European Journal of Computer Science and Information Technology
Vol.7, No.2, Pp.36-47, April 2019
Published By European Centre For Research Training And Development UK (www.eajournals.org)

THE ROLE OF CYBER SECURITY IN MINIMIZING CRIME RATE IN POSTWAR SIERRA LEONE

Ibrahim Abdulai Sawaneh

Director of Academic Affairs, Institute of Advanced Management and Technology (IAMTECH), Freetown - Sierra Leone

ABSTRACT: *There are numerous benefits one can get from using technological innovations ranging from comfort to minimal cost in telecommunications, health, aviation, commerce, energy, agriculture, intelligence, education via Internet and Internet of things (IoT). However, criminals have over the past decade accelerated highly sophisticated techniques to steal billions of sensitive and costly data either from private individuals, government or corporations costing billions of US dollars globally. Therefore, the research provides awareness as to how these Cybercrimes can be mitigated especially within the scope of Sierra Leone. It largely focuses on the establishment of the Cybercrime Unit at the Central Intelligence Department (CID), and the Office of the National Security (ONS), both units was created by an act of Parliament to secure and protect citizens against imminent cyber criminals within the confirmed of Sierra Leone. These agencies has been able to solve some of the crimes issues but yet still there exist unsolved problems. This is because of lack of many indigenous cyber security experts in the country. Also, the study indicated that the laws governing Cybercrimes are too weak to be able to tackle all the numerous issues relating the internet crime.*

KEY WORDS: Cyber Security Crime, Crime Rate, Postwar, Sierra Leone

INTRODUCTION

The essential increase in information and communication technology and its constituents is alarming in regard to the how it is managed especially developing countries such as Sierra Leone. The Sierra Leone Government enacted the Office of National Security (ONS) by an act of Parliament in 2002. Since the end of the civil fought in between 1991 to 2001, Sierra Leone has gradually experience security threats with huge challenges especially the Internet and other related domains. The objective of this thesis is to help the office of national security, the ministry of information, and other IT reputable institutions in Sierra Leone due to the transformative growth in the communication industries, help implement the government strategies relating to ICT policies serving as tool for cyberspace defense strategy. Subsequently, cyberspace defense system is centered on a single model for countries with established structures. Sierra Leone as an emerging nation with weak IT infrastructures faces many challenges in building state of the art cyberspace defense system though the office of national security has been created by the Sierra Leone Parliament to handle such challenges and threats. ICT Policy makers, such as the of office of national security (ONS), Sierra Leone ministry of information, Sierra Leone national telecommunication (NATCOM), HAFCOM, etc. viewed the current regulation as not viable, because the existing structures do not reflects the current needs of the state. The thesis is geared

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

towards providing best practice that tackles countries with developing internet structures to detect the key challenges faced by the existing structures, which includes affordability of required gadgets, and availability of trained cyber security personnel. Moreover, the challenges faced by Sierra Leone in the area of internet security relating to cyber defense practice is imminently different from other nations which is based on either the geographical location, or other factors.

The utilization of the internet has both merits and demerits depending on the intention of the user. E-commerce, E-shopping, E-learning, E-health, E-communication, E-business, E-sport, E-transportation (VARNET) and others have transformed people's lives greatly making life comfortable thereby improving on the life expectancy. These improvements are as a result of Internet technology with countless valuable benefits.

Notwithstanding, the creative innovations in the internet industries in the 21st century has created several advantages and disadvantages especially the disadvantages for hackers and malicious users to create havoc to both private and public sectors. Even countries thought in the past to be well equipped technologically are now vulnerable to these threats and challenges as seen in the United States 2016 Election and the WANA CRY crisis in some part of Europe and Russia. This is possible because of the intervention of several software platforms that target governments and financial institutions around the world.

Cyber – attacks nowadays are great weapon used against both industrialized and developing nations. The probable mischief by attackers can raise a potential security threats to a national security of all countries. Essentially, it deters the economic growth of developing countries (Sierra Leone). Most developing nations welcome the idea of using the Internet but failed to prepare well for the cyberspace. This is a result of poor knowledge in the cyberspace warfare faced by all nations around the globe.

Unfortunately, the utilization of such technology without providing solutions to the imminent challenges will make any country defense system vulnerable thereby letting malicious users creating havoc and mayhem to the natural resources. Therefore, this research is aim at providing some solutions needed to mitigate the plight of all stakeholders at both government and private sectors as cyberspace is becoming hard to control day by day.

Monitoring and securing the cyberspace such as the ICT industries is vital for any nation security defense system because of the international consequence of cyber uncertainty in today's competitive global stage. Internet is a borderless globally connected network empowering hackers inflicting endless mayhems to nations with weak ICT infrastructures via computer technology in launching attacks, making them stay unidentified using virtual private networks. Internet use demands all countries to effectively design and implement cyber security guidelines and policies that renders safe and efficient secure Internet platform crucial not only to undeveloped nations but also industrialized nations.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Several government agencies such as the FIB, CIA, MI-6, Interpol, KGBI, and others have continually developed and implemented strict policies regarding Internet usage. The United Nations produced a resolution mandating the International Telecommunications Union (ITU), a UN agency, to spearhead an effort at spreading a culture of cyber security. The ITU implemented the globally conventional conceptualization on how to tackle the insecurity posed by cyber security. This mean that, there should be a universal formula to respond to cyber-attack that all nations should adopt and follow as was seen in the Johannesburg resolution, which recommended that all nations establish a national CERT to combat the cyber security problems of nations.

The Johannesburg resolution, a strategy-based on how industrialize nations react to these threats which is evident by the United States seeing the resolution as not well defined. Hacker or attackers all over the world produce new security threats every day and to deal with such threats requires huge money in relation to training of cyber personnel and cost of modern equipment. The research uses data got from the office of the national security, ministry of information and other tech industries, which interact with both private and public sectors thereby enabling secure cyberspace that caters for the wellbeing of the nation economically and defensively.

Problem Statement

Criminals who hijack computers, mobile phones, and other computing devices with viruses and malware do cyber-crimes. Smart-phone serves as a platform were people are targeted as a victim to cyber-crime. More than 5.4 million Internet users were under attack either knowingly or unknowingly by online criminals for the past months, as indicated by Norton's annual Cyber-crime report. Hackers leading to security threats compromise numerous vulnerabilities in Smart-phone applications. A simple game download with a click provides substantial information about the use's activities with phone to a cyber-criminal.

Survey suggests that about forty percent (40%) of mobiles sold globally in 2012 were Smart-phones. It serves as a platform for cyber criminals with them gaining access to person's computer, e-mails, and social media. It is imminent that the world will be faced by numerous cyber attacks especially through smart-phones as reported by world leading cyber security analysts.

Mobile applications are a cutting edge for cyber-crimes around the globe. The applicability and usage of mobile devices exponentially increases day-by-day and it users also increases more than half of the world population. Mobile applications, or mobile apps, known as software are designed to be used on smart-phone, tablets and other ubiquitous mobile devices that enhances and make life comfortable. The rapid usage of mobile devices result to several schemes by hackers to expunged valuable information from its users amounting to millions of US dollars annually.

Erhabor (2008), described Cybercrimes as one of the highest emerging criminal tricks globally. These tricks involve numerous unauthorized activities such as financial crimes, virus attacks, pornographic download, false ideology and recruitment of jihadists, hacking, etc. via the

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Internet. For the past three years, students have extensively engaged in examinations malpractices through mobile phones at the senior secondary school level forcing the West African Examination Council (WAEC) to seized student results in Sierra Leone. Ajao (2008) indicated that Nigeria, Ghana and South Africa are the most vulnerable countries relating to Cybercrimes. Personal computers Apps store serves are used as a platform for downloading software, while mobile apps serve as programs that are downloaded onto our mobile gadgets. Downloading such applications from app stores may result to downloading malware and viruses. This is due to the fact that mobile apps are now the new frontier for security threats. Malicious software (Malware) has become the newest tool used by cyber-criminals. The ignorance in downloading applications especially un-trusted sites poses serous security concerns. The research findings indicated above will help to mitigate cybercrime and cyber security rates in Sierra Leone.

General Analysis

Cyber Security is an essential ingredient of the Internet revolution where user is liable to derive positive or negative results. Cyber security is seen as the combination of several technologies, processes and / or practices done to safeguard computer networks, computer programs and sensitive data from possible attack, destruction or unlawful access. One can also define it as a method that detects and prevents unauthorized use of ones data. Data invaders known as intruders or hackers with malicious intentions are prevented/restricted to gain access of ones data illogically. The process of detection confirms whether an unauthorized entities has breached into your computer networks or systems you want to design whether or not someone tried to break into your system, if it was successful or not. Therefore several governments around the world have increased the financial spending on defensive purpose. For instance, the U.S federal government allotted over $13 billion in December 2010 in the fight against cyber security threats for five years which has double in 2017 due to the Russian interference in the 2016 elections. Furthermore, most industrialized nations have increased their military budgets such as the People's Republic of China, U.S, France, Britain, Russian and some African countries like Nigeria, Ghana, and South Africa.

Moreover securing the on the Internet requires effective and supervised information system known as the key factors of the cyber security framework:

- Application security
- Information security
- Network security
- Disaster recovery

Application security relate to the utilization of software and hardware with a systematic schemes aimed at protecting computer applications from both internal and external threats. Security patches are built into applications to reduce the possibility of unauthorized users to

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

manipulate the applications in order to gain illegal access with the intention to manipulate, disrupt, steal, or delete sensitive data. (B., 2012).

Information security is the act of securing sensitive data and information systems from illegal access, utilization, leak, interference, alteration, assessment, safeguarding of data storage or damage. Donn Parker in 2002 analyzed an optional method for the classic CIA term (Confidentiality, Integrity and Availability) known as the six atomic elements of information. They include confidentiality, ownership, integrity, validity, availability and service.

Networking been an integral component of the internet infrastructures is usually managed by network administrator of system administrator implementing effective internet security parameters, software and hardware to shield a network and its resources from unlawful utilization and ensures that authoritative clients are permitted full access to the system and its resources at all time without interruptions from third parties.

A disaster recovery plan (DRP) is a systematic procedure on how institutions manage possible disasters. Disaster recovery plan encompasses business processes and continuity needs; also it includes momentous concentration on disaster prevention and ensures that being proactive is essential to organizational continuity than being reactive. Disaster recovery is more and more a vital aspect of enterprise computing. Gadgets, systems, and networks are becoming more intricate, and possibly negative impacts on societies and individuals. As a consequence, preventive measures also becoming more difficult. (c5franey, 2011).

Research Objectives

The principal objective of the research is to investigate and suggest important security parameters relating to Cybercrimes and cyber security to the government of Sierra Leone for possible implementation. The authors hope that the Parliamentarians will review the old act on security matters and strengthen it to meet the present demands of the society's security dilemmas. Enforcing rigid laws through the security apparatus will help to mitigate the numerous crimes associated with internet fraudsters and perpetrators to justice.

The specific objectives are as follows:

1. To diagnosis and detect the various techniques used by the cyber criminals in Sierra Leone.
2. To create awareness on the essence and curiosity with regards to cybercrimes and cyber security challenges in Sierra Leone.
3. To investigate the parameters used by the cyber security unit of the Criminal Investigation Department (CID) and the Office of the national Security (ONS) in fighting cybercrimes and to provide a secured environment that will boost the developmental trend of the new government agenda in fighting corruption.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Research Questions

The essential and most vital aspect of the research is how one can minimize cybercrime rate in this emerging and developing postwar toured country with poor cyber security infrastructural and less trained cyber professionals. It try to solve he numerous security challenges:

1. How the CID and ONS deal with cybercrime and cyber security pressure?
2. How honestly and effectively are these units trying to solve cybercrime and cyber security issues in Sierra Leone?
3. How to enhance cybercrime and cyber security in Sierra Leone?

METHODOLOGY

The research deploys a mixed scheme o investigates and renders possible solutions to the numerous challenges faced by the cyber ecosystem in Sierra Leone. It utilizes the theoretical and investigative approaches with mixture of existing literatures along with questionnaires serving as the primary source, internet and textbooks serving as the secondary source. The two departments CID and ONS were targeted in providing the primary source of data for the said research.

Current Information

The ultimate goal of this research is to assess the role of cyber security in minimizing crime rate in postwar Sierra Leone. The emergence of advanced Internet technologies in postwar Sierra Leone has both positive and negative effects. Sierra Leone is a virgin land with little or poor Internet infrastructures attracting several hackers invading both private and public sectors. Most of the financial institutions and government departments have been invaded on the years. Privacy and data security is an essential factor in maintaining and protecting the cyberspace. Several government institutions have unlawfully have terminated the services of its employees because of the above factors.

Cyber security is an essential tool that will help minimize crime rate in Sierra Leone. A large people in Sierra Leone have been affected by cyber-attacks, but they have little acknowledge it effects. For instance several stakeholders mostly politicians have had their characters assassinated using social medium without been catch by the security apparatus. Also, mobile theft is another major problems faced by country's population. Notwithstanding, robbers are in the habit to surveillance the social media such as Face book, Tweeter, etc. for people who post their vacations publicly and subsequently break into their homes and steal while they are away.

The research is therefore aim at helping the Office of National Security (ONS) and the Criminal Investigation Department (CID) to track people who misused such platforms and bring them to book subsequently helping minimize or eradicating crime rate in this postwar country.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

The research reviewed scholarly and intellectual exodus. Which includes books, articles, journals, periodicals, PhD thesis and Dissertations that are related to the research topic in order to clear the lens of understanding of the said topic in the minds of any potential use of this work.

DISCUSSIONS

Cybercrimes are more prevalence nowadays due to the advancement of creative and innovative degrees of success on social networks because it easier access to invade users via scams. Mobile and computer devices on social networking platforms are more liable to cyber attacks because mobile users continue to increase by - by - day. The establishment of online trading in Sierra Leone with poor infrastructure is a major concern as cyber criminals are inspires to steal user's account details. They normally incorporate malicious malware that steal large quantities of individual data, as most users do not install anti-virus software on their mobile and computing devices in most developing countries, even while using their Smartphone's to do e-banking. Most social networking platforms such as Face book, Twitter, My space, We chat, QQ International, What Sapp, Vibe, WowApps, and other are prone to attack in developing nation like Sierra Leone as people have little awareness of Cybercrimes' activities and people most time only look at the positive side been connected to the wider world. Furthermore, most of PCs user in Sierra Leone often click on links in spam messages that spread virus to the entire system and subsequently steal sensitive data that has high monetary value. Facebook is major platform where fake news are been channeled as evident from American president Donald Trump brutal attacks on several media outlets in the U.S. Several corporations and individuals have to pay money as a victim of Cybercrimes at different social media platforms as evident in the Ransoware in 2017 were several tech entities including both private and public sectors were force to pay in bit coins. People with little knowledge on social media vulnerability sometimes terminate and deactivate their social sites account after encountering such mayhem.

Several security threats via social networks are in an alarming state in recent years around the globe and to specific Sierra Leone.

- In Sierra Leone, there have been several attacks from social networks from 2014 to date. For instance, a house was vandalized in Freetown because the family posted their vacation on Facebook that prompted thieves to raid the house whilst they were enjoying their vacation abroad.
- In 2017 to date, people are in the habit to blackmail and tarnish ones character on social media especially politicians who siphoned the country's wealth to the outside world.
- In 2017, Ransoware in the U.S, UK, and France hit several entities, and Russia by a group of hackers believed to have a link with North Korea.
- The US was also hit with Koobface infections and other social network attacks which increased from 8% in 2009 to 13% in 2010 to 18% in 2011.
- The United Kingdom experienced several attacks on their social networks from 6% in 2009 to 12% in 2010 to 15% in 2011.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Countermeasures

- Utilization of genuine anti-virus software from trustworthy source that is regularly updated.
- Using an updated OS renders or solves some security vulnerabilities.
- Using strong passwords helps protect personal information from fraudsters.
- Changing passwords regularly and rendering secrecy is essential.
- Avoiding placing your personal details on the Internet.
- Do not disclose your bank details to unknown entities.
- Never click on a links contained within spam or unexpected emails.

Common security dilemmas affecting cyber security departments in Sierra Leone

Some of the issues that affect the operations of state security apparatus in combating cybercrimes in Sierra Leone are as follows:

1. Inadequate legislature on the policies relating to cybercrimes and cyber security posed by the growing technological innovations. This is because of lack of adequate knowledge on these matters by the country's legislature body hindering the security apparatus with little power to prosecute defaulters in the court of law.
2. The inability to establish a national internet gateway that monitors and report online criminals to the state security forces in Sierra Leone.
3. The inadequate training facilities provided to the state security forces on how to manage and maintain effective cyber security policies that make Sierra Leone a better place to live and invest. Government officials over the years have extensively engaged in siphoning the country's wealth with state banks serving as medium of such transactions to other part of the world.
4. The non-existent of a national automated database that keep records of cyber criminals in the country. With such database, people seeking for employment and political positions within the country are screened properly before such opportunity is granted to them. This will save the country with lot of money falling into the hands of rouge criminals. T
5. Lack of trained and qualified cybercrime experts within the CID and ONS departments to routinely monitor and investigate such act. Unfortunately, most officials in the state security departments are computer illiterates and the absence of state-of-the-act forensic laboratories to investigate and analyze cybercrimes related problems in Sierra Leone.
6. The absence of national database infrastructure that records and publish cybercrime report annually in Sierra Leone.
7. Enforcement of legislature that stop the interference of politicians in prosecuting cybercrime activities in Sierra Leone.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

CONCLUSIONS

The continuous innovations with numerous opportunities rendered by technology has also got it reversed consequence, as the saying goes, every have two sides either a head or a tail. This is most evident due to the advent of big data technology, cloud computing, automation and Internet of Things (IoT). We have seen series of wave in cyber attacks, state sponsored espionage scheme, cyber warfare, and cyber crimes. Therefore, nations around the world today are concern about how to secure and protect their national data, either military or economically. Most powerful nations perform series of espionage either through foreign aid or multi-national companies. Others to maintain their supremacy in the name of controlling the world have adverted to cyber warfare in this competitive information age.

Furthermore, the world have faced numerous attacks such as botnets, ransomware, cyber warfare, identity theft, data breached, Elections meddling, etc. The scope of this study is restricted to the Sierra Leone in ensuring that all the numerous security challenges in relation to cyber crimes, cyber attacks, cyber warfare, identity theft, and other forms of electronic crimes are dealt with in accordance to the laws of Sierra Leone. This will technically provides secure environment that is conducive for businesses and enhance government organs to function correctly. The use of CCTV cameras in certain quarters of both government and private entities have minimize crime rate and perpetrators being brought to justice the ONS and CID departments. Importantly, to reduce Cybercrimes rate demands effective cooperation with neighboring countries such as Republic of Liberia and Republic of Guinea, high quality education among Internet users will also help create awareness on the preventive measures that will definitely minimize the various crimes associated with online activities. The other major issues is the compliance with privacy and security as most telecommunication companies in third world countries breached peoples privacy, because there are no strong laws to defend such act. Lastly, cyber security should be part of all information systems and electronic system within the country. Also, the government should ensure that active firewalls and other preventive applications and measures are designed to protect the citizens' information. Cyber security is therefore the order of the day where hackers get huge amount of monies illegally that needs to mitigated or even eradicated completely.

Recommendation

Cybercrimes and poor cyber security policies hidden the growth of any nation economically, politically, stability and security. Therefore, a though and effective policies and preventive methods are the ultimate solutions to the wave of cybercrimes in Sierra Leone and the world at large. The authors therefore recommend the following as solutions to the several challenges perpetrated in the cyber ecosystem in Sierra Leone:

1. The existing laws on national security should be reviewed to incorporate laws relating to Cybercrimes and cyber security threats as the existed one is old fashioned.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

2. The cybercrime unit of the Criminal Investigation Department should be enhanced with Forensic laboratories facility for examining Cybercrimes.
3. Continuous staff capacity training programs internally or externally is necessary to broaden their expertise in tackling cyber criminals.
4. The government of Sierra Leone should be proactive in monitoring the activities internet service providers and the mobile telecommunication companies to ensure mobile users details are registered to each subscriber's account. SIM cards should not be issued without taking the proper information from the users such as full name, residential and email addresses, occupation, etc.
5. A nationwide security framework with the state-of-the-art cyber security platform established with rigorous requirement control measures with the aim to minimize cybercrime rate in Sierra Leone.
6. Implementation strict policies that promote the awareness on how cybercrimes hinder development all facet of societies.
7. The Anti Corruption Commission (ACC) should prosecute any cyber criminals and levy huge amount of fines or shaming people publicly for committing cybercrimes in Sierra Leone. Moreover, to effectively minimize corruption in Sierra Leone requires the government to automate all systems at its various departments. Corruption is the most disgusting element that destroys any nations' developmental achievements, rendering a country broke.
8. Laws should be enacted in the Sierra Leone House of parliament to prohibit students taking mobile phones to examination halls, thereby curtailing examination malpractices and increase high quality education in Sierra Leone.
9. It is a common trend of most social media users posting vital information online with the aim of showing off to the general public. Therefore, sensitization should be carried out to stop such behaviors as valuable information that endanger or compromise their privacy and security by internet fraudsters is increasing.
10. Finally, the government of Sierra Leone should be proactive rather than reactive in destroying the root cause of corrupt practices especially top government officials stealing the country wealth and siphoned it to other country for safe heaven. Using state-of-the-art software to track banks and people involved in this act is one of the lasting solution that will save millions of Leones for that can be used to development the country economically and financially.

Future Work

Due to the restriction made in interviewing the cyber criminals at the national headquarters of the Criminal Investigation Department Cybercrime unit subsequently narrow our research. Therefore, The researchers recommend that in order to get the root courses to cybercrimes, authorities should grant future researcher (s) the opportunity to interview both the culprits and the victims. Furthermore, the government should impose heavy fine to any telecommunication companies failing to create a comprehensive database for all their subscribers, so that the cyber criminals can be easily tracked via their mobile phone numbers, social media accounts, and email etc.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Finally, the authors further recommend that extensive study should be done into the demographic and social individuality of cyber criminals in Sierra Leone thereby examining the factors that influence perpetuators to commit cybercrime.

References

Eriksson, Johan & Giacomello, Giampiero (2006), *The Information Revolution, Security, and International Relations: (IR) relevant Theory?* International Political Science Review vol. 27: 221-244

Compete site comparison. http://siteanalytics.compete.com/ facebook.com+myspace.com+twitter.com/

C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. Voelker, and S. Savage. Show Me the Money: Characterizing Spam-advertised Revenue. *USENIX Security Symposium*, 2011.

B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kem- merer, C. Kruegel, and G. Vigna. Your Botnet is My Botnet: Analysis of a Bot- net Takeover. In *ACM Conference on Computer and Communications Security (CCS)*, 2009.

B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Econ- omy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2011.

N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose. All your iFRAMEs point to Us. In *USENIX Security Symposium*, 2008.

C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: the underground on 140 characters or less. In *ACM Conference on Computer and Communications Security (CCS)*, 2010.

K.Thomas,D. McCoy, C. Grier, A. Kolcz, and V. Paxson. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *USENIX Security Symposium*, 2013.

Buzan, B. & Hansen, L. (2009), *The Evolution of International Security Studies*, Cambridge University Press, Cambridge Trends in World Military Expenditure, 2017" (PDF). Stockholm International Peace Research Institute. Retrieved 2 May 2018.

"Data for all countries from 1988–2017 in constant (2016) USD (pdf)" (PDF). SIPRI. Retrieved 2 May 2018.

Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Dunn, M. (2003), Securing the Digital Age. *In Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security,* ed. Robert Latham. New York: The New Press, 85-105.

c5franey. (2011). *Disaster Recovery Plan*. Retrieved March 21, 2012, from Study Mode: http://www.studymode.com/essays/Disaster-Recovery-Plan-809693.html

T. Jagatic, N. Johnson, M. Jakobsson, and T. Jagatif. Social phishing. *Commu- nications of the ACM*, 2007.

L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In *World Wide Web Conference (WWW)*, 2009.

G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna. The harvester, the botmaster, and the spammer: On the relations between the different actors in the spam landscape. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2014.

Lewis, James A. (2014). "National Perceptions of Cyber Threats". *Strategic Analysis*, Vol. 38, No. 4

Ibid., 567

Singer & Friedman, 39

Visit report, Sierra Leone Security and Intelligence Service Reform, September 1999.

Hart, Catherine (2011), *Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties*, Cyber-Surveillance in Everyday Life: An International Workshop, May 12-15, 2011, University of Toronto

Acknowledgments

The authors would like to acknowledge Mrs. Elizabeth Guma-Sawaneh for her extensive moral and financial supports in carrying out this research. Much thanks and appreciations go to Professor Paul Kamara, Dr. (Mrs.) Abie Paula Kamara, Dr. Michael N. Wundah and Dr. Umaru Peter Kamara from the Institute of Advanced Management and Technology (IAMTEH) for their tireless financial and technical support to young researchers nationwide.