FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 5 No. 1, March, 2021, pp 193 – 201
DOI: https://doi.org/10.33003/fjs-2021-0501-554

THE CHALLENGES OF SECURITY THREAT IN NIGERIA CYBERSPACE

***[1]Saidu, I. R., [2]Suleiman, T. [3]Akpan, U. E**

[1]Department of Intelligence and Cyber Security, Nigerian Defence Academy, Kaduna State, Nigeria.
[2]Department of Computer Science and IT, Federal University Dutsinma, Katsina State, Nigeria
[3]Department of Intelligence and Cyber Security, Nigerian Defence Academy, Kaduna State, Nigeria.

Corresponding Author's Email: rambo@nda.edu.ng

ABSTRACT

This research work was conducted to examine critically and systematically cyber threat intelligence challenges and prospects in Nigeria. It judges the value and relevance of cyber threat intelligence in the society where they are lacking in providing necessary information. Dealing with these challenges that may cause threat intelligence to be useless has become a major concern to Nigeria. The work was intended to achieve the following objectives: to examine the nature of cybersecurity in Nigeria, to analyse the cybersecurity threats that can disrupt the functioning of the country, to identify the challenges facing the Nigeria cyberspace and the conduct of a cyber threat intelligence analysis, to discuss the means by which cyber threat can be used to boost Nigeria's National Security Policy, to make recommendations to preserve important intelligence capabilities while ensuring the protection of its critical infrastructures through the use of threat intelligence. The scope of the study was limited to the period 2009 – 2019. The research was analytical. Relevant data were collected from both primary and secondary sources of data. The data analysis used the percentage instrument and the following conclusions were drawn: that threat data overload, threat data quality, privacy and legal issues and interoperability issues are some of the challenges of cyber threat intelligence; also, the need to continually invest in research, build local cyber threat management infrastructure and enhance the ability to anticipate, detect, respond and contain information security threats is very crucial. Nigeria can stand out if it utilises the potentials of cyber threat intelligence at an early stage by furthering researches to develop that field of inquiry.

Keywords: cyberspace, cybersecurity, cyberthreat, threat intelligence, data overload and privacy.

INTRODUCTION

The year 2017 witnessed a continuous increase in the use of internet-connected consumer devices but a similar increase cannot be said of the security of these devices as customer experience, cost and time-to-market requirements continue to take precedence over security requirements. The challenge is that many information and communication technology devices are not designed or maintained with security considerations as a priority as they are often sold with old and unpatched operating systems and software (Aladenusi, 2018). Nigeria is also not left out, as 2017 saw a proliferation in the use of Smart TVs, Apple watches, Smart Projectors, Smart whiteboards, etc. These recent might see an increase in ICT-related attacks both on endpoint devices and on the cloud. Businesses should take special care as they are ripe candidates and more liable to be victims, as these devices are being plugged into their corporate networks without proper security checks (Aladenusi, 2018).

Nigeria as a country and existing organizations in the country would need to re-evaluate and set clear policies in order to stay safe. Individuals, on the other hand, have to employ security measures such as immediately updating the device firmware and changing passwords (Aladenusi, 2018). To attain a great level of preparedness in a malicious event outcome the security sector has to be well informed through the use of Cyber Threat Intelligence. Therefore, this study had focused on ways to improve the security state of the country through the use of cyber threat intelligence also, the study provides a guide to security personnel on how to handle and conduct security checks to be able to detect vulnerabilities and possible exploits and implement proactive counter-measures towards these. The rest of the paper contains the research methodology, population, method of data collection, presentation of data, summary of findings, discussion of findings, summary and recommendations.

STATEMENT OF THE PROBLEM

Modern cyber attackers are sophisticated, well-funded, well-organized and use highly-targeted techniques that leave technology-only security strategies exposed. To identify and stop attackers, nations need to understand how they think, how they work, and what they want.

Today, the cybersecurity industry faces numerous challenges — increasingly persistent and devious threat actors, a daily flood of data full of extraneous information and false alarms across multiple, unconnected security systems, and a serious shortage of skilled professionals (RecordedFuture, 2019). Some organizations try to incorporate threat data feeds into their network, but don't know what to do with all that extra data, adding to the burden of analysts who may not have the tools to decide what to prioritize and what to ignore. A cyber threat intelligence solution can address each of these issues. Threat intelligence is actionable — it's timely, provides context, and is able to be understood by the people in charge of making decisions (RecordedFuture, 2019).

National security depends on the integrity of a nation's borders and its institutions. Also, all the spheres that make up the country now have a cyber-dimension (Morgenthau, 2012). This implies that the size and impact of the vulnerabilities of the cyberspace are difficult to predict and complex to measure. In addition, the activities that occur in the cyberspace are now increasingly as important as the activities on the ground.

This puts cyber defenders in a position where both their virtual and real security could be symbiotic. Despite the established fact that the cyberspace is fast creating difficulty in defining the distinction between real and virtual security, Nigeria seems to put cybersecurity on a low priority scale. Other challenges are seen as more important to its existence whereas it is an integral part of national security. Cybersecurity in its nature questions the concept of territory and borders. On the other hand, Nigeria may be incapable of having secured its cyberspace. Examining the strength and preparedness of Nigeria, it is of a vital necessity to identify the means by which Nigeria can overcome this border issue in dealing with the challenges of cybersecurity and its effectiveness. This is the problem this study attempts to address.

AIM AND OBJECTIVES OF STUDY

The aim of this study is to improve the cyber security state of the country through the use of cyber threat intelligence. This aim can be further achieved through the following objectives;

i. Examine the nature of cybersecurity in Nigeria.
ii. Analyse the cybersecurity threats that can disrupt the functioning of the country.
iii. Identify the challenges facing Nigeria cyberspace and the conduct of a cyber threat analysis.
iv. Discuss the means by which cyber threat intelligence can be used to boost Nigeria's National Security Policy.

RELATED LITERATURES

The use of the cyberspace to recruit and carry out other operations by individuals and even terrorist groups to disrupt countries, organizations and even other individual activities led to the rise of global terrorism (Schweitzer, Siboni, & Yogev, 2011). In Nigeria, the database of the Directorate of Secret Service (DSS) was hacked by the Boko Haram insurgent group in August 2012 as a response to Nigeria's Federal Government's attempts to deal with them (Olubayo, n.d.). During the period of the 2015 elections, there was an attempt to hack into the Independent National Electoral Commission (INEC) (Aladenusi & Olukoju, 2016 Nigeria Cybersecurity Outlook, 2016).

"The apparent virtual ungovernability of the cyberspace in Nigeria has provided a platform for the perpetration of cybercrimes, such as advanced fee fraud, terrorist recruiting and financing, hate speech, and ideo-religious radicalization" (Okoli & Idom, 2018). The number one victim of Nigeria's cyber atrocities is the country's national image and reputation.

"Nigeria's notoriety with cyber-crime has, over the years, given the country a negative brand as a fraudulent country" (Okoli A. C., 2013). As observed by Osho and Onoja (2015), "Long term commission of these crimes has left Nigerians and foreigners alike overly cautious to the extent where legitimate interactions of all forms originating in, or concerned with Nigeria and across cyberspace are now characterized with increasing disbelief". As also observed by Omale and Idom (2016), "Nigeria's global cyber notoriety has made it possible that vital country's financial documents such as bank cheques and drafts are now being viewed with suspicion in other countries of the world." This means that our financial documents are no longer viable and reliable pieces for international transactions (Okoli & Idom, 2018). Also, Nigeria e-mails are nowadays often being viewed with extreme caution by the international community. Even internet communication waves from Nigeria are sometimes blocked by other countries internet gateways. Nigerians are now being generally discriminated upon in the world because of the "yahoo boys" syndrome (Okoli & Idom, 2018). According to Idom and Ugal (2016), International Banks now do proper findings and protracted researches on Nigeria financial transactions before clearance often causing a delay. For this reason, foreign investors are scared of investing their capital in the Nigerian economy. The implication of this is that Nigeria commands only a little credibility by the reckoning of the comity of nations. This jeopardizes the prospects of the country as a business and an investment destination.

The issue of cyber-crime is one that has been discussed by many people with various perspectives on the issue, most coming at it from different sides than the others. Cyber-crimes have gone beyond conventional crimes and now have threatening ramifications to the national security of all countries, even to technologically developed countries like the United States (Ibikunle & Eweniyi, 2013). According to an ITU publication in (2012) which states that "the adoption by all countries of appropriate legislation against the misuse of Information and Communication Technology (ICT), for criminal or other purposes, including activities intended to affect the integrity of nationally critical information infrastructures, is central to achieving global cybersecurity". The publication further stated that since threats could originate anywhere around the globe, the challenges are inherently international in scope thus requires international cooperation, investigative assistance, and common substantive and procedural provisions. Thus, countries must harmonize their legal frameworks to combat cybercrime and facilitate international cooperation (Gercke, 2012). In lieu of the above, cybercrime is any illegal acts perpetrated in, on or through the internet with the intent to cheat, defraud or cause the malfunction of a network device, which may include a computer, a phone, etc. the illegal act may be targeted at a computer network or devices e.g. computer virus, denial of service attack (DoS), malware (malicious code), the illegal act may be facilitated by computer network or devices with target independent of the computer network or devices (Ibikunle & Eweniyi, 2013).

Nigeria has moved from being the fifth most attacked country in terms of mobile malware attacks in 2017 to being the third most hit in 2018 (Akiyode-Lawanson, 2019). According to reports by Kaspersky Lab, a global cybersecurity company with deep threat intelligence and security expertise, four African countries made the list in terms of top 10 countries by share of users attacked by mobile malware – Nigeria in third place at 37.72%, Algeria in fifth place (35.06%), Tanzania in eighth place (31.34%), and Kenya in ninth place with 29.72% (Akiyode-Lawanson, 2019).

Cybersecurity plays an important role in the ongoing development of information technology, as well as Internet services (Gercke, 2012). Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy (Gercke, 2012).

Deterring cybercrime is an integral component of national cybersecurity and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICT for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared responsibility requiring coordinated action related to prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus require a comprehensive approach (Gercke, 2012).

Cybersecurity strategies – for example, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime (Gercke, 2012). The development and support of cybersecurity strategies are a vital element in the fight against cybercrime. The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation (Gercke, 2012).

Prevalent in recent times are businesses, establishments, initiatives, organizations or nations as the case may be, creating and being governed by policies and strategies, applicable to all spheres of their operations and spanning their expected lifetime. These oftentimes exist as documents, which serve as guidelines to be followed in all situations, whether favorable or unfavorable, expected or unforeseen. Policies and strategies act as developmental frameworks characteristically crafted by key policymakers and top executives of an organization and meant to be austerely adhered to, regardless of immediate or impending situations, having been developed for these purposes (Osho & Onoja, 2015). The success of any organizational initiative is dependent on the immediate goals set out to achieve as well as the methods prescribed and adopted with which to achieve such goals. These documents are more frequently intertwined in the goals, which they set to achieve and, hence, are often regarded as being the same (Osho & Onoja, 2015).“National Cyber Security Strategy (NCSS) is the nation’s readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country’s presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community” (ONSA, 2014).

The government and the people of Nigeria have jointly taken various strategic measures towards the nation’s fight against cybercrime and enthroning culture of trust & confidence in our digital economy. Key components of Nigeria Cybersecurity Program include the creation of a New Framework for National Security Strategy, National Cybersecurity Policy Framework, National Cybersecurity Strategy, Nigeria Cybercrime Act 2015, Nigeria DNS-Security Policy by NIRA, National Policy on Public Key Infrastructure (PKI) by NITDA (2012). Also, the country has set up a National Coordinating Centre for the implementation of National Cybersecurity Strategy, a National CERT, a National Coordination Council, an International Contact for Cybersecurity, National Sectoral CCERT by NITDA, Framework for Nigeria Child Online Protection, Proactive legislations: Digital and Electronic Evidence Act 2011, Cybercrime Act 2015, Nigerian Digital Piracy Act of the Nigerian Copyright Commission, High level Political and Senior Public awareness as well in OPS, Nigeria Internet Governance Process, Cross sector DNS Security stakeholders engagement, adoption of COBIT 5 by NITDA for MDA IT system governance and risk management, International Law Enforcement Cooperation – Nigeria is a member of the G8 24/7 Network represented by EFCC, established broad based law enforcement relationship with many international law enforcement agencies, including the USA, UK, South Africa, etc. and the Nigerian government hopes to implement a sectorial cybersecurity engagement, operationalization of Cybercrime Act 2015, inauguration of National Cybersecurity Coordination/Advisory Council, Classification Information Infrastructures, strengthening of Nigeria internet governance process, strengthening of internet and cybersecurity industry and greater participation of Nigeria in the regional global multi-stakeholders policy process (Olugbile, 2019).

It is imperative that amidst several existing government concerns, the issue of Cyber Security is one whose relevance should be given utmost attention. Currently, cybersecurity considerations are inevitably gaining global attention. Having such relevance, concerned policymakers, governments and stakeholders cannot help but cautiously craft guiding principles in the form of policies and strategies with which issues of cybersecurity are meant to be governed (Osho & Onoja, 2015).

Jointly, purposeful and operational cybersecurity policy and strategy would facilitate the attainment of a reduced possibility of successful cyber incidents on a national level. It would provide a country with the capacity to prevent such attacks and swiftly address them in the event of their occurrence. It also would represent international equality thereby fostering cooperation amongst countries in areas of security and development (Osho & Onoja, 2015).

THE CYBERSECURITY AND CYBER THREAT INTELLIGENCE CHALLENGES IN NIGERIA

According to the United Nations Economic Commission for Africa (UNECA, 2014), "Africa is going through numerous Internet-related challenges concerning Cybersecurity threats(i.e intellectual property breach and security of personal data). Nigeria as a country is not an exception. Cybercriminals aim at people within and outside their national borders, and various African governments do not have the technical and the financial capability to mark and supervise electronic communications believed to be sensitive for national security."

Challenges of cybersecurity include: (UNECA, 2014)

i. Lesser security availability adequate to avert and manage the technological and informational threat.
ii. Deficiency of technical know-how regarding cybersecurity and failure to watch or monitor and secure national networks, making Nigeria and several African countries susceptible to cyber espionage, and incidences of cyber terrorism.
iii. Failure to develop and improve the required cybersecurity legal structure to battle cybercrime.
iv. Cybersecurity issues are extensive in scope than national security concerns. However, little major significant cybersecurity measures in Nigeria and even in Africa have its implementation done. Cybersecurity is a serious concern that needs absolute tackling.
v. There is also a necessity to develop an information society that respects values, rights, and freedoms and assures same access to information, even as stirring up the establishment of genuine knowledge that can put up assurance and confidence in the use of ICTs in Nigeria.
vi. Limited levels of consciousness of ICT-related security concerns by stakeholders, like ICT regulators, law enforcement agencies, the judiciary, information technology professionals and users (UNECA, 2014).

Other challenges include: (Ibikunle & Eweniyi, 2013)

i. Domestic and international law enforcement.
ii. Unemployment and Poverty Rate.
iii. Corruption.
iv. Lack of Standards and National Central Control.
v. Lack of Infrastructure.
vi. Lack of National Functional Databases.
vii. The proliferation of Cybercafés and Porous Nature of the Internet (Ibikunle & Eweniyi, 2013).

According to Uwaje (2009), the challenges of battling cybercrime by law enforcement agencies are divided into three categories:

i. **Technical challenges** that hamper law enforcement's ability to locate and prosecute criminals operating online.
ii. **Legal challenges** as a result of laws and legal devices needed to investigate and examine cyber-crime covering technological structural, and social changes.
iii. **Operational challenges** to ascertaining that we have developed a network of well-trained, well-equipped investigators and prosecutors who work together with astonishing pace – even over country's borders.

RESEARCH METHODOLOGY

This study is an analytical study, using quantitative procedures. The survey method was used in administering the questionnaires. Analytical research design is a type of survey research design which attempts to describe and explain why certain situations exist in an environment, a setting of the universe. This method allows data to be obtained from a population to assess some physiognomies of the population that would otherwise be too affluent to the study as a whole. The quantitative research method was engaged in rallying data in a numeric form with organized research instruments.

METHOD OF DATA COLLECTION

The method of data collecting included both primary and secondary data methods. The primary source of data for this project was obtained by overseeing questionnaires on individuals who have a broad knowledge of cybersecurity and cyber threat intelligence. This includes contact with personnel such as security experts/public servants in the defense and security sectors in Nigeria, the Nigerian Police Force, and other security/paramilitary agencies, civil servants and students. Data collected with the aid of survey questionnaires as instruments are considered as primary data because they are first-hand data gotten from personal experience or first-hand observation. The secondary sources of data came from archival and library sources such as books, newspapers, magazines, journals and the internet.

METHOD OF DATA ANALYSIS

The accomplished questionnaire forms were collected, coded and subsequently analyzed. In conducting the investigation, percentage analysis was used which was divided into three sections of Section A, Section B and Section C. Section A is the section that deals with demographic characteristics and Section B and C deals with research questions aimed at testing the basic assumptions in this research.

POPULATION

In mutual phraseology, the population is taken to mean all the people or the total number of people who live in a precise area, city or country. More exactly, however, a population can be designated as the totality of all elements, themes, or affiliates that possess a specified set of one or some collective positive features. Consequently, the population in this study comprises of the staff of various agencies that conducts cyber threat intelligence and some citizens that have a broad knowledge of cybersecurity be located in in the central region of the country which is the Federal Capital Territory, Abuja who are from ages 20 and above. According to National Bureau of Statistics (NBS) Nigeria, the last population census of Nigeria in 2016 provided the population of the country to be around 166.2 million people although the UN has placed the population at 202,867,836 million people with FCT, Abuja having over 3,095,118 persons as at 2019.

SAMPLING AND SAMPLING TECHNIQUES

Primary data basically through a questionnaire was collected in addition to the secondary data. A structured questionnaire was distributed to 250 adult citizens with diverse occupation amongst which are; public servants, self-employed, student, and civil servants residing in the central region of Nigeria. Among the distributed questionnaire, only 200 were returned. In other to ensure that the sample size acknowledged above is actually a illustrative of the genuine population as stated in the NBS and UN to ensure only the well-informed in the field are given the questionnaire, the simple random sampling techniques were adopted. Random samplings of two hundred and fifty (250) respondents were drawn out of over (3,095,118 million in FCT) people leaving in the six (6) districts in Abuja Municipal which includes; Gwarinpa, Maitama, Wuse II, Wuse Zone 5 and 6, Garki districts and having also ten (10) cadastral zones. The researcher multiplies the number of districts (6) by the number of cadastral zones (10) which is 60, by the average number of houses in the area (200) which gives a total number of (12,000).

To derive a sample size, the researcher divides the population size of the six districts (3,095,118 million) by the total number of houses in the area (12,000), which is (258) individuals randomly selected from the pool of people that are in the field of IT and Cybersecurity.

RESEARCH DESIGN

The study is an critical study, using quantitative measures. The survey technique was used to distribute the questionnaires. Analytical research design is a type which attempts to pronounce and enlighten why certain situations exist in a surroundings or a setting of the universe. This method allows data to be obtained from a population to assess some characteristics of the population that would otherwise be too expensive to study as a whole. The quantitative research method was employed in gathering data in a numeric form with structured research instruments.

DATA PRESENTATION AND DISCUSSION

The questionnaire as a primary source of data was used to collect the data for testing the basic assumption for the project. Tabulation and percentage were engaged to present the data collected so as to ensure easy understanding. The items on the questionnaire were analysed using basic statistical techniques of percentage i.e. $\% = \frac{no\ of\ responses}{total\ no\ of respondents}\ x\ 100$

PRESENTATION OF DATA

Table 4.1: Questionnaire administered to respondents

QUESTIONNAIRES	FREQUENCY	PERCENTAGE
Filled and Returned	200	80%
Not Filled but Returned	15	6%
Not Returned	35	14%
Total Distributed	250	100%

Observation: Table 4.1 shows that two hundred and fifty (250) questionnaires were distributed two hundred (200) which represents (80%) were filled and returned, while fifteen (15) questionnaires which represented (6%) were not filled but returned and thirty-five (35) questionnaires which represented (14%) were not returned.

Table 4.2: Sex distribution of respondents

GENDER	FREQUENCY	PERCENTAGE
Male	117	58.5%
Female	83	41.5%
Total	200	100%

Observation: The larger percentages of respondents were male 58.5% with 117 out of 180 representations while females made up 41.5% of 83 out of 180. Therefore, the population which this research covered were more of male than female as shown in Table 4.2.

Table 4.4: The cybersecurity threats that can disrupt the functioning of the country.

S/N	CYBERSECURITY THREATS THAT CAN DISRUPT THE COUNTRY	Strongly Agree (SA)	Agree (A)	Undecided (U)	Dissgree (D)	Strongly Disagree (SD)	Total
1	Malware	103 51.5%	77 38.5%	14 7%	0	0	200 100%
2	Phishing, Pharming, Spear Phishing	98 49%	82 41%	20 10%	0	0	200 100%
3	“Man in the Middle” (MitM) Attack	126 63%	65 32.5%	9 4.5%	0	0	200 100%
4	Denial of Service Attack or Distributed Denial of Service Attack (DDoS)	172 86%	28 14%	0	0	0	200 100%
5	Ransomware	168 84%	20 10%	12 6%	0	0	200 100%
6	Trojans	180 90%	20 10%	0	0	0	200 100%
7	Data Breach	165 82.5	30 15%	5 2.5%	0	0	200 100%
8	Malware on Mobile Apps	96 48%	74 37%	13 6.5%	17 8.5%	0	200 100%
9	Cyber Espionage	180 90%	20 10%	0	0	0	200 100%
10	Hackers	180 90%	20 10%	0	0	0	200 100%

Observation: Table 4.4, on the cybersecurity threat that can disrupt the functioning of the country; Malware had 51.5% or 103 out of 200 respondents that strongly agreed with the statement another 38.5% or 77 out of 200 respondents agreed also, while 7% or 14 out of 200 respondents remained undecided. Phishing, Pharming and Spear Phishing had 49% or 98 out of 200 respondents that strongly agreed with the statement another 41% or 82 out of 200 respondents agreed also, while 10% or 20 out of 200 respondents remained undecided. “Man-in-the-Middle” (MitM) Attack had 63% or 126 out of 200 respondents that strongly agreed with the statement another 32.5% or 65 out of 200 respondents agreed also, while 4.5% or 9 out of 200 respondents remained undecided. Denial of Service (DoS) or Distributed Denial of Service (DDoS) had 86% or 172 out of 200 respondents that strongly agreed with the statement another 14% or 28 out of

200 respondents agreed. Ransomware had 84% or 168 out of 200 respondents that strongly agreed with the statement another 10% or 20 out of 200 respondents agreed also, while 6% or 12 out of 200 respondents remained undecided. Trojan had 90% or 180 out of 200 respondents that strongly agreed with the statement another 10% or 20 out of 200 respondents agreed also. Attacks on IoT Devices had 61.5% or 123 out of 200 respondents that strongly agreed with the statement another 28% or 56 out of 200 respondents agreed also, while 9.5% or 19 out of 200 respondents remained undecided. Data Breach had 82.5% or 165 out of 200 respondents that strongly agreed with the statement another 15% or 30 out of 200 respondents agreed also, while 2.5% or 5 out of 200 respondents remained undecided. Malware on Mobile Apps had 48% or 96 out of 200 respondents that strongly agreed with the statement another 37% or 74 out of 200 respondents agreed also, while 6.5% or 13 out of 200 respondents remained undecided and 8.5% or 17 out of 200 respondents disagreed with the statement. Cyber Espionage had 90% or 180 out of 200 respondents that strongly agreed with the statement another 10% or 20 out of 200 respondents agreed also. Bot network operators had 48% or 96 out of 200 respondents that strongly agreed with the statement another 38% or 76 out of 200 respondents agreed also, while 6% or 12 out of 200 respondents remained undecided and 8% or 16 out of 200 respondents disagreed with the statement. Hackers had 90% or 180 out of 200 respondents that strongly agreed with the statement another 10% or 20 out of 200 respondents agreed also. Respondents also mention some other threats that can disrupt the functioning of the country to include: crypto-jacking and politically motivated attacks like hacktivism. The implication, therefore, is that these are not the only cyber-attacks that a nation can face, several other attack forms and vectors exist and are emerging to a stronger form as the day goes by.

SUMMARY OF FINDINGS

It has been established from the simple percentage that response with the highest percentage i.e. above fifty per cent (50%) are picked and analysed in percentage form. However, from the research conducted, it is discovered that cybersecurity which includes cyber threat intelligence analysis is important in any state structure and its continued maintenance is fundamental to the proper functioning of such state especially when reliance on information and communication technology is inevitably in use in that state. Also, it has been established that several challenges are faced by a nation in conducting cyber threat intelligence and thus may reveal threats at a slower rate, as much as this is the case this research has made effort to outline ways through which these challenges can be mitigated. And finally, strategic policies that can help the government to conduct its cyber threat analysis thus maintain a high data security level were all discovered and outlined in the research work.

DISCUSSION OF FINDINGS

In analysing the objectives, of this research work, a greater percentage accepted the assumptions in this research. Which means that cyber threat intelligence is very important in this information technology age and that certain strategies and policies are needed in place for the continuous gathering of threat intelligence which is germane to the protection of state's critical infrastructures. The essence is to provide secured cyberspace for the country and its citizens and the creation of CIRT, CERT and CSIRT team(s) to respond to issues as relating to cyber threats or threat of attack or potential attack, creating acceptable standards for usage of information and communication systems by the citizens and the nation at large.

CONCLUSION AND RECOMMENDATIONS

This chapter covers the summary of the research work, a review of achievements during the research and discoveries in the research, including the areas of application of these findings and achievements. The major contribution to knowledge would be highlighted and suggestions for further research would be stated. Recommendations would be made as it relates to the study this would help future researchers and also would enrich the existing stock of literature expanding the frontiers of knowledge through its findings.

SUMMARY

This project started by dwelling on all the technicality in chapter one, where four specific objectives were stated including three research questions. The issues, time frame and subjects covered by the study were also highlighted. The main definitions of terms used in this study were as well justified. In chapter two, related extent and relevant literature were reviewed and also one theory was analyzed to support the project. Chapter three of the work fully covered the methodology while chapter four included data assessment and analysis and presentation. Finally, in chapter five, the entire work was summarized and we drew some conclusions on the basis of which we made some recommendations.

This research work is aimed at studying cyber threat intelligence challenges and prospects in Nigeria. Respondents were made up of public servants, civil servants, self-employed and students. These respondents were, however, were drawn mostly from the Federal Capital Territory Abuja and Kaduna. A total of four basic objectives were formulated from which twenty-six questions were deduced to form part of the questionnaires. Thus, the instrument of data collection is the questionnaire.

RECOMMENDATIONS

The need, to recognize the different approaches to building and implementing cyber resilience depends entirely in detection, prevention, response and recovery. According to a study, the recovery process after a cyber-attack gulp 19% of the cost, followed by containment 16%, investigation 13% and incident management and ex-post response 11%. In view of this and in light of the discoveries made in the cause of this research work, the following recommendations are made:

i. They should be policies on cybercrimes which would be circulated all around the country.
ii. The policy should make clear what type of breach that should be reported and companies that have been attacked should endeavour to report such and also ways to prevent further attacks so that others could learn from.
iii. Cyber insurance is very important as companies are advised to make sure their insurance covers cyber incidents.

iv. More investment should be made into cybersecurity research and new ideas should be further studied and made known to the general public

v. The absence of a general data protection framework implies there is no law imposing strict responsibility on organizations to ensure the security of personal data. The government should make laws to prevent cover of this.

vi. Awareness is key; thus, training should be conducted periodically to ensure that people are aware of their level of exposure to cyber-attacks.

vii. Increased investment in cybersecurity is very essential.

viii. Government organization should engage in threat intelligence sharing and also come together to build strategies that can be adopted by all in protecting the cyberspace.

REFERENCES

Ajayi, K. (2015). *Intelligence Data Sources Methods and Problems.* Ado - Ekiti, Ekiti: Intelligence and Security Studies Programme.

Akiyode-Lawanson, J. (2019, March 09). *Cybercrime: Nigeria ranks 3rd most attacked country in Africa*. Retrieved October 08, 2019, from Businessday NG: https://businessday.ng/technology/article/cybercrime-nigeria-ranks-3rd-most-attacked-country-in-africa/

Akpan, U. E. (2019). *An Argumentative Review Essay on the Conceptualization and Definition of Cyber Security Synthesizing a Proprietary Definition of Cyber Security.* Kaduna: Unpublished.

Aladenusi, T. (2018). *2018 Nigeria Cybersecurity Outlook [Online]*. Retrieved September 25, 2019, from Deloitte Nigeria: https://www2.deloitte.com/ng/en/pages/risk/articles/2018_nigeria_cybersecurity_outlook.html#

Aladenusi, T., & Olukoju, A. (2016). *2016 Nigeria Cybersecurity Outlook*. Retrieved September 26, 2019, from Deloitte Nigeria: http://www2.deloitte.com/ng/en/pages/risk/articles/2016-nigeria-cybersecurity-outlook.html

Aniche, D.C.P. (2019). *General Introduction to Cybersecurity.* Kaduna: Unpublished.

Bureau of Justice Statistics, U.S. Dept. of Justice. (1989). *Computer Crime: Criminal Justice Resource Manual.*

Buzan, B. &. (2013). *Regions and powers: the structure of international security.* Cambridge: Cambridge University Press.

Buzan, B., Waever, O., & Wilde, J. (2013). *Security a new framework for analysis.* Boulder, CO: Lynne Rienner.

CIS. (2017, April 24). *What is Cyber Threat Intelligence?* Retrieved September 28, 2019, from CIS: https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence/

Deloitte. (2019). *Cyber 101 | Deloitte SEA | Risk Advisory.* Retrieved October 11, 2019, from Deloitte Singapore: https://www2.deloitte.com/sg/en/pages/risk/articles/cyber-101.html

Denardis, L. (2014). The Internet Governance Oxymoron. *The Global War for Internet Governance,* 1-32. DOI:10.12987/yale/9780300181357.003.0001

Digital-Guardian. (2019, July 15). *What is Cyber Security? Definition, Best Practices & More.* Retrieved September 28, 2019, from Digital Guardian: https://digitalguardian.com/blog/what-cyber-security

DOD, J. C. (2016). *Department of Defense Dictionary of Military and Associated Terms.* Washington: Joint Publication 1-02.

ENISA. (2019, September 19). *National Cybersecurity Strategies.* Retrieved September 28, 2019, from ENISA: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

Fireeye. (2019). *FireEye Threat Intelligence. [online]*. Retrieved September 25, 2019, from FireEye.com: https://www.fireeye.com/solutions/cyber-threat-intelligence.html

Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response. Geneva, Geneva, Switzerland. Retrieved October 08, 2019, from www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Hallingstad, G., & Dandurand, L. (2010). *Cyber Defence Capability Framework.* The Hague: NATO C3 Agency.

Hansel, M. (2013, June 27). *Cyber Security Governance and the Theory of Public Goods.* Retrieved from E: https://www.e-ir.info/2013/06/27/cyber-security-governance-and-the-theory-of-public-goods/

Ibikunle, F., & Eweniyi, O. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE), 1*(1), 1-11. Retrieved September 25, 2019

Idom, A. M., & Ugal, D. B. (2016). Influence of ICT competence on cybercrimes in selected cities of the six geo-political zones in Nigeria. *FULafia Journal of Humanities and Social Sciences, 1*(1), 220 - 241. Retrieved September 25, 2019

Marzoni, D. (2019, January). *IT Law: Lawyer: Dmitriy Marzoni: +38097-44444-55*. Retrieved December 30, 2019, from Lawyer: https://www.dmlawyer.top/it-law/

Morgenthau, H. (2012). *Politics among Nations: the Struggle for Power and Peace.* (K. Thompson, Ed.) New Delhi: Kalyani.

Odinma, A. C. (2010). *Cybercrime & Cert: Issues & Probable Policies for Nigeria.* DBI Presentation.

Oforji, J. C., Udensi, E. J., & Ibegbu, K. C. (2017). Cybersecurity Challenges in Nigeria: The Way Forward. *SosPoly Journal of Science & Agriculture, 2*, 1-5.

Okoli, A. C. (2013). 'Rebranding Nigeria' as a Reputation Management Drive: Implications for National Image. *Journal of Communication and Media Research, 5*(2), 81 - 87.

Okoli, A. l., & Idom, A. M. (2018). The Internet and National Security in Nigeria: A Threat - Import Discourse. *Covenant University Journal of Politics & International Affairs, 6*(1), 1. Retrieved September 25, 2019

Okonigene, R. E., & Adekanle, B. (2009). Cybercrime In Nigeria. *Business Intelligence Journal*.

Olubayo, A. (n.d.). *Cybersecurity: Africa's Next Challenge*. Retrieved September 26, 2019, from Linkedin.com: http://www.linkedin.com/pulse/20140722215101-5180516-cybersecurity-africa-s-next-challenge

Olugbile, S. (2019). *Overview of Nigeria Cybersecurity Readiness.* Retrieved October 09, 2019, from Aficta.africa: https://aficta.africa/images/stories/roundtable/overview-of-nigeria-cybersecurity.pdf

Omale, D. J., & Idom, A. M. (2016). Fibre optics technology and cybercrimes in Calabar Metropolis, Nigeria. *International Journal of Social Relevance & Concern*, *4*(4), 1 - 15. Retrieved September 25, 2019, from www.ijournals.in/ijsrc

ONSA, (2014). *National Coordinator for Security and Counterterrorism.* Nigeria: National Cyber Security Strategy.

Osho, O., & Onoja, A. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology (IJCC), 9*(1), 120 - 143. doi:001:10.5281/ZENODO.22390

PaloAlto. (2016). *New from Unit 42.* Retrieved October 11, 2019, from The Insider Report November 2016 - Palo Alto Networks: https://www.paloaltonetworks.com/customers/customer-newsletter/the-insider-report-november-2016

RecordedFuture. (2019). *What is Threat Intelligence?* Retrieved September 25, 2019, from Recorded Future: https://www.recordedfuture.com/threat-intelligence/

Roehrs, P. (2005). *Weak States And Implications For Regional Security: A Case Study Of Georgian Instability And Caspian Regional Insecurity*. Athens: Research Institute For European And American Studies, RIEAS.

Schweitzer, Y., Siboni, G., & Yogev, E. (2011). Cyberspace and Terrorist Organizations. *Journal of Military and Strategic Affairs, 3*(3), p. 40. Retrieved September 26, 2019

Schweitzer, Y., Siboni, G., & Yogev, E. (2011). Cyberspace and Terrorist Organizations. *Journal of Military and Strategic Affairs, 3*(3), p. 40. Retrieved September 26, 2019

SuperUser. (2017). *Nigeria Faces Greatest Cyber Security Threat Ever In 2017*. Retrieved October 11, 2019, from Stop. Think. Connect. | Nigeria: https://stopthinkconnect.ng/index.php/blog/item/23-nigeria-faces-greatest-cyber-security-threat-ever-in-2017

Techopedia.com. (n.d.). *What is Cyber Defense? - Definition from Techopedia.* Retrieved September 28, 2019, from Techopedia.com: https://www.techopedia.com/definition/6705/cyber-defense

Underwood, K. (2018, August 30). *Cyber Threat Intelligence Leader Warns of Changing Nature of Attacks [Online]*. Retrieved September 25, 2019, from AFCEA International: https://www.afcea.org/content/cyber-threat-intelligence-leader-warns-changing-nature-attacks

UNECA, U. N. (2014). *Tackling the challenges of Cybersecurity in Africa*. Retrieved from Tackling the challenges of cybersecurity in Africa | United Nations Economic Commission for Africa: https://www.uneca.org/publications/tackling-challenges-cybersecurity-africa