Journal for Business, Development and Leadership (JBDL)

Original Article

Analysis of the Zambian courts adequacy to prosecute cybercrime cases.

Michael Tembo[1]

[1] Africa Research University (ARU), Keystone University of Africa, Lusaka, Zambia

* Correspondence: mtembo@keystoneuoa.com; Tel.: *(+260) 976 782 131*

Received: 04 March 2024; Accepted: 15 July 2024; Published: 30 August 2024

Abstract: This study focused on analyzing the Zambian courts adequacy in prosecuting cybercrime cases. The aim was to investigate whether the courts in Zambia had necessary capacity to prosecute cybercrime cases and make recommendations. To carry out this research the researcher used an exploratory research design because it enabled the researcher to collect both qualitative and quantitative data using questionnaires with closed and open-ended questions. Respondents were judges from the high court and magistrates from subordinate courts in Lusaka district and lawyers came from different law firms in Lusaka district. The prosecutors came from the National Prosecution Authority, the registrar came from the high court in Lusaka district and court clerks as well as interpreters came from the subordinate courts in Lusaka district.
The study revealed; that both the high court and subordinate courts had no dedicated personnel apportioned to deal with cybercrime cases, that both the high court and subordinate courts had no necessary technological infrastructure to support the prosecution of cybercrime cases. On the other hand, the study reveals that both the high court and subordinate courts have a streamlined process for obtaining and admitting digital evidence and that both high court and subordinate courts have mechanisms in place to protect the confidentiality and integrity of digital evidence.
The study recommends; that both the high courts and subordinate courts need to be equipped with the necessary technological infrastructure to support cybercrime prosecutions. The study further recommends that the judiciary should consider having dedicated personnel who are expert to be apportioned to deal with cybercrime cases.

Keywords: Cybercrime, Capacity, Prosecution, Court, Technological infrastructure, law enforcement agencies

1. Introduction

Cybercrimes are crimes committed using the internet and information technology systems. It is a new phenomenon where criminals are able to commit crime anywhere in the world through the use of computers, smartphones, or other information technology gadgets without being present at a crime scene (Kobia, 2021).
As a result of the advancing of computer information technology, there has been an increase in the number of cybercrime related cases (Siampondo & Chansa, 2023). There has been also a public concern about whether the Zambian courts have adequate resources to prosecute cybercrime cases following the high number of cases reported and only a few out of those cases have been successfully prosecuted. In a case of Fredrick Chiluba and the internet data processing manager Patrick Mkandawire (1999), the accused managed to hack the government website and replaced the photo of the president with a cartoon on July 7, but it took officials ten full days, until July 17, 1999, to notice he had substituted Chiluba's official portrait with the "offensive" cartoon. When the matter was taken to

court for prosecute, it was discovered that there was no legal system in place to prosecute such kind of cases and judges lacked sufficient knowledge to prosecute such a case as it was a new kind of case which required a different legal framework (Sichula, 2023).

Another example, on 3rd January 2023 the Police Spokesperson Mr. Rae Hamoonga bemoaned on the increase of cybercrimes in Zambia and warned the public to be cautious of the same phenomenon. He further stated that the Zambia police service had received 78 cybercrimes cases across the nation and that out of the 78 cases, 32 where in court while 46 where under investigation (Kaumba, 2022) With the increases in cybercrime cases the court has been cited to be one of the institutions which need adequate manpower, resources, and tools in order to successfully prosecute cybercrime cases (Chikumbi, 2022).

It has also been observed that most cases are being reported to police but only few cases have been exhausted in the court of law. A good example of such a case is the case of Mwamba and Luchinde (2023) who was arrested on June 8, in Lusaka contrary to Section 342 of the Penal Code Chapter 88 of the Laws of Zambia and also on three counts of publication of information contrary to Section 54 of the Cyber Security and Cyber Crimes Act No. 2 of 2021. This also has raised concerns whether the court has enough resources and capacity to prosecute cybercrime cases (Sichula, 2023).

These cases exposed how weak and vulnerable the Zambian legal system was in prosecuting cybercrimes. It also exposed how Zambia lacked a rigorous legal framework in combating cybercrimes. This led to the Zambian government to come up with a series of legislation in order to deal with these cases. One such legislation is the Cyber Security and Cyber Crimes Act of 2021. Although Zambia has enacted legislations to deal with cybercrime cases, it has been reported that there was a lack of capacity, resources, knowledge, and awareness when it comes to dealing with cases of cybercrimes in Zambia (Siampondo & Chansa, 2023).

In view of the above this research was conducted to analyze whether the Zambian courts in the current state, have adequate resources to prosecute cybercrime cases. If not, what are the needs of the courts in Zambia in order to successfully prosecute cybercrime cases?

.

Cybercrime cases are supposed to be prosecuted in the court of law as soon as possible, just like any other type of cases in Zambia and this promote order and peace in the nation and shows how firm the court is in executing their duties as shrined in the constitution of Zambia article 118 sub article 2(b) of the Constitution of Zambia (Amendment) (No. 2 of 2016). However, the opposite is what is currently prevailing. It has been observed that even when the government of Zambia has managed to come up with a legal framework to deal with cybercrime, cybercrime cases are still not prosecuted very fast (Maluleke, 2023). In the year 2022 alone, 78 cases were reported, and 32 cases were pending trial in the court of law but still up to date there is only few cases which has been successfully prosecuted (Kaumba, 2022). If this problem persists, it will result into criminals taking advantage of the same and commit more crimes and if those who commit cybercrime are not punished in order to send a strong warning to the public and deter who would be offenders, this will lead to delayed justice and failure by court to deliver justice on time as enshrined in article 118 sub article 2 (b) of constitution of Zambia (Maluleke, 2023). It will also make the public at large loose trust in the court of law and compel them to take law into there on hands (Njovu, 2020). Therefore, this research, was conducted in order to (a) understand the current position whether the Zambian courts and its officials have necessary capacity to prosecute cybercrime cases and (b) make recommendations on what the courts in Zambia need to successfully prosecute cybercrimes cases.

2. Literature

Prosecuting cybercrime cases is one of the challenges which the courts are facing across the globe and Zambia is not excluded from the same. The capacity of Zambian courts to prosecute cybercrime cases hinges on a variety of factors, including legal frameworks, technological infrastructure, and expertise among legal professionals. Existing literature sheds light on these aspects:

Legal Frameworks:

Studies such as Mwansa and Kabwe (2019) underscore the importance of robust legal frameworks in prosecuting cybercrime. The research evaluates the adequacy of Zambian cybercrime legislation and suggests improvements to align it with international standards. To prosecute cybercrimes requires a different approach and framework from the traditional way of prosecuting cybercrime. For example, the law requires that a person who commits a crime in Lusaka should not be tried in a different district but should be tried in the same district where he or she committed a crime. But when it comes to cybercrime cases, the defendant may commit a crime online in a certain district whilst at the same time he or she is physically present in a different district. This has rendered the traditional way of ascertaining jurisdiction to be actually invalid when dealing with cybercrimes cases (Mwansa & Kabwe, 2019).

Technological Infrastructure:

Technological Infrastructure Challenges in Prosecuting Cybercrimes hinges on the following:

1. Digital Evidence Management:

One significant challenge faced by courts in prosecuting cybercrimes is the effective management of digital evidence. The exponential growth in digital data poses challenges in preserving, authenticating, and presenting evidence in court (Casey, 2018).

2. Cybersecurity Threats and Attacks:

The very nature of prosecuting cybercrimes exposes courts to cybersecurity threats (Holt and Bossler, 2016). Courts need robust cybersecurity measures to protect sensitive case information and prevent unauthorized access, ensuring the integrity of the judicial process) (Marotta, 2019).

3. Technical Expertise and Training:

The complexity of cybercrimes demands a high level of technical expertise (Brenner, 2010). Courts often face challenges in having judges, attorneys, and law enforcement personnel with the necessary skills to understand and effectively prosecute cases involving intricate technological aspects (Décary-Hétu, 2016).

4. International Jurisdictional Issues:

Cybercrimes often transcend national borders, creating jurisdictional challenges (Bellovin, 2007). Courts struggle with issues of extradition, international cooperation, and the enforcement of judgments when prosecuting cybercriminals operating across different countries (Kerr, 2014).

5. Privacy Concerns and Legal Compliance:

The prosecution of cybercrimes may involve accessing private digital information (Svantesson, 2015). Courts must navigate the delicate balance between investigating cybercrimes and respecting privacy rights, complying with legal standards and ethical considerations (Buchanan, 2020).

6. Resource Constraints:

Courts may face resource constraints, hindering their ability to invest in state-of-the-art technologies and hire specialized personnel (Choo, 2011). This can impede the timely and effective prosecution of cybercrimes (Taylor, 2016).

7. Rapid Technological Advancements:

The ever-evolving landscape of technology presents challenges for courts to keep pace with the latest developments (Kshetri, 2018). Prosecutors and judges need to stay informed about emerging cyber threats and technologies to adjudicate cases effectively (Goldsmith, 2006).

8. Legislation and Legal Frameworks: novel cyber threats, ensuring that the legal system remains relevant and effective (Kerr, 2014).

Chileshe (2018) examines the technological infrastructure required for cybercrime prosecutions. The study emphasizes the need for investments in secure storage and retrieval systems for digital evidence (Chileshe & Smith, 2018).

3. Materials and Methods

The researcher used an exploratory research design because it focuses on exploring a research problem when little is known about it and generates insights and identifying variables for further investigation. This design allows researchers to gather a broader and more comprehensive understanding of a research problem by combining the strengths of both qualitative and quantitative methods (Creswell & Creswell, 2017). It helped in understanding the challenges both the high courts and subordinate courts faces as well as its adequacy in prosecuting cybercrime cases. In this study, qualitative data was gathered to explore challenges and perceptions of court officials when prosecuting cyber-crime cases while quantitative data was used to assess the efficacy of legal processes. For this study court officials which includes (judges/magistrates, lawyers, prosecutors, court registrars and interpreters were the target population). The researcher considered 50 participants across different strata using judgment sampling and also based on what other researchers used as a sample size in similar previous research and this was due to little and sparsely population of court officials. This method of selecting participant and sample size was subjective and relied on the researcher's knowledge and judgment to identify participants who are considered most relevant or representative of the population of interest (Babbie, 2015). Neuman (2006) also states that when using judgement sampling saturation should be considered. So, the researcher considered 50 participants across different strata as justifiable to reach saturation point looking at the smallness of the target population. Creswell (2014) also affirms that determining an appropriate sample size is a crucial aspect of research design, influencing the reliability and generalizability of study findings and the researcher should make sure that the sample size selected from the total population can help to inform research. The researcher used judgmental sampling technique. Judgmental sampling, also known as purposive or subjective sampling, is a non-probability sampling technique in which the researcher uses their

judgment to select participants or elements for inclusion in a study based on specific criteria. This method is often used when the researcher believes that certain individuals or elements are more relevant to the research objectives and the total population is small which is making it difficult to easily find participants (Babbie, 2015). The researcher used a survey data collection method to collect data from 50 respondents. Surveys can be conducted through various means, including paper-based questionnaires, phone interviews, face-to-face interviews, online forms, or a combination of these methods and is suitable in a mixed method approach (Dillman, 2014). The researcher used questionnaires with both closed and open-ended questions. Instrument for data collection refer to the tools to be used in collecting information from the respondents. To analyze data the researcher used both qualitative and quantitative analysis. Under qualitative analysis the researcher used specifically thematic analysis to examine non-numerical data, such as text to uncover patterns, themes, and insights. Creswell and Cresswell (2017) assert that thematic analysis is one of the effective ways of analyzing qualitative data. While under quantitative analysis the researcher used Statistical Package for the Social Sciences (SPSS) software to identify patterns, relationships, and trends within the data to draw conclusions and make predictions. (Pallant, 2021). Qualitative data, which consists of non-numerical information, was interpreted by making sense out of patterns, themes, and relationships within the data. While quantitative data was interpreted by analyzing using statistical methods to identify patterns, relationships, and trends within the data to draw conclusions and make predictions.

4. Results and Discussion

Capacity of the court to prosecute cybercrime.
Examining the court's ability to handle cybercrime prosecutions.
The respondents' main profession

The respondents of this research included judges from the high court and magistrates from subordinate courts in Lusaka district, lawyers came from different law firms in Lusaka district. The prosecutors came from the National Prosecution Authority, the registrar came from the high court in Lusaka district and court clerks as well as interpreters came from the subordinate courts in Lusaka district. In Zambia, Judges, magistrates, lawyers, prosecutors, registrars, court clerks and interpreters are all collectively referred to as officers of the court.

The respondents' main profession (n=50).

	Frequency	Percent
Judge/Magistrate	9	18.0
Lawyer	29	58.0
Prosecutor	3	6.0
Registrar	1	2.0
Court Clerk	4	8.0
Interpreter	4	8.0
Total	50	100.0

Source: Field data 2024

The table above shows that 18% were either judges or magistrates, 58% were lawyers, 6% were prosecutors, 2% registrars, 8% court clerks and 8% were interpreters.
Dedicated personnel with expertise in cybercrime investigations and prosecution.

Dedicated personnel apportioned to deal with cybercrime cases(n=50).

	Frequency	Frequency	Frequency total	%	%	total %
	yes	no		yes	no	
Judge/magistrate	0	9	9	0	18	18
Lawyer	0	29	29	0	58	58
Prosecutor	0	3	3	0	6	6
Court Clerk	1	3	4	2	6	8
Registrar	0	1	1	0	2	2
Interpreter	1	3	4	2	6	8
Total	2	48	50	4	96	100

Source: Field data 2024

The table above shows data on whether the court has dedicated personnel apportioned to deal with cybercrime cases. 9 magistrates/ judges representing 18% said that both high court and subordinate courts do not have dedicated personnel apportioned to deal with cybercrime cases. 29 lawyers representing 58% said that both high court and subordinates court does not have dedicated personnel apportioned to deal with cybercrime cases. 3 prosecutors representing 6% said that both high court and subordinates court does not have dedicated personnel apportioned to deal with cybercrime cases. 1 court clerk representing 2% stated both high court and subordinates court have dedicated personnel apportioned to deal with cybercrime cases. 3 court clerks representing 6% stated both high court and subordinates court does not have dedicated personnel apportioned to deal with cybercrime cases. 1 high court registrar representing 2% said that both high court and subordinates court does not have dedicated personnel apportioned to deal with cybercrime cases. 1 interpreter representing 2% stated both high court and subordinates court have dedicated personnel apportioned to deal with cybercrime cases and 3 interpreters representing 6% stated both high court and subordinates court does not have dedicated personnel apportioned to deal with cybercrime cases.

These results reveal that both the high court and subordinate courts have no dedicated personnel apportioned to deal with cybercrime cases. As the results have shown, there is a lack of expertise in the high court and subordinate courts which hinders effective investigation and prosecution of cybercrime. Hence, there is a need for the high court and subordinate courts to have dedicated personnel apportioned to deal with cybercrime cases. These findings are similar to Mwape (2021).

If there is a streamlined process for obtaining and admitting digital evidence in court.

Streamlined process for obtaining and admitting digital evidence in court(n=50).

	Frequency	Frequency	Frequency total	%	%	total %
	yes	no		yes	no	
Judge/magistrate	8	1	9	16	2	18
Lawyer	26	3	29	52	6	58
Prosecutor	3	0	3	6	0	6
Court Clerk	2	2	4	4	4	8
Registrar	1	0	1	2	0	2
Interpreter	1	3	4	2	6	8
Total	41	9	50	82	18	100

Source: Field data 2024

Table above shows data on whether there is a Streamlined process for obtaining and admitting digital evidence in court. 8 magistrates/ judges representing 16% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court. 1 magistrate/ judges representing 2% said that both at the high court and subordinate courts there is no streamlined process for obtaining and admitting digital evidence in court. 26 lawyers representing 52% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court. 3 lawyers representing 6% said that both at the high court and subordinate courts there is no streamlined process for obtaining and admitting digital evidence in court. 3 Prosecutors representing 6% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court. 2 court clerks representing 4% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court. 2 court clerks representing 4% said that both at the high court and subordinate courts there is streamlined process for obtaining and admitting digital evidence in court. 2 court clerks representing 4% said that both at the high court and subordinate courts there is no streamlined process for obtaining and admitting digital evidence in court. 1registrar representing 2% said that both at the high court and subordinate courts there is streamlined process for obtaining and admitting digital evidence in court. 8 magistrates/ judges representing 16% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court. 1interpreter 2% said that both at the high court and subordinate courts there is a streamlined process for obtaining and admitting digital evidence in court and 3 interpreter 6 % said that both at the

high court and subordinate courts there is no streamlined process for obtaining and admitting digital evidence in court.

These results reveal that both the high court and subordinate courts have a streamlined process for obtaining and admitting digital evidence in court. The majority of the respondents, being judges and lawyers, confirmed that there is an existing procedure on how digital evidence is obtained and administered in courts. This implies that the courts have had a streamlined process which they employ when it comes to the handling and administration of digital evidence in courts. The minority of the findings being prosecutors, interpreters, and a registrar were of the thought that the processes in the courts were not streamlined, and the obtaining and admission of digital was a challenge in the courts. These findings are contrary to Chanda (2020).
If the court has the necessary technological infrastructure to support cybercrime investigations and prosecutions.

Technological infrastructure supporting cybercrime investigations and prosecutions(n=50).

	Frequency	Frequency	Frequency total	%	%	total %
	yes	no		yes	no	
Judge/magistrate	1	8	9	2	16	18
Lawyer	3	26	29	6	52	58
Prosecutor	0	3	3	0	6	6
Court Clerk	2	2	4	4	4	8
Registrar	0	1	1	0	2	2
Interpreter	1	3	4	2	6	8
Total	7	43	50	14	86	100

Source: Field data 2024

The table above shows data on whether the court has the necessary technological infrastructure to support cybercrime prosecution. 1 magistrate/ judge representing 2% said that both the high court and subordinate courts have the necessary technological infrastructure to support cybercrime prosecution. 8 magistrates/ judges representing 16% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution. 3 lawyers representing 6% said that both at the high court and subordinate courts have the necessary technological infrastructure to support cybercrime prosecution. 26 lawyers representing 52% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution. 3 prosecutors representing 6% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution. 2 court clerks representing 4% said that both the high court and subordinate courts have the necessary technological infrastructure to support cybercrime prosecution. 2 court clerks representing 4% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution. 1 registrar representing 2% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution. 1 interpreter representing 2% said that both at the high court and subordinate courts have the necessary technological infrastructure to support cybercrime prosecution. 3 interpreters representing 6% said that both at the high court and subordinate courts there is no necessary technological infrastructure to support cybercrime prosecution.

These results reveal that both the high court and subordinate courts have no necessary technological infrastructure to support cybercrime prosecution. As the results have shown, the lack of necessary technological infrastructure hinders the effectiveness of the court in investigation and prosecution of cybercrime. Hence, there is a need for the high court and subordinate courts to have the necessary technological infrastructure to deal with cybercrime cases. These findings coincide with Chileshe and Smith, (2018).

If the court has mechanisms in place to protect the confidentiality and integrity of digital evidence.

Mechanisms in place to protect the confidentiality and integrity of digital evidence(n=50).

	Frequency	Frequency	Frequency total	%	%	total %
	yes	no		yes	no	
Judge/magistrate	8	1	9	16	2	18
Lawyer	26	3	29	52	6	58
Prosecutor	3	0	3	6	0	6
Court Clerk	2	2	4	4	4	8
Registrar	1	0	1	2	0	2
Interpreter	3	1	4	6	2	8
Total	43	7	50	86	14	100

Source: Field data 2024

Table above shows data on whether the high court and subordinate courts have mechanisms in place to protect the confidentiality and integrity of digital evidence. 8 magistrate/ judge representing 16% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 1 magistrate/ judge representing 2 % said that both in the high court and subordinate courts there are no mechanisms in place to protect the confidentiality and integrity of digital evidence. 26 lawyers representing 52% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 3 lawyers representing 6 % said that both in the high court and subordinate courts there are no mechanisms in place to protect the confidentiality and integrity of digital evidence. 3 prosecutors representing 6% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 2 court clerks representing 4% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 2 court clerks representing 4 % said that both in the high court and subordinate courts there are no mechanisms in place to protect the confidentiality and integrity of digital evidence. 1 registrar representing 2% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 3 interpreters representing 16% said that both in the high court and subordinate courts there are mechanisms in place to protect the confidentiality and integrity of digital evidence. 1 interpreter representing 2 % said that both in the high court and subordinate courts there are no mechanisms in place to protect the confidentiality and integrity of digital evidence.

These results reveal that both the high court and subordinate courts have mechanisms in place to protect the confidentiality and integrity of digital evidence. The majority of the respondents, being judges and lawyers, confirmed that there is a mechanism in place to protect the confidentiality and integrity of digital evidence in courts. This implies that the courts have had a mechanism in place to protect the confidentiality and integrity of digital evidence in courts. These findings are contrary to the findings of Buchanan (2020).

5. Conclusions

The study was conducted to investigate the Zambian courts adequacy to prosecute cybercrime cases. The following is what were revealed by this study; that both the high court and subordinate courts had no dedicated personnel apportioned to deal with cybercrime cases, that both the high court and subordinate courts has no necessary technological infrastructure to support cybercrime investigations and prosecutions and on the other hand that both the high court and subordinate courts have a streamlined process for obtaining and admitting digital evidence in court, and that both the high court and subordinate courts have mechanisms in place to protect the confidentiality and integrity of digital evidence. The study recommends that there is need for both high courts and subordinate courts to be equipped with necessary technological infrastructure to support cybercrime prosecutions and the judiciary should also consider having dedicated personnel who are expert to be apportioned to deal with cybercrime cases in both high courts and subordinate courts.

Author Contributions: The author confirms sole responsibility for the following: study conception and design, data collection, analysis and interpretation of results, and manuscript preparation.

Funding: This research received no external funding.

Acknowledgments: The author thanks Africa Research University for approving their study as this is an extract from a PhD Thesis.

Conflicts of Interest: The authors declare no conflicts of interest.

6. References

1. Babbie, E. (2015). The Basics of Social Research. Cengage Learning.
2. Bellovin, S. M. (2007). "Thinking Security: Stopping Next Year's Hackers." Addison-Wesley.
3. Brennan, M. (2018). "Building Cybercrime Capacity: A Training Model for Legal Professionals." Journal of Digital Forensics, Security and Law, 13(2), 11-24.
4. Brenner, S. W. (2010). "Cybercrime: Criminal Threats from Cyberspace." ABC-CLIO.
5. Buchanan, B. G., et al. (2020). "Ethics of Digital Forensics." ACM Computing Surveys, 53(3), 1-32.
6. Casey, E. (2018). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press.
7. 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
8. Chileshe, A., B., & Smith, J. (2018). Examining the Technological Infrastructure for Cybercrime Prosecutions. *Journal of Cybersecurity Research*, 12(3), 45-60.
9. Chiluba vs Mkandawire (1999)
10. Choo, K. R. (2011). "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws." International Journal of Digital Evidence, 9(2), 1-18.
11. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications.
12. Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications.
13. Creswell, J. W., & Creswell, J. D. (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Sage Publications.
14. Décary-Hétu, D., et al. (2016). "The Role of Digital Evidence in the Identification and Prosecution of Traffickers." International Journal of Cyber Criminology, 10(1), 40-63.
15. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method.* John Wiley & Sons.
16. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method.* John Wiley & Sons.
17. Goldsmith, J., & Wu, T. (2006). "Who Controls the Internet? Illusions of a Borderless World." Oxford University Press.
18. Holt, T. J., & Bossler, A. M. (2016). "An Assessment of Cybercrime Training and Education Needs for Criminal Justice Professionals." International Journal of Cyber Criminology, 10(1), 1-20.
19. Kerr, O. S. (2014). "A Theory of Law." Harvard Law Review, 127, 789-934.
20. 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.
21. Kshetri, N. (2018). "Cybercrime and Cybersecurity in the Global South." Springer.
22. Maluleke, W. (2023) Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. International Journal of Social Science Research and Review, 6, 223-243.
23. Marotta, G., et al. (2019). "Digital Forensics and Cyber Crime: 12th International Conference, ICDF2C 2020." Springer.
24. Mwansa, P., & Kabwe, H. (2019). "Adapting Legal Frameworks: Enhancing Cybercrime Legislation in Zambia." *Zambian Journal of Legal Studies*, 14(3), 245-263.
25. Neuman, W. L. (2013). Social Research Methods: Qualitative and Quantitative Approaches. Pearson.
26. Njovu, S.M. (2020) Cybercrime and a Critique on the Effectiveness of Cyber Laws in Zambia. Doctoral Dissertation, Cavendish University, Kampala.
27. Pallant, J. (2021). *SPSS Survival Manual: A Step-by-Step Guide to Data Analysis Using IBM SPSS* (7th ed.). Open University Press.
28. Siampondo, G. 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. doi: 10.4236/jis.2023.144017.
29. Sichula, A. (2023, June 17th) Police formally charge Mwamba, Luchinde of forgery, false publication. Zambian Monitor Newspaper, https://www.zambiamonitor.com/police-formally-charge-mwamba-luchinde-of-forgery-false-publication/
30. Svantesson, D. J. B. (2015). "The Oxford Handbook of International Cyber Law." Oxford University Press.
31. Taylor, R. W., et al. (2016). "Cybercrime and Digital Forensics: An Introduction." Routledge.
32. Kaumba, M (2022, January, 3rd) Police Record 78 Cyber Crimes Cases. ZNBC, https://www.znbc.co.zm/news/police-record-78-cyber-crimes-cases/