Oct 20th, 1:00 PM - 1:25 PM

Capturing the Existential Cyber Security Threats from the Sub-Saharan Africa Zone through Literature Database

Samuel B. Olatunbosun
Norfolk State University, sbolatunbosun@nsu.edu

Nathanial J. Edwards
Norfolk State University, n.j.edwards@spartans.nsu.edu

Cytyra D. Martineau
Norfolk State University, c.d.martineau@spartans.nsu.edu

Abstract
Abstract - The Internet brought about the phenomenon known as Cyber-space which is boundless in nature. It is one of the fastest-growing areas of technical infrastructure development over the past decade. Its growth has afforded everyone the opportunity to carry out one or more transactions for personal benefits. The African continent; often branded as 'backward' by the Western press has been able to make substantial inroads into the works of Information and Computer Technology (ICT). This rapid transition by Africans into ICT power has thus opened up the opportunities for Cybercriminal perpetrators to seek and target victims worldwide including America for personal financial gains. This existential threat has been growing in bounds and leaps over the past few years that the news media has been awash with cyber-attacks from African countries including Nigeria, South Africa, Ghana, Zimbabwe, and a host of other African nations. There have been several academic research and articles published on the African cyber-criminal activities by several authors; most of which are in silos and in non-subject specific databases everywhere. Our sponsored summer long project therefore re-analyzed the African style cyber- attacks culminating in the creation of an Access based database that captured the pertinent data about the reported cases through the use of secondary data sources.

Location
KC 460

Disciplines
Information Security | Management Information Systems | Technology and Innovation

1. Background and Introduction

Computer crimes of various kinds have been perpetrated by people of different nationalities across the globe for many years and it seems more sophisticated and ingenious methods are being devised to beat the many known strategies that have been put in place by cyber security experts to prevent or stop the crimes (Okonigene, 2009). In monetary terms, billions of dollars have been lost by individuals and corporate entities who unfortunately have fallen victims to these cyber criminals (Anderson, 2012).

The Internet and its derivative World Wide Web (WWW) have been described as some of the most innovative and amazing technological addition to mankind's way of socializing and doing business. It is now more like a global meeting place where citizens of the world now come together to make things happen – business, social, political, and just about any kind of association one can imagine capable of being done electronically (ECEG, 2015).

One or more computers are often involved for basic service provision and through which everything imaginable under the Sun could be done in one fingertip especially where smart devices are now ubiquitous. Pretty much anyone with access to the Internet can become productive in a short space of time. The Internet, it seems, is like an opportunity galore that makes possible several other variety of things including emailing, information access and retrieval, social networking, on-line chatting, telecommunication, e-commerce (electronic shopping), software purchasing, upgrading, and downloading, to mention just a few (Valacich, 2003).

The list of other ingenious things that the Internet can be used for has been growing steadily. But just as the Internet has proved so indispensable, so are the potentials for abuse and several other negative uses considered unethical and most times, illegal. The computer industry has used many names to describe the negative side of the internet such as "computer crime", "cyber-crime" and "cyber-terrorism" to mention a few. Some of these names have often been used interchangeably many times as well and it depends on who you ask. In a nutshell, computer crime has been defined as "the act of using a computer to commit an illegal act" (Okonigene, 2009).

Compiled by the Center for Strategic International Studies (CSIS) on behalf of McAfee, it was estimated that the global impact of cybercrime is larger than those of the national economy of many countries with a staggering sum of more than $400 billion (Anderson, 2012).

Interestingly, cyber-crime is no longer about monetary gains only. It has evolved into using it to settle scores on an international scale where the attacking party will carefully select their target based on political, commercial, and

security interests using available social engineering techniques. The Internet search company, Google, FBI have revealed the existence of large-scale computer intrusions, apparently coming from Russia and China with some support from the perpetrators' state government. Iran, India, North Korea are no exception either and where hacking into the United States infrastructural system is now common place ("FBI, 2016).

Infiltration of the year 2016 US general election was a case in point with the general belief that the Russian attacks cost the Democratic Party the presidential election. The FBI and the Department of Homeland Security (DHS) in December 2016 in fact released a joint report detailing how federal investigators linked the Russian government to hacking of the Democratic Party organizations. A 13-page report at the time provides technical details about the tools and infrastructure used by the Russian civilian and military intelligence services to compromise and exploit the networks associated with the U.S. general election, as well as a range of U.S. Government, political, and private sector entities ("FBI, 2016).

The cyber security threat race unfortunately is no longer about Russia, China, Iran, etc. The threat is everywhere with African countries fast joining the foray. For example, Nigeria, the so called "giant of Africa" and the most populated country in the African continent (c.170 million people) seem not to be too far behind in the league of countries that can 'shock and shake' America if the US becomes complacent (Okonigene, 2009). Blessed with abundance of natural and human resources, crime of all kinds are of regular occurrence in many urban cities in Nigeria. The introduction of the Internet in the mid-nineties actually ensured that cybercrime was quickly added to the mix of undesirable criminal activities taking place in Nigeria (Adebusuyi, 2008).

The spread of specific cybercrime activities in Nigeria in recent years has become a source of embarrassment and concern to many law-abiding Nigerian citizens because of its peculiarity. For instance, the so- called "Yahoo boys" from Nigeria have been having a field day scamming foreign nationals with their victims incurring huge monetary losses. In fact, some recent cyber study survey concludes that Nigeria ranked third as the most internet fraudulent country in Africa (Adebusuyi, 2008).

The two leading economic powerhouses in Africa; Nigeria and South Africa in particular have been in severe economic recession for quite a while and still recovering. Same is true for many smaller African nations with some embroiled in disastrous civil strives where citizens have been engaging in whatever means possible to survive (Trends", 2016). African news media and social networks have been awash with news of untold hardships being felt by citizens of these countries with high poverty levels forcing people into crimes of all kinds including well documented and sophisticated international cyber strikes unheard of just a few years ago. United States, unfortunately has had her

'unfortunate' share of cyber- attacks by African perpetrators.

Previous study on the Nigerian case has also revealed that the so called "Yahoo Boys" perpetrators are basic young high school/college dropouts with incredibly high Intelligent Quotient (IQ) and with the brilliance to hack into any targeted computer worldwide (Okonigene, 2009). One can imagine when University trained jobless computer science graduates with higher skills join the basic perpetrators.

As Africa becomes more sophisticated with computer technology, the thought is that one or more large scale attacks directed to US homeland are a possibility from the region. Our previous study uncovered many published papers on the subject. Unfortunately, all of these exists in isolation making the task of sifting through the reports for specific information a very time consuming exercise. In addition, there is no centralized database capturing specific data that can be used to understand the seriousness of the crimes. In fact, it is hard to predict the likelihood of a more serious attacks on the US homeland in the near future.

With this project therefore, we sifted through at least 100 published materials, extracting, collecting and organizing data pieces from the publications and storing the data items into one centralized Microsoft Access database. Our database is robust and capable of providing several useful information from a single source about the African cyberattack incidents. The next possible phase is to migrate the existing database into one or more of the more advanced DBMS software driven by Artificial Intelligence (AI), and Machine learning (ML) technologies. Such platform will be capable of forecasting and predicting the possibility of, and occurrence of future attacks as well as providing measures that can help prevent such attack.

2. Description of the Project

Reviewing and analyzing existing published works, we gathered data for cybersecurity breaches and threats from each of the fifty-eight nations in the African continent. In addition, we recorded the data based on cybercrime types, anti-cybercrime laws in each Country, as well as describing publication sources and authors. We also wrote annotated bibliographies (short summaries) on each of the paper reviewed.

Existing research papers and publications on African cybersecurity have mostly discussed who the specific perpetrators are, their modes of operation, where the perpetrators came from, reasons for committing the crimes, and who have been impacted by their peculiar cyber-crime activity in one way or the other. There appears to be no formal data repository where the events have been captured and stored in a single database. The published materials exist in isolation everywhere in multiple databases. This project therefore took the extra

step of accessing some of the documents, reviewed one hundred of them, and looked for patterns, themes, and common factors between these African nations. The data set were further categorized and grouped in such a way that the development of the actual database was possible.

One of the objectives was to have the database help provide useful information about the following when queried:

- Cyber-security breaches peculiar to a named or specific African country
- Country of perpetrators and groups involved
- Motivation for the attacks
- Factors influencing the attacks
- Types of attack and their foreign targets/victims
- Influence of perpetrator countries' government and their respective preventive measures (legal)
- Other unknown pieces of information that may be relevant to the research emerging from the study

In the long term, our ideal database should not only be able to document data. It should be capable of carrying out a more comprehensive risk assessment based on the following:

I. Probability and Possibility Assessment
II. Impact and Vulnerability Assessment
III. Magnitude (scale) Assessment
IV. Detection and Prevention Assessment

3. Research Methodology

Secondary Data Analysis Rationalization

Secondary analysis is an empirical exercise that applies the same basic research principles as studies based on primary data. It involves using existing data – collected for the purposes of a prior study – to investigate a research interest that is distinct from the original work (Houston, 1998). Leveraging existing data allows projects to be completed and findings to be produced much faster, enabling

contributions to the body of knowledge to occur before they are superseded by new developments in the field (Johnston, 2014).

In addition, the following steps were taken:

Step 1: Searched and reviewed the literatures. Gathered evidence based on one hundred published materials, journals, artifacts in the University library domains that included the following library sources:

- Utilizing published work contained in academic databases e.g. (Proquest, JSTOR, Google Scholar, ACM digital library etc.)
- Archived data from other public and quasi- public bodies
- Report and survey results already available from research organizations available publicly
- Research works and information available from the academic units in Colleges and Universities of the targeted African countries

Step 2: Extract statistical data from the one hundred sources identified in step 1. These data pieces were further documented in an Excel spreadsheet.

Step 3: Analyze data set, identify key terms, phenomenon, categorize terms, and identify pervasive themes that were grouped in an Excel spreadsheet.

Step 4: Design and develop the basic data repository. This was accomplished using MS Access Database Management Software, DBMS.

Step 5: Provide project formal (summative) report for project to project sponsoring agencies including Oak Ridge Associated Universities (ORAU), Department of Homeland Security (DHS), Borders, Trade, and Immigration (BTI) center of the University of Houston, Texas.

4. Sample Database Test and Analysis

Table A

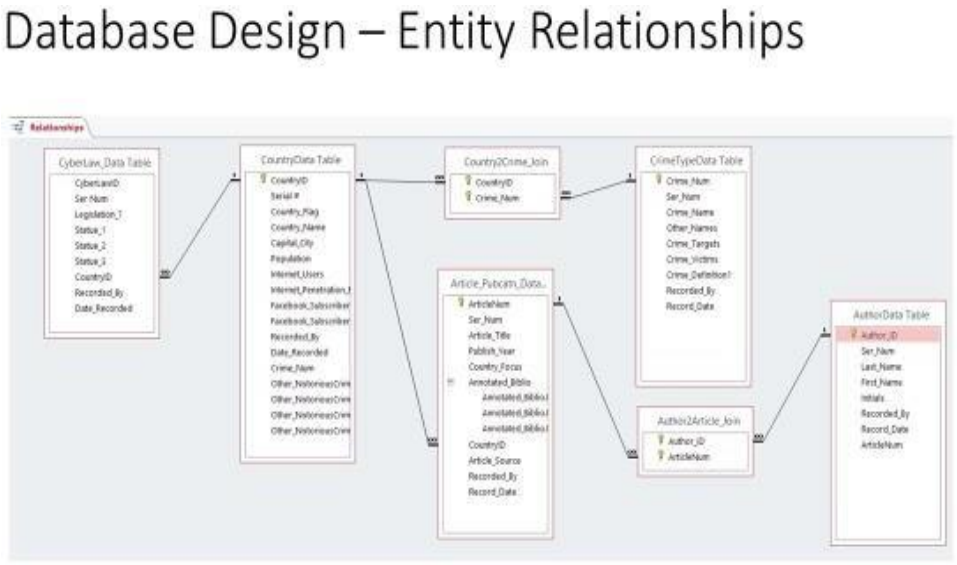
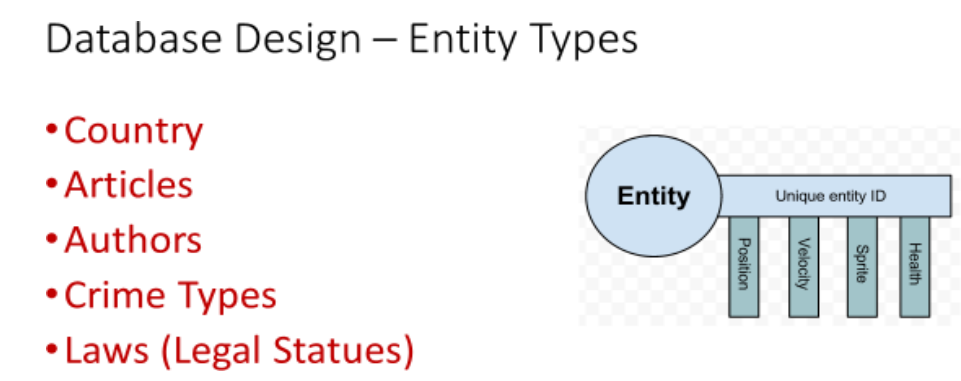


Table B



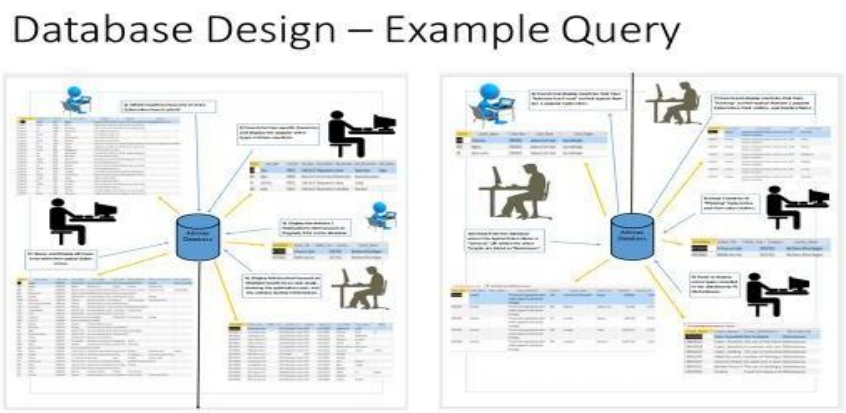


Table D

Table F

Table G

Database Design – Sample Reports

Example Query Statements

1. Which Countries have one or more Cybercrime laws in place?
2. Search for four specific Countries and display the popular crime types in those countries.
3. Display the Articles/Publications that focused on Region1, RG1 in the database.
4. Display Articles that focused on Multiple Countries as case study, showing the publication year, and the articles' Author information.
5. Query and Display All Countries with their typical Cybercrime.
6. Search and display countries that have **"Advance Fee Fraud"** as their typical Number 1 popular Cybercrime.
7. Search and display countries that have **"Hacking"** as their typical Number 1 popular Cybercrime, their victims, and Country Name.
8. Show Countries of "Phishing" Cybercrime and their crime victims. ***(VictimOfPhishing Query)***
9. Show or display crime types recorded in the database by PI Olatunbosun.
10. Show from the database where the typical Crime Name is "General" OR where the crime Targets are listed as "Businesses".

Qn1 Screenshot:

CyberLawID	Legislation_?	Country	Country_Name	Statue_1	Statue_2	Statue_3
CBL1	Partial	ALG	Algeria	Criminal Code of 2004 fi	Law n° 09- 04 on specifi	Partial legislation in force
CBL3	Partial	BEN	Benin	Substantive criminal pro	No specific procedural l	_
CBL4	Yes	BWN	Botswana	Cyber Crime and Compu	Electronic (Evidence) Re	_
CBL8	Yes	CMR	Cameroon	Law 2010/012 (21 Decer	_	_
CBL10	Partial	CHD	Chad	Loi relatifs à la cyber séc	_	_
CBL13	Yes	IVC	Côte d'Ivoire	Law 2013-451 (19 June 2	_	_
CBL21	Partial	GMB	Gambia	Information and Commu	_	_
CBL22	Yes	GHN	Ghana	Electronic Transactions .	Mutual Legal Assistance	Accession to Budapest Convention
CBL25	Partial	KNY	Kenya	Legislation partially in fc	Draft law on cyber crime	_
CBL29	Partial	MSR	Madagascar	Loi 2014-006 sur la lutte	_	_
CBL32	Yes	MRT	Mauritania	Loi 2016-007 relative à l	Note: Implementing reg	_
CBL33	Yes	MTS	Mauritius	Computer Misuse and C	_	_
CBL35	Partial	MRC	Morocco	Amendments to crimina	Partial legislation in forc	_
CBL36	Partial	MZQ	Mozambique	Partial substantive law p	_	_
CBL39	Yes	NGR	Nigeria	Cyber Crimes (Prohibitio	Evidence Act as amende	_
CBL41	Partial	RWD	Rwanda	Partial substantive law p	_	_
CBL44	Yes	SNG	Senegal	Law 2008-11 (25 Januar	Accession to Budapest C	_
CBL48	Partial	SAF	South Africa	Draft law (Cyber Crimes	Partial legislation in forc	_
CBL50	Partial	SDN	Sudan	Cyber Crime Act 2007	_	_
CBL52	Yes	TZN	Tanzania	Cyber Crimes Act 2015 (:	_	_
CBL54	Partial	TNS	Tunisia	Few provisions in Penal (	Draft law on cyber crime	_
CBL55	Yes	UGD	Uganda	Computer Misuse Act 20	_	_
CBL57	Yes	ZMB	Zambia	Computer Misuse and C	Electronic Communicati	_
CBL58	Partial	ZBW	Zimbabwe	Chapter VIII Criminal La	Computer Crime and Cy	_

Qn2 Screenshot:

Country	Country_Name	Crime_Num	Crime_Name	Crime_Definition1	Other_Notorious(	Other_NotoriousCrime	Other_Notoriou
GHN	Ghana	CRM1011	Credit Cards ID	Taking someone's cr	General	Romance Scams	Sakawa
NGR	Nigeria	CRM1002	Advance Fee Fra	A form of fraud, ofte	Romance Scams	Business Email Compromi	-
SAF	South Africa	CRM1011	Credit Cards ID	Taking someone's cr	Hacking	Cracking	-
ZMB	Zambia	CRM1011	Credit Cards ID	Taking someone's cr	Cyber Bullying	Ransomware	-

Qn3 Screenshot:

ArticleNum	Article_Title	Publish_Year	Country	Country_Name
ART00003	A Focus on Cybe	2010	RG1	Northern Africa Region
ART00062	Middle East, No	2015	RG1	Northern Africa Region

ArticleNum	Article_Title	Publish_Year	Country_Foc	Country	Author_ID	Last_Name	First_Name	Initials
ART00012	Analyzing Cyber	2016	Multiple Countr	MLT	AUT10005	Alqatawna	Ja'far	-
ART00012	Analyzing Cyber	2016	Multiple Countr	MLT	AUT10064	Halaseh	Rola	Al
ART00024	Challenges of C	2013	Multiple Countr	MLT	AUT10125	Sarrab	Mohamed	-
ART00037	Cybercrime in A	2016	Multiple Countr	MLT	AUT10056	Fassassi	Amzath	-
ART00037	Cybercrime in A	2016	Multiple Countr	MLT	AUT10127	Shiloh	Jean	-
ART00051	Fighting Cybercr	2012	Multiple Countr	MLT	AUT10092	Martin-Odoom	Alexander	-
ART00051	Fighting Cybercr	2012	Multiple Countr	MLT	AUT10120	Quarshie	Henry	Osborn
ART00063	Namibia a top A	2016	NMB	MLT	AUT10015	AWA06	-	-
ART00079	Sub-Saharan Afr	2014	Multiple Countr	MLT	AUT10022	AWA13	-	-
ART00080	Tackling the cha	2014	Multiple Countr	MLT	AUT10126	Seck	Mactar	-
ART00080	Tackling the cha	2014	Multiple Countr	MLT	AUT10030	Belai	Tsega	-
ART00083	The Current Sta	2017	Multiple Countr	MLT	AUT10010	AWA01	-	-
ART00086	The impact of ir	2008	Multiple Countr	MLT	AUT10123	Salifu	A.S	Adam
ART00094	West African Cy	2017	Multiple Countr	MLT	AUT10023	AWA14	-	-
ART00095	West African Sc	2016	Multiple Countr	MLT	AUT10084	Lemos	Robert	-

Qn5 Screenshot: (Terminated deliberately at Lesotho, just to emphasize)

Country	Country_Name	Crime_Num	Crime_Name	Crime_Targets	Other_Notor	Other_NotoriousC	Other_NotoriousCrime	Other_Notoriou
AGL	Angola	CRM1043	Identity Theft	Any Users Identity, Social	Cyber Espionage	Identity Theft	General	Money Laundering
ALG	Algeria	CRM1029	Dexter	Windows PCs	Hacking	General	Identity Theft	-
BEN	Benin	CRM1060	Romance Scam	Dating and Video Chat Site	Advance Fee Fra	Account Takeover	Romance Scams	Cyber Bullying
BKF	Burkina Faso	CRM1020	Cyber_Terrorism	Political Groups, Governm	Romance Scam	General	-	-
BRD	Burundi	CRM1043	Identity Theft	Any Users Identity, Social	Credit Cards ID	Piracy	General	-
BWN	Botswana	CRM1055	Phishing	Anyone Responder - Corp	Malware	Cyber Espionage	Social Media Crime	-
CAR	Central African Republic	CRM1040	General	Political Leaders, SA Econ	Institutional Cyb	-	-	-
CBV	Cabo Verde	CRM1055	Phishing	Anyone Responder - Corp	Economic Crime	Distributed Denial of	-	-
CGO	Congo Republic	CRM1043	Identity Theft	Any Users Identity, Social	E_Commerce	Simbox Fraud	-	-
CHD	Chad	CRM1043	Identity Theft	Any Users Identity, Social	E_Commerce	-	-	-
CMR	Cameroon	CRM1002	Advance Fee Fra	Any Individuals	Embezzlement	Romance Scam	Hacking	-
CMS	Comoros	CRM0000	Data Unavailabl	Not Available	-	-	-	-
DBT	Djibouti	CRM1040	General	Political Leaders, SA Econ	-	-	-	-
DRC	DR Congo	CRM1042	Hacking	Computer Devices, Banks,	Social Media Cri	-	-	-
EGT	Egypt	CRM1043	Identity Theft	Any Users Identity, Social	Business Attack	Cyber Bullying	-	-
EQG	Equatorial Guinea	CRM1043	Identity Theft	Any Users Identity, Social	Institutional Cyb	-	-	-
ERT	Eritrea	CRM1034	Embezzlement	Businesses with Large Fina	-	-	-	-
ETP	Ethiopia	CRM1057	Pornography	SA citizens, Government si	Pornography	Scams	-	-
GBN	Gabon	CRM1042	Hacking	Computer Devices, Banks,	Identity Theft	Data Theft	-	-
GBU	Guinea-Bissau	CRM0000	Data Unavailabl	Not Available	-	-	-	-
GHN	Ghana	CRM1011	Credit Cards ID	Individuals, Small and Mec	Advance Fee Fra	General	Romance Scams	Sakawa
GMB	Gambia	CRM1011	Credit Cards ID	Individuals, Small and Mec	General	Pornography	Telecommunication Fraud	-
GUN	Guinea	CRM1033	E_commerce Ha	Businesses	Spam	Hacking	Internet Fraud	-
IVC	Côte d'Ivoire	CRM1044	Internet Crime	Government, Social Media	Phishing	Website Defacement	Botnet	-
KNY	Kenya	CRM1044	Internet Crime	Government, Social Media	Cyber Threats	Phishing	-	-
LBR	Liberia	CRM1036	Encryption Serv	Secure Encrypted Content	General	-	-	-
LBY	Libya	CRM1050	Malware	Computer Systems	Phishing	Internet Fraud	-	-
LST	Lesotho	CRM1040	General	Political Leaders, SA Econ	Social Media Cri	Cyber Threats	Credit Card ID Theft	-

5. Discussion

Through this work, we discovered several emerging cyber threats from the many nations of Africa. The most common include: **a)** Bogus Cashier's Check; that is, when the victim advertises an item for sale on the Internet, and the criminal buyer issues a bogus cashier's check, carting away the merchandise before the dud check is discovered to be bogus (Adebusuyi, 2008). **b)** Online Charity Scam; where cyber perpetrators will set up a website that appears like a charity organization soliciting cash or credit card donations when in fact, such organization does not even exit. Many unsuspecting people have been exploited through this cybercrime method (Adebusuyi, 2008) (Trends", 2016) **c)** Beneficiary of a will Scam; where the criminal sends out an e-mail to claim that the victim is named as the beneficiary in the will of an estranged or dead relative and stands to inherit an estate worth millions (Adebusuyi, 2008) (Olumide, 2009). **d)** The "Winning Ticket in Lottery you never entered" Scam; even the Department of State Green Card lottery program has been reportedly featured in this crime type. (Oliver, 2010) (Adebusuyi, 2008). **f)** Next of Kin Scam: Collection of money and transfer fees from various banks by tempting the victim to claim an inheritance of millions of dollars in an African bank belonging to a lost relative (Oliver, 2010) (Olumide, 2009). **g)** Lottery scam; a method that allow targeted victim to believe they are the benefactors of an online lottery that is in fact a bogus scheme (Adebusuyi, 2008) (Olumide, 2009). **h)** Computer/Internet Service Time Theft; is a method where cyber criminals develop means to connect Cyber Café operators to the Network of some ISP provider in an ingenious way that is hard to detect and thus allowing the Cybercafé to continue operating at zero cost (Okonigene, 2009) (Trends", 2016).

6. Africa Cybercrime Challenges

Several studies examined in this project were of the opinion that the inability to effectively police criminal activities on the Internet is a principal reason why cybercrime is on the increase and will continue to rise in Africa. The articles also gave several additional reasons for the upsurge of e-crime perpetrators that include the following:

A) Ineffective Domestic and International Policing and Law enforcement: A perpetrator residing thousands of miles away somewhere in Africa with good Internet access can potentially attack innocent users anywhere in the world as if they were next door. The perpetrators are difficult to track and prosecute across International borders, and with differences in laws for each country, prosecution can be very problematic (Trends", 2016) (Okonigene, 2009). **B)** High Poverty Index: On the global scale, many African Countries are regarded as third world economies with rising poverty rates. With widening gaps between the rich, insufficient infrastructure, little cottage or small industry to sustain the poor, poverty rate continues to be a reason for taking to crimes (Okonigene, 2009) (Olumide, 2009). **C)** Corruption: Most African countries are notorious for high level of corruption. When the leaders are severely corrupt, the tendency for citizens to be corrupt is also high. This is sometimes seen as a way of life. This ultimately leads to citizens taken to online crimes. Nigeria, for example, has often been rated as one of the most corrupt nation in the world, according to various articles. (Adebusuyi, 2008) (Okonigene, 2009) (Trends", 2016). **D)** Limited Standards and Legislations: Studies have shown that lack of regulations or meaningful standards on computer security and protection are true enemies of true e-business in Africa. (Oliver, 2010) **E)** Low Industrial Output and High unemployment: When compared with most developed economies of the world, there are too few major industries in Africa providing the badly needed jobs for the teeming young population. The spate of unemployment in most African nations have been concerning for a while and growing. With companies declaring bankruptcy and liquidating businesses daily, the economic situation remains grim and dire indeed. The consequence is more of the citizens taking to e-Crimes to survive (Trends", 2016).

Finally, the end product of this project was the creation of a data repository to store data available on the African Cybercrime threats. Using Microsoft Access, this database was created, tested, and working for the most parts. However, there were several limitations. Going forward, the plan is to migrate this to a more powerful database management software driven by Artificial Intelligence (AI), and Machine learning (ML) technologies. Such platform will be capable of forecasting and predicting the possibility of, and occurrence of future attacks as well as providing measures that can help prevent such attack.

Additional plan is to continue gathering more data from more secondary data sources looking for additional cybercrime signatures that can be ported into the existing database. This project will continue to be carried forward at our home base (Norfolk State University, NSU) where some students would be invited to participate as a future project work.

7. Conclusion

This project gave us the opportunity to conceive and develop a data repository to capture the existential cybersecurity threats from the African continent. The basic database was

developed and met the basic requirements of this project. We discovered that Africa has a young population that is growing rapidly and adapting to new technologies manufactured and imported from America, Europe, and Asia. The Internet boom that has taken the world by storm and has not excluded Africa. African countries, it seems, will continue to make giant strides into electronic commerce and thus creating more opportunities for cybercriminals with cybersecurity implications and challenges for law enforcements worldwide. This study has revealed the need for African country governments to redouble their efforts in the prevention of cybercriminal activities. They must stay focused and rather urgently, address the rapidly growing cybersecurity challenges on the continent in collaboration with other continents. Doing so will drastically begin to improve the continent's perceived weak cyber security infrastructure, negative image and posture. The general believe is that the cyber security threat landscape from Africa will continue to increase at worrying pace with victims being impacted by threats that are currently trending globally as well as the notorious crimes that are specific to each sub-Saharan African region. However, concerted efforts from international bodies including law enforcements, the Interpol, governments, industry, and civil society organizations would be required to fight the specific African cybercrimes and help improve the global cyber security battle. Doing so will ensure that sub-Saharan Africa reaches its full potential in the comity of nations, using technology wisely and productively, and stay on the trajectory to becoming a major player in the global economic landscape.

REFERENCES

"FBI, D. R. (2016). *FBI, DHS Release Report on Russia Hacking.* Retrieved August 2017, from "The Hill" on Line: http://thehill.com/policy/national-security/312132- fbi-dhs-release-report-on-russia-hacking

Adebusuyi, A. (2008, July-December). Nigeria Ranks 3rd in Cyber Crimes Rating Globally. *International Journal of Cyber Criminology, 2*(2), 368-381. Retrieved July 2017, from Nigeria ranks 3rd in cyber crimes rating globally

Anderson, R. e. (2012). Measuring the cost of Cybercrime. *11th Workshop on the Economics of Information Security.* Retrieved August 2017, from http://weis2012.econinfosec.org/papers/Anderson_ WEIS2012.pdf

ECEG, 2. (2015). e-Government Proceedings 2015. *Proceedings of the 15th European Conference on e-Government, ECEG 2015.* Retrieved August 2017, from https://books.google.com/books?id=ri47CgAAQBAJ &pg=PA115&dq=Nigerian+cyber+security+threats & hl=en&sa=X&ved=0ahUKEwii0M7F6ujRAhXCYS YKHbKsDV8Q6AEISDAE#v=onepage&q=Nigerian%20cyber%20security%20threats&f=false

Houston, J. (1998). *Secondary Analysis of Qualitative Data.* Surrey, United Kingdom: University of Surrey Press. Retrieved August 2017

Johnston, M. (2014). Secondary Data Analysis: A Method of Which Time Has Come. *Qualitative and Quantitative Methods in Libraries, 3*(1), 619-626. Retrieved August 2017

Okonigene, R. A. (2009). Cybercrime in Nigeria. *Business Intelligence Journal*. Retrieved Auguast 2017, from http://www.saycocorporativo.com/saycoUK/BIJ/jour nal/Vol3No1/Article_7.pdf

Oliver, E. (2010, November). Nigeria: Cybersecurity Issues. *International Journal of Cognitive Research in Science, Engineering, and Education.* Retrieved August 2017

Olumide, R. V. (2009, May). E-Crime in Nigeria: Ternds, tricks, and Teratment. *The Pacific Journal of Science and Technology., 11*(1). Retrieved July 2017

Trends", C. (2016, November). CyberCrime and Cyber Security Trends in Africa. Retrieved July 2017,

from https://www.symantec.com/content/dam/symantec/docs/reports/cyber-security-trends-report-africa-interactive-en.pdf

Valacich, J. S. (2003). *Information Systems Today - Managing in the Digital World.* New Jersey: Prentice Hall. Retrieved July 2017