Strategic Assessment of Risk Mitigation Resources of Dark Web and Cybercrime Threat in Nigeria

BY

EBUTE, Joel U., *Ph.D, MCP, MCSA, MCDBA, MCSE, CCNA, CCNP, CEH, CFI, CSA, CFE,*
Department of Security and Strategic Studies
Institute of Governance and Development Studies
Nasarawa State University, Kefi

ABSTRACT

The study was carried out to strategically assess risk mitigation resources of dark web and cybercrime threat in Nigeria. The population of this study comprised all professionals in computer science, computer engineering and security agents who have been exposed to cybercrimes, 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 cybercrimes activities in Nigeria. It was also observed that the services and websites used in perpetrating dark web and cybercrime threats are Tor, I2P for services and Silk Road, Sheep Marketplace, Black Market, etc. for the websites. The result identified the risk mitigation resources and strategies to disrupt the dark web and cybercrimes threats in Nigeria to be "raising public awareness of the risk and impact of cyber activity and the need to deploy basic protective measures, providing cyber security education on the use of strong passwords, application of system updates in a timely and efficient manner, securing devices by enabling a firewall and deploying solutions to address viruses, malware and spyware; leveraging trusted resources and finally, building an economic framework. 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 along with national, state, local, tribal and territorial agencies to produce successful outcomes in identifying and addressing threats, vulnerabilities and overall risk in cyberspace.

KEYWORDS: Services, websites, dark web, cybercrime, threats, risk mitigation resources, strategies, Nigeria.

Introduction

Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim, 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)". 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 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. 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 paedophilia content, hitman services, conventional and chemical weapons purchase, and illegal medical research.

Statement of Problem

In Nigeria today, several internet 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 threat 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 cybercrime 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 risk mitigation resources of dark web and cybercrime threat in Nigeria.

Objectives of the study

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

1. To determine the services and websites used in perpetrating dark web and cybercrime threats.
2. To identify the risk mitigation resources and strategies which helps in disrupting the dark web and cybercrimes threats in Nigeria.

Research Questions

The following research questions will be answered:

1. What are the services and websites used in perpetrating dark web and cybercrime threats?
2. What are the risk mitigation resources and strategies which helps in disrupting the dark web and cybercrimes threats in Nigeria?

Hypotheses

The following null hypotheses will be tested:

1. There is no significant influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria.

Literature Review

Services and Websites used in Perpetrating Dark Web and Cyber Crime Threats

According to Paganini (2012), the 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. Onion routing is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes, called onion routers. Like someone peeling an onion, each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router, where the process is repeated. This technique prevents intermediary nodes from knowing the origin, destination and contents of the message (Tor, 2014). Websites such as Silk Road act as anonymous marketplaces selling everything from tame items such as books and clothes, to more illicit goods such as drugs and weapons. Aesthetically, these sites appear like any number of shopping websites, with a short description of the goods, and an accompanying photograph (Bartlett, 2014).

The Assassination Market website is a prediction market where a party can place a bet on the date of death of a given individual, and collect a payoff if the date is "guessed" accurately. This incentivizes the assassination of individuals because the assassin, knowing when the action will take place, could profit by making an accurate bet on the time of the subject's death. Because the payoff is for knowing the date rather than performing the action of the assassination, it is

substantially more difficult to assign criminal liability for the assassination (Greenberg, 2013). There are also websites to hire an assassin, popular ones are White Wolves and C'thuthlu (Pocock, 2014). Websites such as Banker & Co. and InstaCard facilitate untraceable financial transactions through various methods. They either launder bitcoins by disguising the true origin of the transactions or give users an anonymous debit card issued by a bank. Users are also given virtual credit cards issued by trusted operators in the dark Web (Dean, 2014). Buying stolen credit card information has never been easier. A website called Atlantic Carding offers this service, and the more you pay, the more you get. Up for grabs are business credit card accounts and even infinite credit card accounts associated with ultra-high-net-worth individuals. The user's details; name, address and so on are available at an additional cost (Dahl, 2014).

The main directory on the dark Web is the Hidden Wiki. It also promotes money laundering services, contract killing, cyber-attacks and restricted chemicals, along with instructions to make explosives. As with other dark Web sites, the links to these sites frequently change to evade detection (Williams, 2011). The Human Experiment was a website that detailed medical experiments claimed to have been performed on homeless people who were usually unregistered citizens. According to the website, they were picked up off the street, experimented on and then usually died. The website has been inactive since 2011 (Falconer, 2012).

Strategies to Help Disrupt the Dark Web and Cyber Crime Threats in Nigeria

Maitanmi (2013) asserts that the collaborative efforts of individuals alongside with government intervention can go a long way in minimising dark web activities and cybercrime to a reasonable level. Measures and strategies to take are:

a) Government intervention: Michael, Boniface and Olumide (2014) assert that there is still need for the nation to come up with adequate laws to tackle this issue. These laws should be formulated by the government and should strictly be adhered to. However, it is worthy to note that a bill was recently passed in year 2015 that would protect and punish electronic fraud and other cyber related crimes. The full implementation of this bill will hopefully bring a strategic approach to fight against cybercrime. Some of the bills are highlighted below:

- There will be seven years' jail term for offenders of different types of computer related fraud, computer related forgery, cyber-pornography, cyber-stalking and cyber-squatting.
- Defines the liability of service providers and ensures that the use of electronic communications does not compromise national interest. It provides a legal framework to punish cyber criminals thereby improving electronic communication.

It specifies all criminal acts and provides guidelines for the investigation of such offences. If these laws are effectively enforced, cybercriminals will be deterred and penalized. This will indirectly reduce the incident of cyber-crimes, increase customer's confidence while transacting business online and also correct the negative impression about Nigeria and the citizens (Michael, Boniface and Olumide, 2014).

b) Individuals on their part should ensure proper security controls and make sure they install the latest security up-dates on their computer systems. In addition, they should observe the following (Lakshmi, 2015):

1. Carefully select the sites you visit. Do not visit an un-trusted site. Avoid visiting a site by clicking on a link you find in your email, found on a Facebook page, or on an advertisement

2. Avoid pirated software and never disclose your Personal Identification Number (PIN), bank account and email access code to unknown persons.

3. Always ignore any e-mail requiring your financial in-formation. Do not send sensitive information in an email since its security cannot be guaranteed.

4. Use strong passwords that are difficult to guess and employ a combination of characters (upper case and lower-case letters), numbers and symbols.

5. Avoid inputting your information in a pop-up. If you have interest in any offer you see on a pop up, it is always safer to go directly to the website of the retailer.

c) Raising awareness

A comprehensive and sustained national cyber security education campaign is essential for raising public awareness of the risk and impact of cyber activity and the need to deploy basic protective measures on desktops, laptops, tablets, phones and other mobile devices. The explosion of connected devices, from smart refrigerators, lighting systems, heating and air conditioning, security services to autonomous automobiles, puts an exclamation point behind the importance of cyber protection for individual users and organizations of all sizes and levels of sophistication (Hoffman, 2014). Cyber security education should cover the basics:

- Apply system updates in a timely and efficient manner.

- Secure devices by enabling a firewall and deploy solutions to address viruses, malware and spyware.

- Learn not to click on email links or attachments, unless the sender is known and trusted. Even then, phishing emails sometimes spoof the sender's identity to trick the user into clicking a link or attachment.

d) Leveraging trusted resources

Additionally, building, maintaining, scaling and updating an online source of information on how users of all levels of sophistication can establish and improve their protection profiles in cyberspace is imperative.

e) Building an economic framework

Grabosky and Peter (2001) assert that by simply purchasing every new tool or security product is not the answer. From the individual user to the small business to the large enterprise, it is important to make investment decisions for cyber security in a risk management construct that includes trying to secure the biggest bang for the buck.

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 cybercrimes, 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 questionnaire was made up two sections, (sections A and B). Section A was used to collect information on personal data of the respondents while section B of the questionnaire was made up of two variables such as dark web and cybercrimes activities; threats of dark web and cybercrimes; services and websites used in perpetrating dark web and cybercrime threats and finally risk mitigation resources and strategies to disrupt the dark web and cybercrimes threats. 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

Research Question One: The research question sort to find out the services and websites used in perpetrating dark web and cybercrime threats. In order to answer the question, percentage analysis was used. (See table 1).

Table 1: Percentage analysis of the services and websites used in perpetrating dark web and cybercrime threats

Services and websites used for dark web and cyber crime threats	FREQ	%	Remark
Tor	56	14	4th
I2P	35	8.75	5th*
Silk Road	67	16.75	3rd

Sheep Marketplace	117	29.25	2nd
Black Market	125	31.25	1st**
Total	**400**	**100%**	

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

From the result of the above table 1, It was observed that the highest services and websites used in perpetrating dark web and cybercrime threats was "Black Market" 125(31.25%) while the lowest services and websites used in perpetrating dark web and cybercrime threats was "I2P" 35 (8.75%).

Research Question Two: The research question sort to find out the risk mitigation resources and strategies which help in disrupting the dark web and cybercrimes threats in Nigeria. In order to answer the question, percentage analysis was used, (See table 2).

Table 2: Percentage analysis of the mitigation resources and strategies which help in disrupting the dark web and cybercrimes threats in Nigeria

Risk Mitigating Resources/Strategies	FREQ	%	Remark
Raising public awareness of the risk and impact of cyber activity and the need to deploy basic protective measures	104	26	1st**
Provision of cyber security education on the use of strong passwords	99	24.75	2nd
Application of system updates in a timely and efficient manner	78	19.5	3rd
Securing devices by enabling a firewall and deploying solutions to address viruses, malware and spyware	65	16.25	4th
Leveraging trusted resources	23	5.75	6th*
Building an economic framework	31	7.75	5th
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 risk mitigation resource and strategy which help in disrupting the dark web and cybercrimes threats in Nigeria was "Raising public awareness of the risk and impact of cyber activity and the need to deploy basic protective measures" 104(26%) while the lowest risk mitigation resource and strategy which helps in disrupting the dark web and cybercrimes threats in Nigeria was "Leveraging trusted resources" 23(5.75%).

Hypotheses Testing

Hypothesis 1: The null hypothesis states that there is no significant influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria. In order to test the hypothesis regression analysis was performed on the data, (see table 3).

TABLE 3: Regression Analysis of the influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria.

Model	R	R-Square	Adjusted R Square	Std. error of the Estimate	R Square Change
1	0.96a	0.92	0.92	0.65	0.92

***Significant at 0.05 level; df= 398; N= 400; critical R-value = 0.098**

The table shows that the calculated R-value 0.96 was greater than the critical R-value of 0.098 at 0.5 alpha level with 398 degree of freedom. The R-Square value of 0.92 predicts 92% of the influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria. This rate of percentage is highly positive and therefore means that there is significant influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria.

Discussion of the Findings

The result of the data analysis in table 3 was significant due to the fact that the calculated R-value 0.96 was greater than the critical R-value of 0.98 at 0.05 level with 398 degree of freedom. The result implies that there is significant influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria. The result therefore was in agreement with the research findings of Maitanmi (2013) who asserts that the collaborative efforts of individuals alongside with government intervention can go a long way in minimising dark web activities and cybercrime to a reasonable level. 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 various services and websites used in perpetrating dark web and cybercrime threats and there are various risk mitigation resources and strategies against dark web and cybercrime threats in Nigeria. There is significant influence of risk mitigation resources and strategies on the level of dark web and cybercrime threats in Nigeria.

Recommendations

The following recommendations are deemed necessary:

1. Education should be rendered to people on how to better protect themselves from the threat of dark web and cybercrimes.

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. 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.

REFERENCES

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

Akinsuyi, J. (2009). *The drawing of Information Security Legislations*, What Nigerian Corporations Can Do to Prepare.

Barford, D. & Yegneswaran, F. (2007) Transforming the weakest link a human computer interaction approach to usable and effective security. *BT technology, Journal 19*(3): 122-131.

Bartlett, J. (2014). *Dark Net Markets: The eBay of Drug Dealing*, The Observer, October 5.

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.

Colbaugh, M. & Glass, G. (2012) Social Change and Crime Rate Trends: A Routine Activity Approach », *American Sociological Review*, 44 (4), 1979, pp. 588-608.

Dahl, J. (2014). "Identity Theft Ensnares Millions while the Law Plays Catch Up." *CBS News*, July 14.

Dean, M. (2014). "*Digital Currencies Fueling Crime on the Dark Side of the Internet.*" *Fox Business*, December 18.

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.

Falconer, J. (2012). "A Journey into the Dark Corners of the Deep Web." *The Next Web*, October 8.

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.

Grabosky, L. & Peter, B. (2001). "Virtual Criminality: Old Wine in New Bottles?" *Social & Legal Studies* 10: 243–49. http://sls.sagepub.com/content/10/2/243.full.pdf.

Greenberg, A. (2013). *"Meet the 'Assassination Market' Creator Who's Crowdfunding Murder with Bitcoins."* Forbes, November 18.

Halder, D. & Jaishankar, K. (2011) "*Cybercrime and the Victimization of Women: Laws, Rights, and Regulations".* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

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.

Hoffman, R. (2014) *Practical Application of Cyber Crime* Issues Retrieved on May 6, 2016 available at: http://ijma3.org/Admin/Additionals/Cybercrime/Nibal%20Idlebi%20-Presenta-tion.pdf

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

Mac, R. (2014). "Feds Shutter Illegal Drug Marketplace Silk Road 2.0, Arrest 26-Year-Old San Francisco Programmer." *Forbes*, November 6.

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

Michael. A., Boniface, A. & Olumide, A. (2014) Mitigating Cybercrime and Online Social Networks Threats in Nigeria, *Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz*, vol. Vol I WCECS 2014, 22–24.

Moar, J. (2015) *The Future of Cybercrime & Security: Financial & Corporate Threats & Mitigation 2015–2020*, Juniper Research, www.juniperresearch.com/ researchstore /strategy-competition/cybercrime-security/financial-corporate-threats-mitigation.

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

Pocock, Z. (2014). "How to Navigate the Deep Web." *Critic*, Issue 03, March 19.

Shandilya, A. (2011) *Online Banking: Security Issues for Online payment*, from www.buzzle.com/articles.

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.