International Journal of Intelligent Information Systems
2018; 7(3): 23-27
http://www.sciencepublishinggroup.com/j/ijiis
doi: 10.11648/j.ijiis.20180703.11
ISSN: 2328-7675 (Print); ISSN: 2328-7683 (Online)

Examining the Effects and Challenges of Cybercrime and Cyber Security Within the Cyberspace of Sierra Leone

Ibrahim Abdulai Sawaneh

Department of Computer Science, Institute of Advanced Management and Technology (IAMTECH), Freetown, Sierra Leone

Email address:
ciddiisawaneh@hotmail.com, ciddiisawaneh@yahoo.com

To cite this article:
Ibrahim Abdulai Sawaneh. Examining the Effects and Challenges of Cybercrime and Cyber Security Within the Cyberspace of Sierra Leone. *International Journal of Intelligent Information Systems.* Vol. 7, No. 3, 2018, pp. 23-27. doi: 10.11648/j.ijiis.20180703.11

Received: September 16, 2018; **Accepted**: September 29, 2018; **Published**: October DD, 2018

Abstract: The use of information is increasing everyday with the advent of more applications of social media platform that utilizes millions of data per second globally. These data include sensitive information such as trade secret, privacy and security issues. Most importantly, some organizations, both private and public use this medium to disseminate messages among colleagues especially in Africa. Also, the emergence of smart-phone has accelerated more problems with having little knowledge on security matters. Furthermore, cybercrimes use this opportunity to launch more cyber-attacks by invading people's privacy and steal sensitive information such as credit card details, online shopping information of customers, online ticket booking. Government official's details have being hacked or eavesdropped over the years when using their smart-phones for communications. Emails of prominent people have also being hacked or disrupted, causing huge financial lose. These attacks are on the increase and therefore, countermeasures are vital to combat cybercrimes and cyber warfare in this hostile cyberspace. The research study the sociological and technological issues that impact cybercrime and cyber-security within the boundary of Sierra Leone, as a national security threats. The study provides answers to the issues highlighted in the research. An extensive survey was conducted, which highlighted the need for a robust and proactive approach to mitigate the frequency on which cybercrime is carried out in the country and its neighbors. Data amassed were subjected to relevant questionnaires issued and collected from the respondents in the state security apparatus, based on the conventional approaches or methods of investing crime in Sierra Leone. The research shows that the state has weak laws regarding cybercrime and cyber security, and most people working in these departments or agencies have little knowledge in cyber security and cybercrime. In fact, most are on political appointment rather than on merit-base that supposed to be the right procedure that will accelerate and achieve the goals of these institutions.

Keywords: Cybercrime, Cyber Security, Internet of Thing

1. Introduction

The rapidity of informatization, big data technology, Internet of Things (IoT), and cloud computing innovation is a big concern for companies and government around the world. People with high-tech skills have turned to clandestine internet warfare through computers and computer related devices known as cybercrime to either amass riches or disrupt corporations or institutions around the world. Technology comes with merits and demerits depending on the intention the user have. In terms of its demit, people misuse these innovations meant to make life comfortable. People with the required talents perform certain criminal actions through the utilization of electronic devices via telecommunications is seen to be the new platform for cyber criminals to extort money and valuable information costing billions of US dollars annually. The escalation of criminal actions masquerade challenges for both legal systems and law enforcement units [1].

The Internet, a new stage of informatization has changed our ways from a text-book-based to internet-based, getting all our information needs from the Internet. This has resulted into a boom in the economics of individual nations with ease of reproduction. Additionally, the web and Computer network have played vital role in economics distribution and has exposed researchers to a greater opportunity. With more and more social media applications, with improved functionalities to handle both voice calls, video calls and

video conferencing with cheaper rate have energized majority of people to utilize these facilities. It is cost-effective and result oriented with lesser time.

To combat the escalating cybercrime in Sierra Leone especially after the bloody civil war that ended in 2002 is a dilemma for the security agencies. Most youths are without jobs and the only way for survival is crime, as one of the conduits through which cybercrime is conducted. The Sierra Leone Anti-Corruption Commission (ACC), the Office of the National Security (ONS), and the Cyber Security Unit (CSU) of the Sierra Leone Police Criminal Investigation Department (CID), and some international agencies have mitigated some of these cybercrimes. As most Internet users especially social media users, have little knowledge on security issues relating to their personal computers and smart-phones, they are easily tricked to disclose their personal data online and also the act of download from un-trusted sites. Unfortunately, Sierra Leone has got no legislation regarding cybercrime and cyber security, except the National Telecommunications Commission (NATCOM) who is mandated by the House of Parliament to handle national cyber security strategy, policy and roadmap.

1.1. Statement of the Problem

There are numerous benefits one can derive from the network of networks ranging from e-financial platform, e-health, e-learning, online facilities, and social media interaction. With all the opportunities offered by the Internet, yet there exist great challenges and threats due to the unauthorized activities called cybercrime and cyber security threats that are faced by Internet users in Sierra Leone.

The President of the Republic of Sierra Leone and his government are kin to eradicate or minimize corrupt practices by 2023 through ACC. Most corrupt practices in the country are being committed in the form of cybercrime. Cybercrime totally hinders any nation's development. This can be referenced to Aluko indicated that cybercrime abates corruption [3]. Cybercrime and cyber security are universal problems that have completely destabilized the smooth running of organizations or nations to achieve its full potentials. Series of cyber-attacks occurred spontaneously, globally and they accelerated cyber warfare involving nations to hack or eavesdrop individual government functionaries. According to the US elections in 2016, some senior government officials and presidential candidates' mobile phones were hacked including emails. The rise in new technological innovations such as smartphones, android phones, social media applications (Twitter, Whatsapp, Facebook, Skype), all of which run on both computers and mobile phones platforms. Lots of software on the Internet that aid people to perpetrate criminal activities using the network of networks called Internet.

Erhabor stated that cybercrimes as one of the rapidly increasing criminal platforms globally. Erhabor indicated that cybercrimes involve numerous activities such as Internet fraud, electronic and computer hacking, pornographic downloading, online scams, and hate speech on social media platform. Unfortunately, most students in Sierra Leone use social media platform on their mobile phones in order to involve in examination malpractices at the senior secondary school level. Also, lazy students have reverted to document forgery to unlawfully gain admission into colleges and universities in Africa. Awe indicated that Nigeria, Ghana and South Africa top cybercrime in Africa [5], of which Sierra Leone is no exception. To mitigate such issues, one has to be proactive in order to make Sierra Leone a safe nation to invest.

1.2. Research Objectives

The main objective of the work is to study the root causes of cybercrimes in Sierra Leone and provide an effective solution that can be debated in Parliament and enacted into laws that will help mitigate cybercrimes and legislate laws on both cybercrime and cyber security threats and challenges in this country.

Specific objectives of the research are:

To spot out the informal, sociological and technological root causes of cybercrime and cyber security in Sierra Leone.

To examine the various methods used by the Sierra Leone cyber security unit and the office of the national security in curbing internet crimes rate and enhance cyber security.

1.3. Research Question

The study is carried out in order to examine the vulnerability and weakness of cybercrime and cyber security in Sierra Leone. The research tries to solve the following questions:

How the cyber security unit of the Criminal Investigation Department and Office of the National Security remedy cybercrime and cyber security challenges and their threats?

How the Anti-Corruption Commission does sees cybercrime as one of the factor aiding corruption in Sierra Leone?

How do stakeholders sensitize and create awareness on the effect of cybercrime and cyber security enacted into laws in Sierra Leone?

What should be done to enhance and implement strong cyber security policies in Sierra Leone?

1.4. Research Methodology

This research uses both primary and secondary data from relevant sources on the internet and the agencies associated with cyber activities within Sierra Leone. Questionnaires designed were distributed to stakeholders of the Cyber Security Unit (CSU) in the Criminal Investigation Department (CID) of the Sierra Leone Police Force and Office of the National Security (OSN).

2. Related Works

The research utilizes several literatures as the spring boards to examine the root causes of cybercrimes in Sierra Leone. It is hard to define cybercrime because of the

activities that constitute a cybercrime have different dimensions [6]. Smith et al [7], referred to cybercrime as a conceptual complexities. Depending on the nature or medium through which a specific crime is perpetrated. It has got several nomenclatures such as computer crime, computer-related crime, digital crime, information technology crime [8], and Internet crime [9]. The introduction of fiber optic in Sierra Leone has enhanced Internet connectivity. Subudhi and Panigrahi published a research on telecommunication fraud using the features of a telephony communication as the input and Quarter- Sphere Support Vector Machine to differentiate fraudulent calls [10]. The input features include call duration, call type, call frequency, location and time, and it has achieved good recognition accuracy. They then in 2017 utilized a type of C-means clustering for telecommunication fraud detection. Again, a superb result was attained in [11]. Li et al. indicated in their work "telecommunication fraud detection" in which they adopted a machine-learning algorithm in detecting mischief calls [12].

2.1. Study Sample

The study population includes:

The cyber security unit at the criminal investigation department

The office of the national security (ONS)

The Anti-Corruption Commission (ACC)

Non-probability sampling scheme was applied, as the research focus was the state security apparatus and legislators in the field of cyber security sectors.

2.2. Sample Size

The sample sizes contained involved in the research are:

2.3. The Cyber Security Unit at the Criminal Investigation Department

This was created recently in order to combat the rising cybercrimes. It is the leading cybercrime unit within the security forces that tracks down cyber criminals and bring them to justice. Though this unit has greatly set the pace to enhance Internet security issues, but yet still, there exists huge tasks due to the advert of big data, informatization, cloud computing and Internet of Things. There is no sophisticated forensic laboratory to investigate such crimes. Most often, they use the traditional approach of investigations.

2.4. Office of the National Security

The unit was enacted by the Sierra Leone House of Parliament in 2002 and became the first department to monitor and investigate cybercrime and cyber security threats in the country. It's mandates go beyond cyberspace, but include all security issues of the state.

2.5. The Anti-Corruption Commission

The Sierra Leone Anti-Corruption Commission (ACC) came into existence immediately after the bloody civil in 2002. It mandates are to investigate and bring to justice all perpetuators who steal the nation's wealth. It was effective from 2002 to 2007 but became dormant from 2007 to 2017. Its working with those agencies or departments will reduce the poverty level in the country.

2.6. Survey Sample

The following survey questionnaires were extracted from a doctoral thesis titled "The Role of Cyber Security in Minimizing Crime Rate in Postwar Sierra Leone".

How does the Sierra Leone cyber security unit identify cybercrime threats?

Which techniques apply in acquiring evidence for cybercrime prosecution?

What authorized instruments are obtainable in the Criminal Law of Sierra Leone to address internet crime?

How do institutions in the country ensure cyber security is achieved?

Is there any backup policy for recording sensitive state documentation in place?

What security challenges do institution face in Sierra Leone?

Is there any pre-requisite qualification for key positions within the state security forces?

Do you perceive positive results against cybercrime?

Are there any recent cybercrime cases in Sierra Leone that demonstrate the importance of having laws against such cybercrime?

What is the insight on the common awareness of cybercrime and cyber security in Sierra Leone?

Does the government provide enhanced training on cyber security either internally or externally?

How often is security-testing procedure done in the country?

How often is data collected?

Is there any life insurance policy in place?

Does the agency or department have any CCTV cameras installed to properly monitor the activities of staff, if yes how?

3. Result

The result of the research shows that the public now has awareness on cyber security and cybercrimes, and it consequences. Also, key stakeholders in the Information Ministry, and the state security forces including, the police, military, city council police, immigration officers, prison officer and parliamentarians are pushing the central government to enact a stronger laws on cyber security and cybercrime in Sierra Leone. Furthermore, intensive seminars and workshops are now conducted to create more awareness on how to proactively react to cybercrime challenges and threats, and a testing forensic laboratory has been established.

4. Discussion

4.1. Manpower Development

There is not a certified educational institution in Sierra Leone to train and capacitate people in the field of

cyberspace and cyber security. This means that the country lacks cyber security experts and professionals who possess the right skills and knowledge to create the awareness of the impact of e-crimes.

4.2. Professional Certification Body

There are no government agencies or private agencies with international accreditations to offer any cyber related threats and challenges solutions.

4.3. International Partnership

Sierra Leone is a member of the ITU-IMPACT initiative with access to important cyber security features. It is also a beneficiary to the EU/ITU co-founded project.

4.4. Child Online Protection

Sections 1 and 26 - 28 of the sexual offences Act of Sierra Leone were enacted to protect child online protection [13].

The UN convention and Protocol with no declaration or reservation to articles 16, 17(e) AND 34(c) was acceded by Sierra Leone.

In 2016, a review was carried out with the International Telecommunication Union (ITU), and the Global Cyber Security Capacity Centre (GCSCC), and the Ministry of Information and Communications [14]. They identified the most common cybercrimes in the country such as, telecom-related fraud (SIM boxing), computer-related fraud (Phishing, spam), messaging applications, gender-based violence and online grooming. There are now policies such as ICT and cyber security policy in draft waiting to be enacted by the House of parliament. Other departments complimenting cyber security deployment include the Ministry of Information and Communications, Ministry of Defense, the Central Intelligence and Security Unit, Force Intelligence and Security Unit, and the Internet Society Sierra Leone Chapter. Sierra Leone is also a signatory to the African Union Convention on Cyber Security and Personal Data Protection signed on the 29th January 2016.

5. Conclusion

Impressively, the introduction of the 5G which itself is in the initial stage will subsequently solve some security issues. Unfortunately, man is now left completely dependent on technology from homes to offices daily routine. As online data usage increases, so the challenges posed by cyber criminals who do it for fun or financial reward. Weaker laws on cyber security and cyberspace in Sierra Leone have resulted into numerous forms of internet crimes as seen in the senior secondary school examination malpractice cases, the unlawful forgery of documents to gain admission into higher institutions within the country, the use of manipulated numbers appearing to be foreign numbers or numbers from state security agencies, tapping into voice calls, internet fraud and theft. Therefore, it is incumbent on the government through its security agencies or departments to be proactive in combating the cybercrime rate in Sierra Leone. Public awareness should also be created to illustrate the impacts of cybercrimes and stop the siphoning of the country wealth to other parts of the world.

Cyber security sabotage the growth of a country and the world at large, therefore, it needs to be tackled. Nowadays, almost everything can be done online posing a greater risk, meaning more effective and efficient regulations should be adopted globally that will track and punish those involved in Internet crimes, making people to have confidence to invest in the country.

There should be standardized policies and regulations to combat cybercrimes. Stronger cyber security provides tangible and feasible cyberspace laws to establish a safer business ecosystem that will attract indigenes and foreigners to invest heavily in the socio-economic of the country. Noting that weaker laws and less qualified staff are found in most of the state security forces. This raises more concerns on how to mitigate or implement stronger policies that will track those cyber criminals.

Therefore, numerous schemes should be applied either as a mixture or a unit to salvage the rising cybercrimes in Sierra Leone. Combating cybercrime and cyber security challenges and threats demand both technical and theoretical applications of all security features that render systems and applications safe, and denouncing access to unauthorized system's users.

5.1. Recommendation

As evident from the several study and findings globally, cybercrimes subsequently hinder the development and growth of a nation, security and stability. Therefore, the researcher recommends the following to mitigate or eradicate crimes in the cyberspace within the boundaries of Sierra Leone and its neighbors.

The House of Parliament should enact that more rigid law in order to solve the numerous threats posed by cybercrimes in Sierra Leone.

Enhanced Forensic laboratories be created in order to examine all cybercrime related crimes nationwide.

Strong passwords should be used and there should be a policy to change them regularly.

Continuous staff capacity building should be established in order to improve their reasoning power and match them against the rest of the globe.

Stop political appointment in the field of security and recruit the right staff with the pre-requisite requirements, as security is very paramount.

Build a culture with the aim of security awareness in terms of cyber security and cybercrimes right from primary to university level.

A rigid policy on the use of electronics and computing devices during examinations nationwide be enacted. Having such students is a catastrophe for national development.

Cybercrime influences massive corruption, economic collapse, and acute poverty in any nation, means that the Anti-Corruption Commission, the Office of the National

Security and the Cyber Security Unit at the Criminal Investigation Department should work as a team to combat e-crime. Also, the state security agencies should be vigilant and proactive in the 2023 Sierra Leone National Elections, as most people spread hate speeches on social media. That threatens and undermines the peace and democracy of the nation.

A national sensitization and awareness campaign on the relevance and effect of cyber security is important; it reduces the cybercrime rate in the country.

A specific unit within both the Sierra Leone Police and the Armed Forces should be trained to mainly handle cyber related crimes.

The government should legislate tougher laws relating to copyright issues, telecommunications, privacy and security.

Enhancing awareness and skills in information security and sharing best practices via Cyber security culturization at all stages, is vital.

Promoting a secure e-commerce and e-government platforms is a necessity.

Protection of privacy rights for individuals using electronic communications

A national database system should be established in order to record all citizens' biometric data and other important details that should be cross-matched in the case of crime.

An effective platform should be provided in order to produce early security warning, deterrence, resistance and recovery process.

5.2. Future Research

The researcher was deterred in conducting a national survey and only restricted his survey in Freetown. This may in one way or the other reduce the accuracy of the information produced in this report. Therefore, future researchers are encouraged to conduct a broader and even national survey to cover all the four corners of the country. The country has to finally enact the 2016 draft review report on cyber security, which is a great initiative.

Acknowledgements

This piece of work should not have being made possible without the intervention of Professor Paul Kamara, Professor Prince Sorie Conteh, Dr. (Mrs.) Abie Paula Kamara, Dr. Michael N. Wundah and Dr. Umaru Peter Kamara from the Institute of Advanced Management and Technology (IAMTECH) - Sierra Leone. Special thanks to Dr. Musa Tarawally from the University of Electronic Science and Technology of China (UESTC), and Assistant Professor Nadir Mustafa Mohammed Osman of the University of Blue Nile, Sudan for their inspiration and mentorship.

References

[1] Brenner S (2007). Law in an Era of Smart Technology, Oxford: Oxford University Press p. 374.

[2] Longe OB, Chiemeke SC (2008). Cybercrime and criminality in Nigeria – What roles are internet access points in playing? Eur. J. Soc. Sci. 6 (4): 133-139.

[3] Aluko M (2004). 17 ways of stopping financial corruption in Nigeria. www. comcast. net. April 5, 2010.

[4] Erhabor IM (2008). Cybercrime and the Youths (PGDE Thesis), Department of Education, Ambrose Alli University, Ekpoma, Nigeria, p. 37.

[5] Awe J (2004). Nigeria, South Africa, Ghana top Cybercrime in Africa. www. davidajao. com. 25th June 2010.

[6] Yar M (2005). The novelty of cybercrime: An assessment in light of routine activity theory. Eur. J. Criminol. 2 (4): 407-427.

[7] Smith RG, Grabosky P, Urbas G (2004). Cyber Criminals on Trial. Cambridge (UK): Cambridge UP.

[8] Maat S (2004). Cybercrime: A Comparative Law Analysis (Doctoral thesis), University of South Africa, Pretoria, South Africa p. 239.

[9] Wall DS (2001). Maintaining order and law on the internet. In: Wall DS (Ed.), Crime and the internet. London: Routledge pp. 167-183.

[10] Sharmila Subudhi, Suvasini Panigraphi (2017). Quarter-Sphere Support Vector Machine for Fraud Detection in Mobile Telecommunication Networks. December 2015 Procedia Computer Science 48: 353-359. DOI: 10.1016/j.procs.2015.04.193.

[11] Zhao et al (2017). Detecting telecommunication fraud by understanding the contents of a call. DOI: 10.1186/s42400-018-0008-5

[12] https://www.researchgate.net/publication/327356991_Detecting_telecommunication_fraud_by_understanding_the_contents_of_a_call/fulltext/5b8a6e15299bf1d5a7363752/327356991_Detecting_telecommunication_fraud_by_understanding_the_contents_of_a_call.pdf?origin=publication_detail

[13] https://www.coe.int/en/web/cybercrime/-/glacy-improving-international-cooperation-on-cybercrimeand-electronic-evidence-in-west-africa.

[14] http://www.au.int/en/sites/default/files/treaties/29560slafrican_union_convention_on_cyber_security_and_personal_data_protection.pdf