Cyber-Attack as a Menace to Effective Governance in Nigeria

Oluyemi Fayomi, Oly Nelson Ndubisi, Charles Ayo, Felix Chidozie, Lady Ajayi and Uchechukwu Okorie
Covenant University, Ota, Ogun State, Nigeria
nike.fayomi@covenantuniversity.edu.ng
olynel@hotmail.com
charles.ayo@covenantuniversity.edu.ng
felix.chidozie@covenantuniversity.edu.ng
adaina.yartey@covenantuniversity.edu.ng
ucheson4excel@yahoo.com

Abstract: Cyber-attack is an attempt by hackers to damage or destroy a computer network or system for purposes of mischief, fraud, and/or hedonism. To say that the incidences of cyber-attack are increasing rapidly in Nigeria is not only an understatement but also a cliché. From the organized private sector to public service, hackers have not spared any entity. More recently, governments in both developed and developing countries have had to deal with this menace on a frequent basis. The government of Nigeria is not an exception the thorn in the flesh. Indeed some government officials have blamed ineffective governance on the menace of cyber-attack, thereby creating the impetus for this research. The study therefore investigates the incidences of cyber-attack in Nigeria and its impact on democratic governance. The study was based on descriptive and explorative research design. This involves the use of research instrument administered to retrieve vital information from the target audience. The information gathered were coded into scale variables that support empirical investigation of the subject matter. In this study a total of 150 questionnaires from which a total of 126 were retrieved and used for the analysis. The data analysis utilized frequency distribution involving percentage and factor analysis. This method is frequently used in the Social Sciences research. Both factor analysis and relational analysis were applied. Factor analysis establishes the most prominent factor responsible for cyber-attacks motivation while the relational analysis was further utilized in examining the determined effect of incidence and nature of cyber-attacks on the assessment of the effectiveness governance in Nigeria. The evidence from the study provides significant result in support of a significant influence of cyber-attack menace on the perception of governance. Analysis of the motivating factors suggests that financial benefits and wide spread dissemination of the virus accounted for most factor responsible for the attacks. The study therefore recommends that government and law enforcement agencies should strategize on means of providing a more comprehensive data base to facilitate effective investigation and further research in this area.

Keywords: cyber attack, governance, e-governance, factor analysis, Nigeria

1. Introduction

Cyber-attack is often described as a crime that has some form of computer or cyber facet to it. The phenomenon is constitutes a bigger risk recently than before due to the precipitous number of connected people and devices. The distinguishing features of cyber-attack are: Cyber-attack crime has now surpassed illegal drug trafficking as a criminal moneymaker; an identity of an individual is stolen every 3 seconds as a result of cyber- attack; without a sophisticated security package, unprotected PC can become infected within four minutes of connecting to the Internet.Perpetuators of cyber-attack use a number of methods, depending on their skill-set and their goals. These include theft of personal data, copyright infringement, fraud, child pornography, cyber stalking, bullying. It should be noted that cyber-attack covers a wide range of different attacks, that all deserve their own unique approach when it comes to improving the computer's safety and protecting the users and the citizens as a whole. In Nigeria, the survey led by Gantz (2013) reveals that perpetuators of cyber-attacks entrench or implant counterfeit software with dangerous malware as a new technique of preying on computer users who are unaware of the potential danger. Therefore, more danger awaits the computers of those acquire counterfeit and pirated software.The Internet has facilitated dramatic increases in worldwide interconnectivity and communication. This form of globalization has yielded benefits, such as improved standards of living in the developing world, but it has also given rise to new weapons of resistance for groups seeking to oppose certain political measures and ideologies**.** Hence**,** for a proper understanding of the study, this paper will be focusing on the following objectives;

- To identify whether there is a significant link between incidences of cyber-attacks and the assessment of effective governance in Nigeria and
- Secondly this study intends to examine the influence of variant cyber-attacks on perception of governance performance in Nigeria.

1.1 Conceptual clarifications:

The concepts that are germane and will be discussed in this article include Cyber-attack and Governance.

Cyber-attack: It has been observed that the concepts cyber-attack and cyber-terrorism are used by scholars have most times interchangeably to mean the same thing (Ristucci and Baich, 2012). But in actual sense the two concepts are different. Therefore, it is necessary to demystify the concepts cyber-attack and cyber terrorism.

McEachern (2011) defines cyber terrorism as:

> *a computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism. Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples. . . . Attacks that disrupt nonessential services or that are mainly a costly nuisance would not [be cyber terrorism].*

McEachern (2011) describes Cyber-attack as an umbrella term for several types of cyber-related activities, each of which has different motivating factors. For example Hacking, is a cyber-attack motivated by political activism that often involves ruining a website for the explicit purpose of publicly shaming the target. Cyber-crime may involve using cyber-attack as a means, but its sole motivation is to gain financially from the attack (i.e., using a cyber-attack to steal credit card information); and Cyber-espionage involves an individual or team using various cyber-attack methods to capture sensitive foreign government information and plans, backed by a foreign state, and done by an individual or team. All of these forms of cyber-attacks are performed by what has been known popularly since the 1980s as a computer hacker or hackers. Originally, hacker was used as a term of compliment and egotism among individuals who were interested in programming, and has origins as early as the 1970s at the Massachusetts Institute of Technology, but has since that time come to be better known to represent malicious individuals who break into computer systems by effecting their information with countless tools (Lachow, 1999).

Karnouskos (2014) defines Cyber-attack;

> *as any type of belligerent scheme employed by individuals, organizations and countries that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.*

Also, the U.S. National Research Council (cited in Shackelford, 2013) defines;

> *Cyber-attacks as deliberate actions to alter degrade, deceive, disrupt, or destroy computer networks or systems or the information and/or programs resident in or transiting these networks or systems.*

On the other hand, Shackelford (2013) observes that Cyber-attack is often broken into four main categories namely; espionage, criminal activity, cyber warfare and terrorism. This she disagrees with. She opines that cyber-attacks should not be categorized in this manner; motivations can overlap and targets abound in cyberspace. For example, there has been a spate of high-profile cases of cyber-crime and espionage, as well as alleged state-sponsored cyber- attacks involving criminal organizations and terrorist groups targeting both private and public sectors. Cyber- attacks against states in particular are on the increase. Examples of such attacks can be seen in Estonia in 2007, Georgia in 2008, Iran in 2010, and South Korea in 2013 (Herzog, 2011).These attacks could be said to emanate from foreign rivals in pursuit of exclusive data or hackers demand in revenge or looking for profitable loopholes, or even terrorists anticipating to cause economic havoc and also distort political activities (Brenner, 2013).

Hathaway, Crootof, Levitz, Nix, Nowlan, Perdue and Spiegel (2012) defines a cyber-attack as consisting of any action taken to undermine the functions of a computer system or network for political or national security or hinder the effective governance of any country. Imbedded in this definition is the prerequisite that the conduct must be active: either offense or active defense. Active defense includes “electronic counter-measures designed to strike attacking computer systems and shut down cyber-attacks midstream.”This

definition says that cyber-attack "consists of any action taken". Such actions include hacking, bombing, cutting, infecting, et cetera. But the objective can only be to undermine or disrupt the function of a computer system or network in explaining the phrase, to undermine the function" in the definition. It is certain that the main objective of a cyber-attack must be to undermine the function of a computer network. A computer network may be compromised indifferent ways. Syntactic attacks disrupt a computer's operating system, causing the network to malfunction. Examples of such include viruses, worms, Trojan horses and denial of service attacks.Cyber-attacks are becoming widespread and constantly under attacks are organizations, institutions and countries. Despite the intrusion detection systems (IDS), firewalls (FW), evasion prevention systems (EPS), network patches, anti-virus applications, fuzzers, and other penetration detection tools available in the cyber security marketplace (Udo-Akang,, 2014). It is a posing a serious threat to effective governance and national security of most countries. It has a global origin and every organization or country is a potential target.

Governance: Fukuyama (2013) defines governance as a government's ability to make and enforce rules and to deliver services, regardless of whether that government is democratic or not. It is about the performance of agents in carrying out the wishes of principals, and not about the goals that principals set.

Marc (2011) relates governance to the processes of interaction and decision-making among the actors involved in a collective problem that lead to the creation, reinforcement, or reproduction of social norms and institutions.

Effective Governance in Nigeria: For governance to be termed effective or good it should have attained the following; equity, justice, enhanced participation of citizens, protection of life and property, respect of the rule of law and improved living standard of the populace, responsiveness, a strong civil society, free press, social sanction and reward system, efficient systems and structures. Thus, Anyadike and Emeh (2014) define governance as that process employed to achieve the noble end of the state.

It is an obvious datum that despite Nigeria's vast resources and huge potentialities, she remains grossly undeveloped as abject poverty, acute youth unemployment; heightened crime rate, poor health prospects and widespread malnourishment have been the main features of Nigeria's political economy (Ogundiya 2010 cited in Anyadike and Emeh, 2014). Hence, the problem of development in Nigeria is a problem of governance; especially when defined in terms of the proper, fair and equitable allocation of resources for the achievement of the ends of the state, which is the promotion of the common good of the people. Not to mention most importantly the fact that, Nigeria has been categorized among countries practicing all manners of online fraud such as hacking, fraudulent transactions via the internet, theft of credit cards among others, although, this categorization does not augur well with the country. But irrespective of that, the practice continues unrelenting and the individuals involved are catching fun, as there seems to be no law guiding against cyber-attacks in the country.

Dickson (2012)affirms that one fundamental thing Nigeria lacks in governance and government is the word "good" even when many Nigerians have identified good governance as the sine qua non for peace, progress, and stability, free and fair elections. In fact it is viewed as the only passport to delivering the dividends of democracy. For the nation to work, we need good governance. In order to maximize our potentials, improve the general welfare of the Nigerian people and even development in geo-political terms, there must be good governance. Until good governance is viewed as the process of decision-making and the process by which decisions are implemented, we are still far off simply because the way and manner public persons deal with public institutions, conduct public affairs, manage public resources, are questionable, corrupt, and without due regard for the good of the people.

1.2 Review cyber-attacks on governance in some selected countries

Cyber-attacks have been widely acknowledged as computer-to-computer attacks undermining the confidentiality, integrity, and /or availability of computers and/or the information they hold (Hathaway et al, 2012). The importance of securing cyberspace is increasing, along with the sophistication and potential significance of the results of the attacks. Moreover, attacks involve increasingly sophisticated coordination among multiple hackers across international boundaries, where the aim has shifted from fun and self-satisfaction to financial or military gain, with clear and self-reinforcing motivation (Kim et al, 2012:66). Indeed, cyber-attacks on states have in recent time proliferated both in numbers and severity. While incidences of

cyber-attacks in developed countries are well documented, very little research appears to be available about developing countries.

1.3 State of Estonia

Estonia was attacked in April 27, 2007 in what has come be recognized as the world's first cyber-attack that threatened the national security of an entire state. In a matter of hours, the Web sites of Estonia's leading banks and newspapers crashed. Government communications were compromised. The attack was reported to have originated from thousands of zombie private computers around the world (Shackelford, 2010). In essence, the persistent attacks involved computer robot networks, known as botnets that seized more than a million computers from 75 countries and directed them to barrage targets in Estonia (Beidleman, 2011:57).

Beidleman (2011) further argued that the majority of the attacks came in the form of distributed denial of service (DDOS) attacks that overwhelmed websites with a massive number of requests for information and crippled the underlying network of routers and servers. Despite efforts by government of Estonia to seek international support, especially from advanced countries of Russia and United States to combat the scourge, it nonetheless proved futile. The incident robbed the country of a huge slice of its national income before it was resolved.

1.4 The State of Belarus

The state of Belarus experienced a series of cyber-attacks in April, 2008 when the website of Radio Free Europe/Radio Liberty's Belarus service became a target of a Distributed Denial of Service (DDOS) attack. Corporative Cyber Defense Centre of Excellence (CCDCOE, 2010) argued that service of the radio station was inundated with about 50,000 fake pings every second, which the organization reported as unprecedented in the history of cyber assaults against them. It was also reported by the agency that in a few hours following the commencement of the DDOS attack against the Belarus Service, seven other RFE/RL websites in the Eastern European and Central Asian/Middle East region (Kosovo, Azerbaijan, Tatar-Bashkir (ethnic regions within the Russian Federation), Radio Farda in Iran, South Slavic, and Tajik) were also affected. The attack was reported to have lasted for two days and caused incalculable damage to the Belarus government.

1.5 The Lithuanian State

Following the passage of the amendment of the law and its condemnation by the Russian Federation, on June 2008, cyber-attacks against Lithuanian websites began. According to the report released by the Lithuanian embassy cited in (CCD COE, 2010), the main type of the attack was defacement of websites and some e-mail spam. It furthermore noted that the original content of nearly 300 websites was replaced with communist images on a red background portraying the flag of the Soviet Union. According to the Lithuanian Computer Emergency Response Team (CERT-LT, cited in CCD COE, 2010), the majority of the attacked Web sites were hosted on a single Hostex Web server, which had a vulnerability either in the Web server software or the Linux operating system. CERT-LT further reported that the hackers launched the attack against all that was accessible in Hostex' Servers with no specific regard to any particular website. CERT-LT has estimated that about 95% of the sites that were hit belonged to private sector organizations, since the public sector largely avoided the damage due to early warning.

1.6 The State of South Africa

The South African Consumer Union (SACU) had in 2003 drawn the attention of the South African government to the urgent need to protect their clients against Internet Banking Fraud. According to Herselman and Warren (2010) hackers defaced more than 60 South African web sites in 2003. They contended that the incident was a new daily record and significantly higher than the previous record of 52 web sites defaces in one 24-hour period. They reported that on 20 July 2013, a hacker cleaned out a number of ABSA bank accounts, noting that the hacker used spyware to obtain usernames and passwords, essentially engaging in identity theft in siphoning off funds from unsuspecting users.

Similarly, The Cape Times, (cited in Herselman and Warren 2010), had in June 2003 reported that the African Bank website was hacked onto by an unknown party. According to the report, the "7up hacker" had invaded their website and defaced the site. 7up removed all the content from the bank's home page and left a

damaging message. Consequently, 7up hacked into more than 52 South African websites – mostly in the Western Cape – in less than 18 hours; however, there is no evidence to suggest that the hacker gained access to bank accounts.

Furthermore, South African universities have come under cyber-attack in the past. On July 2, the IT Services website at the University of Cape Town was defaced by hackers. Before that, the University of Natal fell prey to attacks on May 21 and August 20. The University of the North was hacked on April 18, UCT on April 18 and the Medical University of South Africa on October 20, 2002 (Herselman and Warren, 2010).

1.7 The Nigerian State

Cyber-attacks committed in Nigeria are more than any other country in Africa. World ranking in cyber-attack indicate that Nigeria is on top of the list after United States and Britain but first in Sub-Saharan Africa (Chiroma et al, 2011:7). Documented cases of cyber-attacks most prevalent in Nigeria include yahoo attack, hacking, software piracy, pornography, credit card or ATM fraud, denial of service attack, internet relay chat (IRC) crime, virus dissemination, phishing, cyber plagiarism, spoofing, cyber stalking, cyber defamation, salami attack and cyber terrorism (Olusola et al, 2013). Indeed, Nigeria which boasts of a 29% internet penetration rate, 40 million internet users as at 2013 and projected 70 million users in 2015, the highest in Africa, has suffered for years from cyber related crimes (The Guardian Nigeria, 2013). According to Isaac (cited in the Guardian Nigeria, 2013), Nigeria as a fast emerging market risks higher foreign invasion of cyber-attacks because of the glut in capacity utilization. It is this influx of foreign investors into the country and opportunities that result from such that puts the country on the international sport light in contemporary cyber related crimes.

In 2011, a group of Nigerian hackers known as Niger Cyber Hacktivists attacked government sites including the National Poverty Eradication Programme website and the Niger Delta Development Commission, posting a letter protesting against the N1b ($6.6m) cost of inauguration for President Goodluck Jonathan and the country's Freedom of Information Act. In a similar attack in January 2013, the Economic and Financial Crime Commission (EFCC) was attacked in response to reports of corruption (IDG Connect 2013). It is on this score that I T News Africa estimated the sum of $200 million as the annual cost of cyber-attacks to the Nigerian economy.

According to another report released by the International Data Group (IDG, 2013), the world's largest technology media company, for years Nigeria has been the leading country in spam, with promises of Nigerian Princes offering millions for only small advance fee. It argued that these 419 Scams are so synonymous with the country they are often called Nigerian scams. IDG further reported that back in 2005, Lagos state in South West Nigeria was widely considered the world's leading place for scam crimes. It is important to note that although scam crimes are still common in Lagos state, they have been on the decline of late because the Nigerian Police have been more active in recent years in shutting down these kinds of operations.Perhaps what can be attributed to the persistence of cyber-attacks in Nigeria is the twin factor of the exponential growth in mobile telecommunication users and the rise in social networking – potential sources of globalization - especially among the teeming mass of unemployed youths in Nigeria. According to Akwule (2011), increasingly more cyber-attacks are perpetrated through mobile phones and social networks such as face book, twitter etc. He averred that Nigerian government is demonstrating increased awareness of cyber security issues, but existing capability to deter, monitor, or pursue cyber security is relatively low due to the forces of globalization. He submitted that the African Union is cooperating with other international agencies to arrive at harmonized legal framework that will be suitable to arrest the scourge of cyber-attacks in African countries.

1.8 Research hypotheses

The following statements were hypothesized and tested in the course of this study;

Hypothesis I

H_1: There exists a significant linkage between incidences of cyber-attacks and the assessment of effective governance in Nigeria

H_0: There exists no significant linkage between incidences of cyber-attacks and the assessment of effective governance in Nigeria

Hypothesis II

H_1: The variant cyber-attacks has a significant influence on the perception of governance performance in Nigeria

H_0: The variant cyber-attacks has no significant influence on the perception of governance performance in Nigeria

1.9 Research methodology

Research Design: The exploratory and survey research design were utilized in this study. The survey research design provides the bases for method enquiry and information gathering that cuts across different target audience at a point in time. The exploratory design offers the researcher opportunity to gain more insight into the nature and occurrences of cyber-attack as well as it relationship with the perception and assessment of effective governance in Nigeria. In addition explorative research design enables the researcher to have a better understanding of a situation that is not quit clear and thus has not attracted serious investigation and research in the past, (Asika, 2004).

The analytical techniques were regression and descriptive method of data analysis.

Sample and sampling procedure: The population consists of experts in information and communication network systems in Covenant University, Bells University of Science and Technology cyber Café, internet users, and three major cyber-domains within the two Universities. A sample size of 150 was randomly selected from a targeted population of 250. The target audience was drawn randomly from the different schools. The simple random technique is basic sampling approach that gives opportunity for equal representation and selection of subjects. The sampling procedure was done in such a manner that will include all categories of inter users cutting across the institutions considered. This was to provide necessary variety of information needed for this study.

Target audience: A total of 150 copies were administered while filling of the responses was personally supervised by the researchers from which 126 copies dully filled were retrieved and utilized for this analysis. The response rate was 0.84 percent was recorded from the returned questionnaires. The responses were coded into scale variables that are measurable using a five point likertscale; Very high, High, Moderate, Low and Minimal. The coded responses were subjected to both descriptive and regression analyses that enable the study reach a conclusion.

Research Instrument: The research instrument employed was a well structured questionnaire. The subjects were administered the questionnaire at their respective place of work. The administered instrument contained the instruction on how filling the questionnaire. The respondents assured of the confidentiality of the information provided in the instrument. In developing the research instrument, it was divided into two parts; part A and B. The first part focuses on the demographic information of the subjects. Part B is sub divided into five Sections I-V rated on a 5-1 point scale (Very High – Minimal) with a total of 37 items measured. Section I relates to the outcomes related to types of attacks, section II measures the incidences of a the attacks, section III deals with potential sources of attacks, in section IV, we considered the motivating factors while section V relates to assessment and perception of governance performance. The questions used in this study were gathered from literature and adapted for the current research.

Validity and Reliability: In ascertaining the validity of the research instrument, face and content validities were established from the management professionals and experts in the centre for system and information services (CSIS) department. The CSIS department is responsible for internet security and communication services. The reliability was tested with Cronbach alpha statistic 0.934 with a total of 37 items tested in which the instrument was highly reliable.

Research Model: The analytical frame work for this study was adapted from the cyber incident analytical model approach by Mugavero and Sabato (2014). This present study model measures the relational effects of the outcomes related to types of cyber crime on the assessment and perception of effective governance in Nigeria. The researchers have drawn the constructs for model from the outcomes of related to types of attacks by Vatis (2001). In the research model the explained constructs measured the assessment and perception of

effective governance while the explanatory constructs measured the severity of the outcomes related to the types of threats associated with cyber-crime. In structuring the research instrument, the explanatory constructs were measured as the outcomes (includes; websites defacements, distributed denial of service attacks, internet relay crime, virus and Trojan dissemination effects unauthorized intrusion, attacks and system penetration) of threats and attacks rated on a five point likert scale (Very High, High Moderate, Low and Minimal effects) based on the severity of their effects. The explained construct was measured with the individual assessment and perception of effective governance (in terms of institutional public affairs management, enhanced citizen's participation, sanction and reward system and protection of life and property). However, it is pertinent to note here that only the threats with significant relations with the assessment and perception of effective governance were reported in the case of social sanction and reward system in section IV.

1.10 Data analysis and results

The responses from the survey provided the framework for the analysis. The research instrument was structured into two main parts. The first part deals with the information that relates to the demographic characteristics of the respondents while the second part was intended to ascertain valid information patterning to cyber-attacks and effective governance.

- **Demographic information of the respondents**

Table 1: Age

		Frequency	Percent	Valid Percent	Cumulative Percent
	15-25 years	100	79.4	79.4	79.4
	Between 26-35 years	23	18.3	18.3	97.6
	36-45 years	3	2.4	2.4	100.0
	Total	126	100.0	100.0	

Source; Authors' Survey, 2015

The analysis of table 1 shows the demographic statistics of the respondents who participated in the survey study. It further reveals that of the total respondents 100 which represents 79.4% were between the age bracket of 15-25 years, 23 (18.3%) were between 26-35 years while only 3(2.4 %) were within the age 36-45 age boundaries.

Table 2: Education

		Frequency	Percent	Valid Percent	Cumulative Percent
	None	8	6.3	6.3	6.3
	Primary school leaving certificate	14	11.1	11.1	17.5
	WAEC/NECO	67	53.2	53.2	70.6
	B.Sc./OND	28	22.2	22.2	92.9
	Above B.Sc.	6	4.8	4.8	97.6
	Professional certificate	3	2.4	2.4	100.0
	Total	126	100.0	100.0	

Source; Authors' Survey, 2015

The educational background (table3) of the respondents shows that 8(6.3) had no formal education, 14(11.1%) had primary school leaving certificate, the majority of the respondents were WAEC/NECO holders, 28(22.2%) were B.sc./OND holders, 6(4.8%) had additional qualification beyond B.Sc. while 3 had other professional certificates in their own fields.

Table 3: Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
	Petty Trading	8	6.3	6.3	6.3
	Farming	9	7.1	7.1	13.5
	Skilled Worker	45	35.7	35.7	49.2
	Cyber Operators	64	50.8	50.8	100.0
	Total	126	100.0	100.0	

Source; Authors' Survey, 2015

The occupational distribution of the respondents in table 5 suggests that 8 representing 6.3% of the total respondents were petty traders, 9(7.1%) were farmers; most of the respondents were skilled workers and cyber operators 64(50.8%).

Source; Authors' Survey, 2015

Figure 1: Nature of attacks

In figure 1 above, a large proportion of the respondents (37.30%) observed that the incidence of cyber-attack occurrences in recent time has moderated while (35.71%) also on the high side based on daily occurrences as shown in figure 1 above.

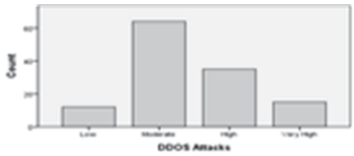

Figure 2: Distributed denials of service attacks

In figure 2, it could be observed that majority (64(50.8%) of the respondents are of the opinion that there is a moderate occurrences of the distributed denial of services attacks on their cyber networks, 35(27.8%) confirm that the attacks has been high in recent times while 15(11.9%) believed that it has been on a very high rate compared to previous incidences.

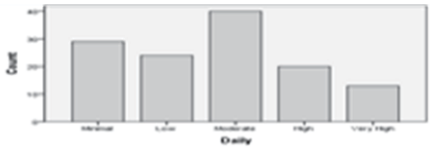

Figure 3: Incidences of attacks on daily basis

As shown in figure3, the greatest proportion of the respondents (31.7%) observed that the incidence of cyber-attack occurrences in recent time has moderated while some (15.9%) also affirmed it is on the high side based on daily occurrences as shown in figure 1 above.

1.11 Discussion of results

The analysis of the regression models for governance assessment, nature and incidence of attacks shows that estimated results are statistically significant at 1 percent given the analysis of variance result of 15.685 for governance perception and nature of attacks and 26.985 for governance perception and incidences of attacks. This further suggests the empirical results are free from spurious effects and reliable for useful policy recommendations. The evidences from the co efficient result of the determined effect of nature of attacks (NOA) and incidences of attacks (INCD) reveals that the frequency of cyber-attacks occurrences (0.423) has more determined effect on governance than the nature of the attack (0.335). This implies that the frequent occurrences of cyber-attacks in its variant forms and corresponding impact such as defacement of public and privates websites, Trojan horses and virus dissemination and unauthorized intrusion effects poses a great threat on governance in Nigeria as revealed by this current study. On the contrary it could deduced from the study that some attacks such as distributed denial of services (DDOS) attacks, internet relay crime (IRC) attack and system penetration have not so dominant compared defacement of public and privates websites, Trojan horses and virus dissemination and unauthorized intrusion effects However, the evidence from principal components analysis suggest that financial benefits and the wide spread dissemination of virus and Trojan effects constitutes the most prominent motivating factor for cyber-attack menace to effective governance in

Nigeria among other motivational factors as exploring break through challenges and development of new destructive exploits scripts.

1.12 Policy recommendations

Empirical evidences from this study reveal that the nature of occurrences and incidences of attacks poses the greatest menace to effective governance in Nigeria. This study thus recommends for the establishment of institutional framework to curb the proliferation of cyber-attack. This can be done by monitoring the various forms and nature of attacks so as to come up with appropriate counter-attack as well as preventive measures as a pro-active strategy to be implemented , considering the vulnerable targets cites and domains.

Finally, this study recommends for a concerted effort by the Nigerian government, law enforcement and security agencies to build and maintain a robust record of reliable data and documented reports of cyber-attack activities as this will provide useful information and necessary data required for effective study and research and investigation on this area as paucity of data and reliable source of information could pose a significant challenge to scientific research in this areas especially for developing economies like Nigeria.

2. Conclusion

It is obvious that the proliferation of internet and websites operations has brought an unprecedented innovation and development in different aspects of Nigerian development. It has significantly increased business networking and communication channels that have enhanced globalization and faster dissemination of ideas in different human endeavors. However, the complexities and negative outcomes associated with this recent development in internet and websites activities have remained a threat to internet users, cyber domains and in general administration of effective governance. Consequently this has implications on the assessment and perception of credible governance among the populace and its role in curbing this menace that have lingered over the time

References

Akwule, R (2011) “The Realities and Challenges of Cyber Crime and Cyber Security in Africa” Being a paper presented at the workshop on Cyber Security and Global Affairs held in DBH, Budapest, Hungary. May 31 to June 2

Anyadike, N. O and Emeh, I. E.J (2014) Effective Leadership for Good Governance in Nigeria; Addressing the Interface, *IOSR Journal of Humanities and Social Science (IOSR-JHSS*)19(1), 69-74.e-ISSN: 2279-0837, p-ISSN: 2279-0845.

Asika, N. (2004) *Research methodology A process approach*, Lagos: Mukugamu& Brothers Enterprises.

Avatis. M.A (2001), Cyber-Attacks during the War on Terrorism: A Predictive Analysis. Institute for Security Technology Studies, Dartmouth College.

Beidleman, S. (2011) “Defining and Deterring Cyber War”. Military Technology – MIL TECH-11, Pp. 57-62

Brenner, J.F (2013)Eyes wide shut: The growing threat of cyber-attacks on industrial control systems. Bulletin of the Atomic Scientists, 69(5) 15–20.

CCD COE (2010) “International Cyber Incidents: Legal Considerations

Chiroma, H., Abdulhamid, S.M., Ya’aGital, A., Usman, A.M and Maigari, T.U (2011) “Academic Community Cyber Cafes: A Perpetration Point for Cyber Crimes in Nigeria”. International Journal of Information Sciences and Computer Engineering, Vol. 2, No.2 pp. 7-13

Dickson, C., (2011) Good Governance in Nigeria: The Tuwo and Soup Metaphor- Retrieved on 8th January, 2014 from http://saharareporters.com.

Fukuyama, F. (2013) What is Governance? Centre for Global Development.Working Paper Series 314.

Gantz, J. (2013)One in Three PCs Risks Cyber-Attack in 2013, Punch Newspapers, Lagos, March 7, p. 14.

Hathaway, O.A., Crootof, R., Perdue, W and Levitz, P (2012) “The Law of Cyber-attack”.California Law Review.Vol.100, Issue 4. Pp. 817-886

Herselman, M and Warren, M (2010) “Cyber Crime Influencing Businesses in South Africa”. Issues in Informing Science and Information Technology

Herzog, S. (2011) Revisiting the Estonian Cyber-attacks: Digital Threats and Multinational Responses*."Journal of Strategic Security.* 4(2), 49-60.

IDG (2013) “Cyber Crime, Hacking and Malware”. An Annual Publication

Karnouskos, S (2014)Stuxnet Worm Impact on Industrial Cyber-Physical System Security. In:37th Annual Conference of the IEEE Industrial Electronics Society (IECON 2011), Melbourne, Australia, 7-10 November, 2011. Retrieved 8 January, 2014.

Kim, S.H., Hong wang, Q and Ullrich, J.B (2102) “A Comparative Study of Cyber-attacks”.Communications of the ACM, Vol.55, No.3. pp. 66-73

Kshetri, N (2014) Cyberwarfare: Western and Chinese. IT Pro.IEEE Computer Society.

MacEachern, C (2011) E-Canada and Cyber-attacks: Peril and Policy*. Dalhouse Journal of Interdisciplinary Management.*7, 1-15.

Marc, H (2011). "Investigating Policy Processes: The Governance Analytical Framework (GAF). In: Wiesmann, U., Hurni, H., et al. editors. Research for Sustainable Development: Foundations, Experiences, and Perspectives". Bern: GeographicaBernensia: 403–424.

Mugavero R. and Sabato (2014), Analysis and Estimation of Expected Cyber-Attack Scenarios and Consequences, Journal of Information and Security10: 138-152, RoutledgeTaylorand Francis Group.

Ogundiya, I.S (2010) Democracy and good governance: Nigeria's dilemma- *African Journal of Political Science and International Relations.* 4(6), 201-208,Retrieved on 8th January, 2014 from http://www.academicjournals.org/ajpsir.

Olusola, M., Samson, O., Semiu, A and Yinka, A (2013) "Impact of Cyber Crimes on Nigerian Economy".The International Journal of Engineering and Science (IJES). Vol. 12, Issue 4. Pp. 45-51.

Shackelford, E.D (2010) "Estonia Three Years Later: A Progress Report on Combating Cyber-attacks". Journal of International Law. Vol.33, No. 10.pp. 22-29

Shackelford, S.J (2009) From Nuclear War to Net War: Analogizing Cyber-Attacks in International Law. Berkeley Journal of International Law.27(1), 192.

Shackelford, S.J (2013)TowardCyberpeace: Managing Cyber-attacks through Polycentric Governance. American University Law Review.62 (5),1273-1364.

Udo-Akang, D (2014) Obamacare Cyber Perspectives: Connecting the Dots on Beneficiaries. Data Security and Speculation.*American International Journal of Contemporary Research*. 4(4), 16-27.

The Guardian News paper (2013)

World Bank (2006), World Development Report. Oxford University Press, New York.