result, the informational form in which it exists may eventually lose its legal existence.

A critical evaluation of some of the factors that continues to aid and deepens cybercrimes among the youth in Nigeria includes the rate of unemployment in the country which remains worrying, and still increasing by the day. Companies are going out of business, and financial institutions are going bankrupt. Nigeria is classified as a third-world country on a global scale. Poverty is becoming more prevalent. The wealthy are becoming richer, while the poor are becoming poorer. Small scale businesses have been grounded due to lack of basic utilities and existing epileptic power supply. All these factors combined have continued to conspire against efforts to stem the tide of cybercrimes amongst the Nigeria youth.

Conclusion and Recommendations

This paper has demonstrated that youth engagement in cybercrimes in Nigeria has been necessitated by a variety of reasons, which if properly contained, will have a good impact on the nation. The government, family, and youngsters all have significant roles to play in this Situation since coordinated efforts would favorably impact present and future Nigerians, restore the country's international standing, and boost its economy. Cybercrime excesses may be greatly reduced by regulating abusive internet and social media use, as China, Japan, and other global powers have done.

In addition, the security of individuals and corporate organizations must be regularly maintained and updated, as cybercrimes lack the traditional paper audit trail, making them difficult to prove and frequently requiring the Knowledge of experts in computer technology and internet protocols. Finally, corporate organizations in Nigeria must be educated by the government at all levels on the best global business practices for effective cyber security management.

References

E. Aghatise (2006), "*Cybercrime definition*," Computer research Centre. International Telecommunication Union, Retrieved fromhttp://www.itu.int/en/Pages/default.aspx

Laura, A. (1995): *Cyber Crime and National Security*: The Role of the Penal and Procedural Law",Research

Roseline, O. Moses-Òkè (2012*): Cyber Capacity Without Cyber Security*: A Case Study Of Nigeria's National Policy For Information Technology (NPFIT), *The Journal Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved from* *www.Miami.Edu/Ethics/Jpsl*

Roseline, O. Moses-Òkè (2012): *Cyber Capacity Without Cyber Security*: A Case Study Of Nigeria's National Policy For Information Technology (NPFIT), The Journal Of Philosophy, Science & Law Volume 12, May 30, 2012, Retrieved from www.Miami.Edu/Ethics/Jpsl

Schaeffer, B. S., et al. (2009): *Cyber Crime And Cyber Security:* A White Paper For Franchisors, Licensors, and Others

Strassmann, P. A. (2009): *Cyber Security for the Department Of Defense*, Retrieved July 10, 2011 Fromhttp://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

Strassmann, P. A. (2009): *Cyber Security for the Department Of Defense*, Retrieved July 10, 2011 Fromhttp://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

Afon R. (2016): *Nigerians responsible for $9.3b in global loss to cybercrime.* Retrieved October 28,2016 Fromhttps://guardian.ng/news/nigerians-responsible-for-9-3b-in-global-loss-to- cybercrime/