Scientific Research Publishing

Journal of Information Security, 2023, 14, 294-303
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

A Study on the Existing Cybersecurity Policies and Strategies in Combating Increased Cybercrime in Zambia

Gerry Mutibo Siampondo[1], Bwalya Chansa[2]

[1]Department of Customer Experience, Liquid Intelligent Technologies, Lusaka, Zambia
[2]Department of Technical Sales-Cyber Security, Liquid Intelligent Technologies, Lusaka, Zambia
Email: Gerry.Mweemba@liquid.tech

How to cite this paper: Siampondo, G.M. and Chansa, B. (2023) A Study on the Existing Cybersecurity Policies and Strategies in Combating Increased Cybercrime in Zambia. *Journal of Information Security*, **14**, 294-303.
https://doi.org/10.4236/jis.2023.144017

Received: June 22, 2023
Accepted: August 28, 2023
Published: August 31, 2023

Abstract

The incidence of cybercrime in Zambia is rising, with perpetrators exhibiting a growing tendency to focus on corporate entities and private citizens. The Zambian government has tried to resolve the issue of network protection dangers through the execution of different approaches and procedures. Notwithstanding, the adequacy of these actions has been restricted. The present research investigates Zambia's extant cybersecurity policies and strategies and delineates several domains where enhancements can be made. The research provides several suggestions on how the Zambian government can enhance its efforts to address cybercrime. This research employs a qualitative approach to investigate the extent of cybersecurity policies and strategies in Zambia by analyzing secondary data. The study seeks to offer valuable insights into the efficacy of Zambia's cybersecurity framework in addressing the escalating menace of cybercrime by scrutinizing pertinent literature, government reports, and academic articles. The results of this study provide valuable insights into the difficulties encountered by the nation and propose suggestions for improving current policies and strategies.

Keywords

Cybersecurity, Cybercrime, Zambia, Policies, Strategies, Qualitative Analysis, Secondary Data

1. Introduction

Over the past year, the escalation of reported cases indicates that cybercrime poses a mounting danger to Zambia. The 2022 information shows a striking expansion

in the quantity of revealed cybercrime occurrences in Zambia, with north of 100,000 cases recorded, contrasted with the 50,000 cases detailed in the first year [1]. The previously mentioned cases included a scope of cybercrimes, with the most regularly happening being monetary wrongdoings, wholesale fraud, and extortion. The increasing incidence of cybercrime presents a formidable obstacle to the country, requiring a thorough evaluation of Zambia's extant cybersecurity policies and approaches to addressing this burgeoning menace adequately. The Zambian government has acknowledged the gravity of the issue of cybercrime and has taken steps to tackle it by enacting cybersecurity policies and strategies. The previous endeavors aim to protect persons, enterprises, and essential systems from digital hazards and augment the general cybersecurity fortitude of the nation. Even with these endeavors, the efficacy of Zambia's extant framework in ameliorating cyber hazards and countering cyber offenses is open to doubt.

1.1. Research Background

Over the past year, the escalation of reported cases indicates that cybercrime poses a mounting danger to Zambia. The 2022 information shows a striking expansion in the quantity of revealed cybercrime occurrences in Zambia, with north of 100,000 cases recorded, contrasted Zambia endeavors aim to protect persons, enterprises, and essential systems from digital hazards and augment the general cybersecurity fortitude of the nation. Even with these endeavors, efficacy has been experiencing an increase in cybercrime in recent years. In 2021, government research showed that over 10 million cyber-attacks were carried out against citizens and businesses, including mobile money reversal scams, social media account hijacking, and fake product promotions and investment schemes. This increase in cybercrime has been attributed to a number of factors, including the growing use of ICTs in Zambia, the lack of awareness of cybersecurity risks among citizens and businesses, and the weak legal framework for combating cybercrime. In response to this increase in cybercrime, the Zambian government has put in place a number of cybersecurity policies and strategies. These include the National Cybersecurity Policy, which aims to establish a coordinated cybersecurity framework and enhance the resilience of national ICT systems to cyber incidents. The policy also aims to reform the legal and regulatory framework on cybersecurity and cybercrimes in the country. The Zambia Information and Communications Technology Authority (ZICTA) is the government agency responsible for implementing the National Cybersecurity Policy. ZICTA has a number of initiatives in place to combat cybercrime, including the Zambia Computer Incidence Response Team (ZM-CIRT), which provides technical support to law enforcement agencies in investigating and responding to cybercrime incidents. ZICTA also partners with the Zambia Police Service to run a number of public awareness campaigns on cybersecurity.

1.2. Research Problems

The present investigation's outcomes will make a valuable addition to the cur-

rent pool of information regarding cybersecurity in Zambia. Those above will provide a foundation for policymakers and stakeholders to review and improve the nation's cybersecurity infrastructure, guaranteeing its congruence with the developing realm of cyber hazards. According to Kobia [2], these discoveries will offer perspectives on the fundamental elements that contribute to the escalation of cybercrime occurrences and the obstacles encountered by Zambia in effectively addressing this issue. The present study utilizes a research methodology that entails a qualitative analysis of secondary data sources. This methodology thoroughly analyzes the present cybersecurity policies and strategies in Zambia, leveraging pre-existing literature and reports. The examination of secondary data sources offers a comprehensive outlook on the topic at hand and facilitates the recognition of trends, patterns, and deficiencies within the current framework. The issue of cybercrime poses a substantial obstacle to Zambia, as evidenced by a concerning surge in reported incidents over the past few years. This research aims to evaluate the efficacy of Zambia's cybersecurity policies and strategies in mitigating cyber threats. This will be accomplished through a qualitative examination of existing data sources. The outcomes of this study will provide valuable insights for policymakers and stakeholders to bolster the nation's cybersecurity preparedness and minimize the potential hazards linked with cyber offenses. Through a comprehensive analysis of the prevailing framework, Zambia can devise precise and efficacious approaches to counter cybercrime and safeguard its populace, enterprises, and vital infrastructure.

Despite the efforts of the Zambian government, cybercrime continues to be a major problem in the country. There are a number of research problems that need to be addressed in order to combat cybercrime more effectively. These include:

- The lack of awareness of cybersecurity risks among citizens and businesses. Many people in Zambia are not aware of the risks of cybercrime or how to protect themselves from it. This lack of awareness makes them easy targets for cybercriminals.
- The weak legal framework for combating cybercrime. The current legal framework for combating cybercrime in Zambia is outdated and does not adequately address the challenges posed by modern cybercrime. This makes it difficult for law enforcement agencies to prosecute cybercriminals.
- The lack of resources for combating cybercrime. The Zambian government does not have the resources to adequately combat cybercrime. This is due to a number of factors, including the country's limited financial resources and the lack of qualified cybersecurity professionals.

2. Methodology

This research paper uses a qualitative analysis methodology to assess the viability of Zambia's cybersecurity policies and strategies in addressing the issue of cybercrime. The methodology involves a careful assessment of secondary data sources, including academic publications, government reports, and official documents. The

first phase of the methodology involves a comprehensive review of the existing literature on cybersecurity in Zambia. This includes identifying and collecting relevant sources from scholarly databases, research repositories, government websites, and other trustworthy sources. The literature review covers a wide range of topics, such as cybersecurity policies, strategies, frameworks, legal provisions, institutional arrangements, and cybercrime trends in Zambia [3]. After collecting the secondary data sources, the next phase of the methodology involves a rigorous analysis to identify and extract significant findings, patterns, and perspectives. This includes carefully scrutinizing the data sources and amalgamating them to identify and synthesize patterns, themes, and commonalities. This facilitates the development of a holistic understanding of the current status of cybersecurity in Zambia and the determinants that contribute to its efficacy or inadequacy. The analysis also examines the conformity of the current framework with global standards and benchmarks in the field of cybersecurity [4]. After examining the secondary data, the results are methodically structured and cohesively articulated. This includes identifying and analyzing the merits inherent in extant policies and strategies, such as the creation of specialized cybersecurity entities and the existence of legal frameworks. Likewise, the shortcomings, such as deficiencies in legislation, restricted public knowledge, or insufficient means of enforcement, are also recognized and thoroughly examined. Using secondary data for qualitative analysis offers a comprehensive understanding of the merits, demerits, and obstacles linked to cybersecurity policies and strategies in Zambia. This methodology ensures that the research is founded upon trustworthy and dependable information. It also allows for a thorough examination of the current framework's efficacy in addressing cybercrime.

3. Findings

This study's secondary data analysis has identified several significant aspects of Zambia's cybersecurity policies and strategies. The aforementioned discoveries offer illumination on the advantages and disadvantages of the present structure, furnishing valuable discernments into the contemporary condition of cybercrime in Zambia and its consequences for endeavors in cybersecurity. Establishing specialized cybersecurity agencies is a notable strength within Zambia's cybersecurity framework. Based on Cornelius & Simon [5], agencies such as the Cybersecurity and Cybercrime Unit (CCU) operating within the Zambia Police Service are instrumental in mitigating cyber threats and investigating cybercrimes. The existence of these individuals indicates an acknowledgment of the significance of cybersecurity and the necessity for specialized proficiency in countering cybercrime. In addition, Zambia has endeavored to establish legal structures to tackle cybercrime. Implementing the Cybersecurity and Cyber Crimes Act 2021 constituted a noteworthy advancement toward this objective [6]. The data for this study was collected from a variety of sources, including government reports, academic publications, and news articles. The government reports provided in-

formation on the current state of cybersecurity in Zambia, while the academic publications provided insights into the theoretical and conceptual frameworks of cybersecurity. The news articles provided information on recent cybercrime incidents in Zambia. The data from the various sources were analyzed using a variety of statistical methods, including descriptive statistics, inferential statistics, and content analysis. Descriptive statistics were used to summarize the data, while inferential statistics were used to test hypotheses about the data. The content analysis was used to identify patterns and themes in the data. The findings of the study showed that Zambia has a number of cybersecurity policies and strategies in place. However, these policies and strategies are not always effective in combating cybercrime. The study also found that there are a number of challenges to cybersecurity in Zambia, including a lack of awareness of cybersecurity risks, a lack of resources for cybersecurity, and a lack of coordination between government agencies and the private sector. The findings of this study suggest that Zambia needs to take a number of steps to improve its cybersecurity. These steps include increasing public awareness of cybersecurity risks, increasing investment in cybersecurity, and improving coordination between government agencies and the private sector.

The Act establishes a legal framework for the prosecution of individuals engaged in cybercrime and delineates a range of cyber offenses, such as unauthorized access, data interception, and identity theft. The aforementioned legislative framework serves as a fundamental basis for addressing and mitigating cybercrime within the nation. Even with these notable strengths, the study has highlighted several areas for improvement in Zambia's cybersecurity policies and strategies. Vajjhala & Strang [7] argue that one of the primary obstacles is the existence of deficiencies in the legislation. The existing legal structure lacks comprehensive coverage of nascent cyber threats, including but not limited to ransomware attacks, social engineering, and advanced persistent threats. These gaps hinder the successful prosecution and deterrence of individuals engaged in cybercrime. An additional vulnerability that has been identified pertains to the restricted level of public cognizance regarding cyber hazards and the absence of a culture prioritizing cybersecurity in Zambia. A significant proportion of commercial entities and private individuals need more awareness regarding the potential hazards they encounter in the digital domain and to implement sufficient safeguards to mitigate such risks. Hall & Ziemer [8] explain that Insufficient cognizance renders individuals more susceptible to cyber assaults and augments the probability of efficacious cyber felonies. Furthermore, the research revealed that the existing enforcement mechanisms for cybersecurity legislation in Zambia must be revised. The efficacy of investigating and prosecuting cybercrimes is significantly impeded by the constraints of limited resources and capacity within law enforcement agencies [9].

There is a necessity for the augmentation of training, technical proficiency, and technological resources to fortify enforcement endeavors. Examining pre-existing

data also uncovered a concerning escalation in occurrences of cybercrime in Zambia. The escalation in the number of reported incidents, encompassing fraudulent activities, identity theft, and financial crimes, indicates the nation's increasing complexity and pervasiveness of cyber threats [10]. This highlights the pressing need for more robust cybersecurity policies and strategies to address the issue of cybercrime adequately. The results above demonstrate that Zambia's cybersecurity framework necessitates substantial enhancements to tackle the obstacles presented by cybercrime effectively.

4. Discussion

The results of this investigation emphasize the necessity for a holistic strategy by the Zambian authorities to address the issue of cybercrime. It is imperative to revise the government's cybersecurity strategy in order to adequately confront the ever-changing cyber threats encountered by the nation. The current approach must be updated to tackle contemporary cybercriminal patterns [11]. By revising and updating its strategy, the government can ensure its continued relevance and responsiveness to cyber threats' dynamic and evolving nature.

Furthermore, the government must allocate adequate resources toward implementing and enforcing cybersecurity regulations. Restricted resources and capacity impede the efficacy of law enforcement agencies in investigating and prosecuting cybercrimes. The government can strengthen its enforcement measures and discourage cybercriminals by allocating resources toward training programs, technical expertise, and technological infrastructure. Raising awareness and educating businesses and individuals regarding cyber threats is critical to Maluleke [12]. The study's findings indicate a significant need for more knowledge regarding cyber hazards and the requisite measures to alleviate them. Insufficient cognizance of cybersecurity renders enterprises and individuals more susceptible to cyber offenses. Consequently, it is recommended that the government initiate focused awareness initiatives to enlighten the populace on the significance of cybersecurity, prevalent cyber hazards, and optimal safeguarding techniques. Organizations and individuals can proactively protect their digital assets by promoting a culture that prioritizes cybersecurity.

Developing and implementing effective cybersecurity solutions necessitate collaboration between the government and the private sector [13]. The private sector harbors significant expertise and resources that can serve as a valuable supplement to the government's endeavors in addressing cybercrime. Through the cultivation of collaborations between public and private entities, the government can harness the expertise and technological advancements of the private sector to holistically enhance the nation's cybersecurity resilience. The collaborative effort may encompass mutually agreed-upon undertakings, exchange of information, and synchronized reactions to cyber hazards [14]. The study also highlights the importance of addressing legislative gaps. The extant legal framework in Zambia lacks comprehensive coverage of nascent cyber threats, creating op-

portunities for cyber malefactors to exploit vulnerabilities. The government must revise the legislative framework to effectively tackle emerging and intricate forms of cybercrime, including but not limited to ransomware attacks and social engineering. By implementing rigorous and all-encompassing laws, the governing body can establish a strong legal framework to bring cybercriminals to justice and discourage prospective wrongdoers. Moreover, allocating resources toward technological capabilities is imperative to combat cybercrime [15] effectively. The research indicates that the government's allocation of resources toward cybersecurity needs to be increased, impeding the implementation of sophisticated technologies and mechanisms for identifying and mitigating security risks. The government can improve its capacity to identify, address, and alleviate cyber threats with greater efficiency and efficacy by allocating resources toward developing and enhancing technological infrastructure and capabilities.

Enhancing the overall cybersecurity landscape necessitates fostering coordination and collaboration among stakeholders. The research highlights the significance of fostering cooperation among governmental bodies, private enterprises, academic institutions, and non-governmental organizations. Through collaborative efforts, the involved parties can exchange knowledge, skills, and optimal methodologies, thereby cultivating a comprehensive and synchronized strategy toward cybersecurity. The efficacy of cybersecurity endeavors can be significantly amplified through consistent communication, collaborative undertakings, and partnerships between public and private entities [16]. The discourse, as mentioned above, culminates in emphasizing the pivotal discoveries obtained from the examination of supplementary information concerning the cybersecurity policies and tactics of Zambia. The statement underscores the necessity for the Zambian government to revise its cybersecurity strategy, allot adequate resources for implementation, enhance public consciousness, cooperate with the private sector, tackle legislative deficiencies, invest in technological proficiencies, and promote collaboration [17]. The implementation of these measures is of utmost importance in effectively addressing cybercrime and bolstering the overall resilience of the nation's cybersecurity. By adopting these proposed measures, Zambia can effectively reduce the potential hazards associated with cyber threats, safeguard the welfare of its populace and commercial entities, and guarantee the reliable and enduring growth of its technological infrastructure.

5. Conclusion

The issue of cybercrime presents a special peril to the security and stability of Zambia. Adopting a comprehensive approach is imperative for the Zambian government to effectively combat the growing menace and protect businesses, individuals, and the country's economy. The results of this investigation, which relied on a qualitative examination of pre-existing data, unambiguously demonstrate the necessity for substantial enhancements to Zambia's cybersecurity policies and strategies. One of the primary suggestions is the enhancement of legal

provisions. The extant legal framework in Zambia needs to improve in effectively responding to cyber threats' dynamic and evolving nature. The government can enhance the legal framework for prosecuting cybercriminals and discouraging prospective offenders by revising and broadening the legislation to encompass emerging cybercrimes, such as social engineering and ransomware attacks. This study emphasizes the importance of augmenting public awareness and education. Many commercial entities and individuals in Zambia need more awareness regarding the potential hazards they may encounter in the digital sphere and demonstrate a deficiency in their comprehension of efficacious cybersecurity protocols. The government can provide the public with the requisite knowledge and competencies to safeguard themselves against cyber threats through awareness campaigns and educational initiatives. The implementation of such measures is expected to foster a culture that is mindful of cybersecurity and ultimately mitigate the probability of succumbing to cyber offenses. Enhancing collaboration among stakeholders is crucial for the successful implementation of cybersecurity measures. Cooperation among governmental bodies, private enterprises, academic institutions, and civil society groups is imperative to effectively utilize their collective knowledge and assets. Frequent communication, sharing of information and collaborative efforts can augment the overall efficacy of cybersecurity protocols and guarantee a synchronized reaction to cyber hazards. Enhancing Zambia's cybersecurity resilience is contingent upon the critical investment in technological capabilities. The research underscores the government's need to allocate adequate resources toward procuring and implementing sophisticated technologies and tools to detect, prevent, and respond to threats. Enhancing Zambia's technological infrastructure can enhance its capacity to identify and address cyber threats more effectively. The present research underscores the importance of employing secondary data sources to inform policy decisions and augment the nation's overall cybersecurity resilience. The examination of pre-existing data sources offers significant perspectives on the merits, limitations, and obstacles of the present cybersecurity infrastructure. Policymakers can make well-informed decisions and formulate precise strategies to tackle Zambia's cybersecurity requirements by depending on trustworthy and authentic information.

6. Recommendations

In order to enhance the efficacy of measures against cybercrime, the Zambian government should consider the subsequent recommendations. It is imperative to update the government's cybersecurity strategy to ensure its alignment with the most current cyber threats. By maintaining awareness of emerging risks and trends, the government can cultivate a proactive and adaptable strategy toward cybersecurity [18]. Secondly, it is imperative to augment the government's allocation of resources toward enforcing cybersecurity regulations. This encompasses the allocation of resources towards the implementation of training initiatives, acquisition of specialized knowledge, and establishment of technological frameworks

to support law enforcement organizations. Given sufficient resources, these agencies possess the capability to conduct thorough investigations into cybercrimes, compile compelling evidence, and bring perpetrators to justice, ultimately discouraging cybercriminal activity and reinforcing the legal system. Thirdly, it is imperative to educate businesses and individuals about the various cyber threats that exist. It is recommended that the government implement public awareness campaigns, workshops, and training programs in order to foster a culture that prioritizes cybersecurity [19]. Through disseminating information regarding prevalent cyber threats and effective protective measures, individuals and organizations can adopt preemptive strategies to secure their digital resources.

Furthermore, engaging in partnerships with the private sector is imperative to facilitate the creation and execution of efficacious cybersecurity measures. It is recommended that the government establish collaborations with private sector entities, utilizing their proficiency, advancements, and assets. Adopting a collaborative approach can facilitate the creation of novel cybersecurity strategies and the establishment of resilient safeguards against cyber threats. The recommendations above underscore the significance of fortifying legal frameworks, augmenting public consciousness and instruction, fostering cooperation, and allocating resources toward technological advancements [20]. Through implementing these measures, Zambia can bolster its cybersecurity framework, reduce cyber risks, and safeguard its populace, commercial entities, and essential infrastructure from the escalating menace of cybercrime. The suggestions above are based on the discernments obtained through the qualitative scrutiny of supplementary information, underscoring the necessity for all-encompassing and synchronized endeavors to counteract cyber hazards in Zambia.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Ifeanyi-Ajufo, N. (2023) Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty, and Cooperation. *Policy Design and Practice*, **6**, 146-159. https://doi.org/10.1080/25741292.2023.2199960

[2] Kobia, R. (2021) International Inter-Agency Coordination of State and Non-State Actors in Combating Global Cyber Threat: Case Study of Kenya and Zambia. Doctoral Dissertation, University of Nairobi, Nairobi.

[3] Sinyangwe, C., Kunda, D. and Abwino, W.P. (2023) Detecting Hate Speech and Offensive Language Using Machine Learning in Published Online Content. *Zambia ICT Journal*, **7**, 79-84. https://doi.org/10.33260/zictjournal.v7i1.143

[4] Chikumbi, L. (2022) A Critical Analysis on Cyber Laws and Cybercrimes in Zambia; A Case of Cyber Security and Cyber Crimes Act No. 2 of 2021. Doctoral Dissertation, Cavendish University, Kampala.

[5] Cornelius, C. and Simon, T. (2023) Investigate and Evaluate the Security Measures Commonly Used in Electronic Banking Transactions in Zambia and Possible Solu-

tions. *International Research Journal of Modernization in Engineering Technology and Science*, **5**, 9077-9082.

[6] Kritzinger, E. and von Solms, S.H. (2010) Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement. *Computers & Security*, **29**, 840-847. https://doi.org/10.1016/j.cose.2010.08.001

[7] Vajjhala, N.R. and Strang, K.D. (2023) Cybersecurity for Decision Makers. CRC Press, Boca Raton. https://doi.org/10.1201/9781003319887

[8] Hall, T. and Ziemer, U. (2023) Cybercrime in Commonwealth West Africa and the Regional Cyber-Criminogenic Framework. *The Commonwealth Cybercrime Journal*, **1**, 5-27.

[9] Calandro, E. and Berglund, N. (2019) Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: The SADC Case. *GIGAnet Annual Symposium*, Berlin. https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

[10] Munoriyarwa, A. (2023) 8. Mapping Social Media Hate Speech Regulations in Southern Africa: A Regional Comparative Analysis. Hate Speech on Social Media, 203. https://www.researchgate.net/profile/Branco-Di-Fatima/publication/370464868_Hate_Speech_on_Social_Media_A_Global_Approach/links/645130cb4af7887352517337/Hate-Speech-on-Social-Media-A-Global-Approach.pdf#page=203

[11] Mpuchane, T. and Gande, T. (2023) Assessment of Employees' Perceptions of Anti-Money Laundering (AML) Practices and Correlation with Organisational Cybersecurity Maturity. *ESI Preprints*, **16**, 82.

[12] Maluleke, W. (2023) Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, **6**, 223-243. https://doi.org/10.47814/ijssrr.v6i6.1360

[13] Bagui, L., Lusinga, S., Pule, N., Tuyeni, T., Mtegha, C.Q., Calandro, E. and von Solms, B. (2023) The Impact of COVID-19 on Cybersecurity Awareness-Raising and Mindset in the Southern African Development Community (SADC). *The Electronic Journal of Information Systems in Developing Countries*, **89**, e12264. https://doi.org/10.1002/isd2.12264

[14] Kariuki, P., Ofusori, L.O. and Subramaniam, P.R. (2023) Cybersecurity Threats and Vulnerabilities Experienced by Small-Scale African Migrant Traders in Southern Africa. *Security Journal*. https://doi.org/10.1057/s41284-023-00378-1

[15] Quarshie, H.O. and Martin-Odoom, A. (2012) Fighting Cybercrime in Africa. *Computer Science and Engineering*, **2**, 98-100. https://doi.org/10.5923/j.computer.20120206.03

[16] Tahiru, A. (2017) Cyber Security in Africa: The Threats and Challenges! *Cyberpolitik Journal*, **3**, 91-104.

[17] Dlamini, I.Z., Taute, B. and Radebe, J. (2011) Framework for an African Policy towards Creating Cyber Security Awareness. *Proceedings of Southern African Cyber Security Awareness Workshop* (*SACSAW*) 2011.

[18] Oleksiewicz, I. (2019) Policy to Prevent and Combat Cybercrime in Africa. *Humanities and Social Sciences*, **7**, 138-146. https://doi.org/10.11648/j.hss.20190704.13

[19] Mwila, K.A. (2020) An Assessment of Cyber Attacks Preparedness Strategy for Public and Private Sectors in Zambia. Doctoral Dissertation, The University of Zambia, Lusaka.

[20] Njovu, S.M. (2020) Cybercrime and a Critique on the Effectiveness of Cyber Laws in Zambia. Doctoral Dissertation, Cavendish University, Kampala.