AN EXAMINATION OF THE TYPES OF DARK WEB AND CYBERCRIME IN NIGERIA

BY

DR THOMAS M. ISRAEL
DEPARTMENT OF LIBRARY AND INFORMATION SCIENCE
UNIVERSITY OF PORT HARCOURT
PORT HARCOURT

ABSTRACT

The study was carried out to strategically assess dark web and cybercrime threats in Nigeria. The population of this study comprised all professionals in computer science, computer engineering and security agents who have been exposed to cyber crimes, cyber security and general computer science. The study adopted a descriptive survey design, while stratified random sampling technique was used in selecting 400 respondents. The instrument for data collection, which was tagged "Dark Web and Cybercrime Threat Mitigation Questionnaire (DWCTMQ)", was administered to the respondents and used for the study. The instrument was vetted by experts in computer science as well as test and measurement before the reliability test was conducted with 40 computer experts who did not form parts of the main work and it produced the average reliability coefficient of 0.87, proving the instrument to be reliable for the study. Data collected were analysed using percentage analysis, mean statistics and goodness of fit chi-square analysis. From the results of the data analysis, it was observed that there is high level of dark web and cyber crimes activities in Nigeria. It was also observed that there are various types of threats caused by dark web and cyber crimes in Nigeria including stealing of data, havoc on individuals and organizations by the criminals, advanced persistent threats, distributed denial of service attacks, botnets, destructive malware, the growing challenge of ransom ware. etc. One of the recommendations was that cyber security should be seen by all as a shared responsibility which requires the attention of a broad range of stakeholders with effective public/private partnership that incorporates businesses and institutions of all sizes to produce successful outcomes in identifying and addressing threats, vulnerabilities and overall risk in cyberspace.

Key Words: Dark Web, Cyber Crimes Activities, Cyber Threats, Nigeria

INTRODUCTION

In recent times, our society has been increasingly relying on the internet and other information technology tools to engage in personal communication and conduct business activities among other several benefits. While these developments allow for enormous gain in productivity, efficiency and communication, they also create a loophole which may totally destroy an organisation. The term cybercrime can be used to describe any criminal activity which involves the computer or the internet network (Okeshola, 2013). This term is used for crimes such as fraud, theft, blackmail, forgery, and embezzlement, in which computers or networks are used.

According to Moore (2005), cybercrime, or computer oriented crime, is crime that involves a computer and a network, the computer may have been used in the commission of a crime, or it may be the target. Warren, Kruse, Jay and Heiser (2002) assert that cybercrimes

can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS)".

The Dark Web is a term that refers specifically to a collection of websites that exist on an encrypted network and cannot be found by using traditional search engines or visited by using traditional browsers. Almost all sites on the so-called Dark Web hide their identity using the Tor encryption tool. A relatively known source for content that resides on the dark Web is found in the Tor network. The Tor network is an anonymous network that can only be accessed with a special Web browser, called the Tor browser (Tor, 2014). It has the ability to hide ones identity and activity and also spoof your location so it appears you're in a different country to where you're really located, making it much like using a VPN service.

Paganini (2012) asserts that each day, our Web actions leave footprints by depositing personal data on the Internet. This information composes our digital identity, our representation in cyberspace. Internet anonymity is guaranteed when Internet Protocol (IP) addresses cannot be tracked. Tor client software routes Internet traffic through a worldwide volunteer network of servers, hiding user’s information and eluding any activities of monitoring. This makes the dark Web very appropriate for cybercriminals, who are constantly trying to hide their tracks (Paganini 2012). The dark Web is also the preferred channel for governments to exchange documents secretly, for journalists to bypass censorship of several states and for dissidents to avoid the control of authoritarian regimes (Gehl, 2014). Anonymous communications have an important place in our political and social discourse. Many individuals wish to hide their identities due to concerns about political or economic retribution. The dark web also hosts markets of illegal goods (such as counterfeit products, drugs, and IDs) and financial crime services (such as money laundering and bank frauds). It hosts markets offering pedophilia content, hitman services, conventional and chemical weapons purchase, and illegal medical research.

According to Maitanmi (2013), responding to cybercrime is even more challenging because the economics favor the criminals. With just a laptop, a single individual can wreak havoc on individuals and organizations with minimal cost and little risk of being caught. More advanced technologies and protective measures will eventually deter nefarious conduct, help security officers catch and prosecute perpetrators and level what has become an unbalanced playing field. This study therefore seeks to strategically assess dark web and cyber crime threat mitigation in Nigeria.

Statement of the Problem

Over the years, the alarming growth of the internet and its wide acceptance has led to increase in security threats. In Nigeria today, several internets assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing. Cybercrime and crimes committed in the dark web are threats against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Lack of strong cyber crime laws has encouraged the perpetrators to commit more crime knowing that they can always go uncaught. There is the need for our government to come up with policies that address cybercrime and the nefarious activities done on the dark web and enforce such laws so that criminals will not go unpunished. This study therefore seeks to strategically assess dark web and cyber crime threat mitigation in Nigeria.

Objectives of the study

The main objective of the study is to strategically assess dark web and cybercrime threats mitigation in Nigeria, while the specific objectives are as follows:

1. To examine the level of dark web and cyber crimes activities in Nigeria.
2. To find out the types of threats caused by dark web and cyber crimes in Nigeria.

Research Questions

The following research questions will be answered:

1. What is the level of dark web and cyber crimes activities in Nigeria?
2. What are the types of threats caused by dark web and cyber crimes in Nigeria?

Hypotheses

The null hypotheses will be tested:

1. There is no significant difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria.

LITERATURE REVIEW

Level of Dark Web and Cyber Crimes Activities in Nigeria

Cybercrime and dark web activities are trends that are gradually growing as the internet continues to penetrate every sector of our society and no one can predict its future. The crime usually requires a hectic task to trace. Sui, Caverlee and Rudesill (2015) asserts that when it comes to the availability of fake goods, everything from counterfeit train tickets to drugs and passports can be found on the dark web. While some consumers purposely seek for places to purchase items on the Deep Web, many internet users find these sites inadvertently or are purposely directed there through suspect links on social media platforms or websites.

Colbaugh and Glass (2012) opine that vast quantities of private information, such as log-in credentials, banking and credit card details, are peddled with impunity on crypto-marketplaces. Cybercriminals also offer their services for hire and even provide tutorials on code-breaking and how to infiltrate corporate networks. Cybercrime itself has become a service that is offered pervasively on the Dark Web. With Bitcoin used as the preferred currency, every transaction between buyer and seller can be conducted anonymously on the Dark Web.

According to Abbasi and Chen (2010), most of the content on the Deep Web contains information for legitimate uses –including corporate intranets or academic resources residing behind a firewall, social media sites hidden behind a log-in page, online forms, pop-up ads and pages that are unlinked to other sites. However, some sites on the Deep Web also represent potentially unauthorized or suspicious content, such as phishing sites that collect user credentials, sites that disseminate malware, websites and marketplaces that sell counterfeit goods and peer-to-peer sites where piracy often takes place. Consumers may unknowingly stumble upon these unauthorized sites through spam emails, advertisements or cyber squatted domains, and are at risk of unwittingly releasing personal information or credentials to fraudulent entities (Abbasi and Chen, 2010).

French, Epiphaniou and Maple (2013) asserts that deeper beneath the surface layer of the Internet lies the Dark Web, a smaller but potentially more dangerous subset of the Deep Web. The Dark Web is a collection of websites and content that exists on dark nets–overlay networks whose Internet Protocol addresses are completely hidden. Both publishers and visitors to Dark Web sites are entirely anonymous. Dark Web content can be accessed only by using special software such as Tor, Freenet, Invisible Internet Project and Tails. Tor is free to download and use, and enables anonymous access and communication within the Dark Net.

Around 2.5 million people access Dark Web content through Tor daily. It is often used by strong privacy advocates, such as journalists and law enforcement agencies that may be searching for dangerous or sensitive information and do not want their online activity tracked. The very anonymity of the Dark Web makes it an ideal foundation for illicit and criminal activity.

According to Lakshmi (2015), as at 2003, the United States and South-Korea had the highest cyber-attacks of 35.4% and 12.8% respectively. With the population of Nigeria placed at 160 million from the last census carried out in 2006, a recent statistics revealed that about 28.9% have access to the internet (Hassan, 2012). It was also proven that 39.6% African users of internet are actually Nigerians, hence, the high increase in the rate of internet crime in Nigeria (Hassan, 2012). Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young ones are mostly involved. Presently, cybercrimes are performed by people of all ages ranging from young to old, but in most instances the young.

In Nigeria, cybercrime has become one of the main avenues for pilfering money and business espionage. According to Check Point, a global network cyber security vendor, as of 2016, Nigeria was ranked 16th highest country in cyber-attacks vulnerabilities in Africa (Ewepu, 2016). Nigerians are known both home and abroad to be rampant perpetrators of cybercrimes. The number of Nigerians caught for duplicitous activities carried by broadcasting stations are much more in comparison to citizens of other countries. The contribution of the internet to the development of Nigeria has had a positive impact on various sectors of the country. However, these sectors such as the banking, e-commerce and educational sector battles with the effect of cybercrimes. More cybercrimes are arising at an alarming rate with each subsequent crime more advanced than its predecessor.

Generally, cybercrime may be divided into one of two types of categories: Crimes that affects computer networks and devices directly. Examples are malicious codes, computing viruses, mal-ware etc. Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer networks or device. Examples include Cyber Stalking, Fraud and identity theft, phishing scams and information warfare.

Types of Threats Caused by Dark Web and Cyber Crimes in Nigeria

Cyber threat can be defined as criminal activities involving an IT infrastructure. Cyber threats in Nigeria started late 1990s, and have continued to escalate in variation and frequency. Efforts to fight cyber threats have involved a growing number of participants including governments, non-governments, public sectors, and non-profit organizations. According to Akinsuyi (2009), threats are categorized into four different forms: attack through email, spam associated threats, malware and phishing. Malware threat was further described to reduce system network. Hence, on the case of threats to email, this disallows employees to have access to the original data of the organization. Phishing threats on the other hand, are in form of hacking of vital information, especially hacking of credit card information or account information. The common types of threats caused by dark web and cyber crimes in Nigeria include:

Phishing: Phishing is simply the theft of an identity. It involves stealing personal information from unsuspecting users and it is also an act of fraud against the authentic, authorised businesses and financial institutions that are victimized (Wada and Odulaja, 2014). Phishing scams are ubiquitous and are exponentially increasing. It has become one of the fastest growing cybercrimes in Nigeria. Fraudsters have devised a means to mimic authorised organisations and retrieve confidential information from clients. In Phishing email messages, the fraudsters find a way to convince and gain the trust of users. In Nigeria, phishing mails are mostly carried out on bank customers.

Cyber-theft/Banking Fraud: Hackers target the vulnerabilities in the security of various bank systems and transfer money from innumerable accounts to theirs. Most cyber-criminals transfer bantam amounts like 5 naira which are sometimes overlooked by the user without questions raised by the users who assumes this was deducted for either SMS or ATM withdrawal charges. Doing this for over a million accounts enriches most fraudsters (Parthiban and Raghavan, 2014).

Cyber-Pornography*:* Cyber-pornography is the act of using cyberspace to create, display, distribute, import, or publish pornography or obscene materials, especially materials depicting children engaged in sexual acts with adults. Cyber-pornography is a criminal offense, classified as causing harm to persons.

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location (Denning, 1999). In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection.

Yahoo Attack: Also called 419, it is characterized by using e-mail addresses obtained from the Internet access points, using e-mail address harvesting applications (web spiders or e-mail extractor). These tools can automatically retrieve e-mail addresses from web pages and send messages to unsuspecting victims defrauding them of their cash.

Credit Card or ATM Fraud: Credit card or ATM numbers can be stolen by hackers when users type the credit card number into the Internet page of the seller for online transaction or when withdrawing money using ATM card. The hackers can abuse this card by impersonating the credit card holder.

Ransomware: This is one of the detestable malware-based attacks. Ransomware enters your computer network and encrypts your files using public-key encryption, and unlike other malware this encryption key remains on the hacker's server. Attacked users are then asked to pay huge ransoms to receive this private key (Choo, 2007).

DDoS attacks: DDoS attacks are used to make an online service unavailable and bring it down, by bombarding or overwhelming it with traffic from multiple locations and sources. Large networks of infected computers, called Botnets are developed by planting malware on the victim computers. The idea is normally to draw attention to the DDOS attack, and allow the hacker to hack into a system. Extortion and blackmail could be the other motivations (Barford and Yegneswaran, 2007).

METHODS

Research Design

A descriptive survey design was used for this study. This was for the purpose of describing the extent and the effect of dark web and cybercrime threats and the extent of mitigation of these treats in Nigeria.

Area of the Study

The research area for this study was Nigeria.

Population of the Study

The population of this study comprised all professionals in computer science, computer engineering and security agents who have been exposed to cyber crimes, cyber security and general computer science.

Sample and Sampling Techniques

A stratified random sampling technique was used to draw the 400 respondents and used for the study.

Instrumentation

The main instrument used in this study was questionnaire titled "*Dark Web and Cybercrime Threat Mitigation Questionnaire (DWCTMQ)"*. The obtained data was coded statistically before the statistical analysis of the data.

Validation of the Instrument

The instrument passed through face and content validated by the experts in computer science as well as test and measurement.

Reliability of the Instrument

Cronbach Alpha technique was used to determine the level of reliability of the instrument. In the trial test, a total of 40 respondents who did not form part of the main study were randomly selected from one of the state not used for the study. The reliability coefficient, obtained was (0.84). This value was considered high enough to justify the use of the instrument.

Method of Data Analysis

The researcher subjected the data generated for this study to appropriate statistical techniques such as percentage analysis, chi-square analysis and regression analysis. The test for significance was done at 0.05 alpha levels.

RESULTS AND DISCUSSIONS

Research Question One

What is the level of dark web and cyber crimes activities in Nigeria? Table 1 was used to answer the research question.

Table 1: Percentage analysis of the level of dark web and cyber crimes activities in Nigeria

Level of dark web and cyber crime activities	Freq	%	Remarks
Very High	241	60.25**	1st**
High	123	30.75	2nd
Low	25	6.25	3rd
Very Low	11	2.75*	4th*
TOTAL	**400**	**100%**	

**** The highest percentage frequency**
***   The least percentage frequency**
Source: Field Survey

The result in Table 1 shows the level of dark web and cyber crimes activities in Nigeria. From the result, it was observed that 60.25% of the respondents affirmed very high level of dark web and cyber crimes activities in Nigeria. 30.75% of the respondents affirmed high level, 6.25% of the respondents affirmed low level and 2.75% of the respondents affirmed very low level of dark web and cyber crimes activities in Nigeria. The result therefore means that there is high level of dark web and cyber crimes activities in Nigeria.

Research Question Two

What are the types of threats caused by dark web and cyber crimes in Nigeria? Table 2 was used to answer the research question.

Table 2: Percentage analysis of the types of threats caused by dark web and cyber crimes in Nigeria

Dark web and cybercrimes threats	**FREQ**	**%**	**Remarks**
Stealing of data	33	8.25	6th
Havoc on individuals and organizations by the criminals	45	11.25	5th
Advanced persistent threats	59	14.75	4th
Distributed denial of service attacks	26	6.5*	7th*
Botnets	62	15.5	3rd
Destructive malware	71	17.75	2nd
The growing challenge of ransom ware	104	26**	1st**
Total	**400**	**100%**	

**** The highest percentage frequency**
***   The least percentage frequency**

From the result of the above table 2, it was observed that the highest types of threats caused by dark web and cyber crimes in Nigeria was “The growing challenge of ransom ware” 104 (26%) while the least one was “Distributed denial of service attacks” 6.5(6.5%).

Hypotheses Testing

Hypothesis One

The null hypothesis states that there is no significant difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria. To test the hypothesis, chi-Square analysis was performed on the data (see table 3).

Table 3: Chi-square analysis of the difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria

----

Level of Dark Web and Cyber Crimes activities	Observed Freq	Expected Freq	X^2
VERY HIGH	241	100	339.56*
HIGH	123	100	
LOW	25	100	
VERY LOW	11	100	
TOTAL	**400**	**400**	

***Significant at 0.05 level; df = 3; Critical = 7.82**

Table 3 shows the calculated X^2-value as (339.56). This value was tested for significance by comparing it with the critical X^2-value (7.82) at 0.05 levels with 3 degree of freedom. The calculated X^2-value (339.56) was greater than the critical X^2-value (7.82). Hence, the result was significant. The result therefore means that there is significant difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria. The significance of the result caused the null hypothesis to be rejected while the alternative one was accepted.

DISCUSSION OF THE FINDINGS

The result of the data analysis in table 3 was significant due to the fact that the calculated X^2-value (339.56) was greater than the critical X^2-value (7.82) at 0.05 level with 3 degree of freedom. The result implies that there is significant difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria. The result therefore was in agreement with the research findings of Akinsuyi (2009) who highlighted that threats are categorized into four different forms: attack through email, spam associated threats, malware and phishing. Malware threat was further described to reduce system network. The significance of the result caused the null hypotheses to be rejected while the alternative one was accepted.

Conclusions

Based on the findings of the research work, it was concluded that there are many cases of dark web and cyber crimes activities in Nigeria. There is high level of dark web and cyber crimes activities in Nigeria. There is significant difference in the perception of people as regards the level of dark web and cyber crimes activities in Nigeria.

Recommendations

The following recommendations are deemed necessary:

1. Cyber security should be seen by all as a shared responsibility which requires the attention of a broad range of stakeholders with effective public/private partnership that incorporates businesses and institutions of all sizes along with national, state, local, tribal and territorial agencies to produce successful outcomes in identifying and addressing threats, vulnerabilities and overall risk in cyberspace.
2. Individual consumers should also have a role of crying out the incidence and threats of dark web to the general public for precaution.
3. Education should be rendered to people on how to better protect themselves from the threat of dark web and cyber crimes.

REFERENCES

Abbasi, A. & Chen, D. (2010) *The Manager's Handbook for Corporate Security:* Establishing and Managing a Successful Assets Protection Program. Butterworth-Heinemann, USA.

Choo, K. R. (2007) "The Cyber Threat Landscape: Challenges and Future Research Directions." *Computers & Security* 30, no. 8 (November 2011): 719–31. doi: 10.1016/j.cose.2011.08.004.

Denning, D. E. (1999). *Information Warfare and Security*, ACM Press, USA.

Ewepu, G. (2016). *Nigeria loses N127bn annually to cyber-crime* — NSA available at: http://www.vanguardngr.com/2016/04/nigeria-loses-n127bn-annually-cybercrime-nsa/Retrieved Jun. 9, 2016.

French, C., Epiphaniou, M. & Maple, H. (2013) *Fighting Cyber Crime in Nigeria.* Retrieved September 10, 2011 from http//www.guide2nigeria,com/news_articles_About_ Nigeria

Gehl, R. W. (2014). *"Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network."* New Media & Society, October 15. http://nms.sagepub.com/content/early/2014/10/16/1461444814554900.full#ref-38.

Hassan, A. B. (2012) Cybercrime in Nigeria: Causes, Effects and the Way Out, ARPN *Journal of Science and Technology*, vol. VOL. 2(7), 626 – 631.

Lakshmi, P. M. (2015), Cyber Crime: Prevention & Detection," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. Vol. 4(3).

Maitanmi, O. S. (2013), Impact of Cyber Crimes on Nigerian Economy, *The International Journal of Engineering and Science (IJES*), Vol. 2 (4), 45–51.

Moore, B. (2005) International Communication Principles, Concepts and Issues. In Okunna,C.S. (ed) Techniques of Mass Communication: A Multi-dimentional Approach. Enugu: New Generation Books.*Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.*

Okeshola, F. B. (2013) The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State*, Nigeria American International Journal of Contemporary Research*, vol. 3(9), 98-114.

Paganini, P. (2012). *The Good and the Bad of the Deep Web*. Security Affairs, September 17.

Parthiban, L. & Raghavan, A. R. (2014), The effect of cybercrime on a Bank's finances*, International Journal of Current Research and Academic Review*, Volume-2(2), no. ISSN: 2347-3215, 173–178, Retrieved Feb. 2014 from www.ijcrar.com

Sui, D. J., Caverlee, D. & Rudesill, X. (2015). *"The Deep Web and the Dark Net."* Accessed August 30, 2016. https://www.wilsoncenter.org/publication/the-deep-web-and-the-darknet.

Tor. (2014) a. *Tor: Overview.* www.torproject.org/about/overview.html.en.

Tor. (2014) b. *Inception.* www.torproject.org/about/torusers.html.en.

Wada, F. & Odulaja, G. O. (2014), Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation, *Afr J Comp & ICT*, Vol 4(3), no. Issue 2.