EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Preventing and Combating Cybercrimes: Case of Cybercrimes Investigation Unit of Tanzania Police

Edgar Rogart Massawe
Department of Informatics, Institute of Accountancy Arusha, P.O.BOX 2798 Arusha, Tanzania

Juma Ally Mshana
Senior Lecturer, Department of Informatics, Institute of Accountancy Arusha, P.O.BOX 2798 Arusha, Tanzania

Suggested Citation

Massawe, E.R. & Mshana, J.A. (2023). Preventing and Combating Cybercrimes: Case of Cybercrimes Investigation Unit of Tanzania Police. *European Journal of Theoretical and Applied Sciences, 1*(5), 1179-1190.
DOI: 10.59324/ejtas.2023.1(5).102

Abstract:

The study was conducted at the cybercrimes investigation unit of Tanzania Police Force. The study investigates the current situation of Tanzania Police Force on combating and preventing cybercrimes in Tanzania and examine the effect of the current legal framework governing them on preventing and combating cybercrime. The study used a sample size of 86 respondents from cybercrimes investigation unit at Tanzania Police Force. Data collection was done by using interview guide and questionnaire. The data was analysed by using multiple regression model and thematic analysis for quantitative and qualitative data respectively. The findings show that, Cybercrimes in Tanzania is on high rate as justified by the respondents regarding on number of reported cases of cybercrimes in Dar es Salaam despite of effort shown by Police Force to battle this problem. It was also found that a unit increases in technological capability of Police Force lead to significant decreases in preventing and combating cybercrimes. Furthermore, the results show that, other things remain constant, a unit increase in the current legal framework governing the Police Force lead to significant decrease of effort on preventing and combating cybercrimes. Therefore, it is recommended that there is a need for the Police Force to invest more in acquiring new technologies well as providing continuous public awareness of cybercrimes. Also cybercrime act of 2015 as well as legal and regulatory compliances governing all cybercrimes stakeholders to be reviewed so that can enable Police Force to perform their duties of preventing and combating cybercrimes efficiently.

Keywords: *Tanzania Police Force, Cybercrimes, Technological Capability, Legal Framework.*

Introduction

There is no universally accepted definition of cybercrime but can be defined as offences committed against computer data, computer data storage media, computer systems, service providers. This thought regularly covers kinds of offences such as illegal access, interfering with data and computer systems, fraud and forgery, illegal interception of data, illegal devices, child exploitation and intellectual property infringements (INTERPOL National Cybercrime Strategy Guidebook, 2021). In cybercrime offences, computer may have been used as a tool to commit an offence or as a target. Cybercrime may threaten a person, company or a nation's security and financial health (Kshetri, 2017). According to security professionals, many cybercrime arise from the African countries, and spread threat easily because many computer

systems are not accurately secured (Cross, 2021) The combating against cybercrime need a strong and coordinated method, but in Africa, poverty and underdevelopment are the main causes for increase of cybercrime in the countries (Lallie *et al.*, 2020)

Cybercrime have been observed to be a big agenda worldwide due to its negative impacts that is why many researchers are invited to study solution that will help laws enforcement organs to prevent and combating it. The studies conducted by Kshetri (2017) and Cross (2021) found that Africa is a most attractive ground for cybercrime activities because of the technology advancement, high crime rate and lack of legislation in some countries. Cyber security professionals think that 75 percent of electronic devices in Africa are already attacked with viruses and other forms of attacks (Lallie *et al.*, 2020). This shows that, the African continent is a place where cybercrime and cybercriminals may operate easily, due to the observed increase in number of "new" internet users who are not security consciousness (Symantec, 2016).

As of June 2021, Tanzania had 33.2 million mobile money accounts relying on a network of agents managing transactions across rural and urban areas (TCRA Statistics report 2021/2022). The number of mobile connections in January 2021 was equivalent to 82.7% of the total population. Due to this statistics, Tanzania found to be fertile ground for cybercrime activities and where the need for fighting against it raised. Like many other countries around the globe; Tanzania has embraced ICT as a key enabler for educational, social and economic development in the country, however, the country faces challenges of cybercrimes. Cybercrime in Tanzania is increasing and the country has been experiencing massive cyber-attacks on their websites/ISs since January 2010 up to June 2013 (TCRA Statistics report 2021/2022). Tanzania mostly experiencing these types of cybercrimes such as computer related fraud, illegal access, pornography, publication of false information, denial of service, cyber bullying, unsolicited message (ile ela tuma kwa namba hii) (Pallangyo, 2022) and most of them have been reported to cybercrimes investigation unit but preventing and combating them is observed to be a challenging task (Bakar, Issa Hamad, 2016).

The literature review has revealed various studies across the world that has conducted by researchers across different geographic location in the field of cybercrime. But there are very few studies that address the Challenges of preventing and combating cybercrime in Dar es salaam, Tanzania specifically in cybercrime investigation unit within Tanzania Police Force. Therefore, this study targeted to bridge the gaps by examine the challenges facing Tanzania Police Force in preventing and combating cybercrimes in Dar es salaam, Tanzania specifically in cybercrime investigation unit within Tanzania Police Force. It is a motivating research area in Tanzania where by many cases of such crimes have been reported, since establishment of cybercrime investigation unit hence it provides a room for research to find out the challenges for this social problem.

Literature Review

Preventing and combating refer to effort established by Tanzania Police Force specifically cybercrime investigation unit to detect the crime liquidate it before or after its occurrence in cyber space, hardware or in software. The study conducted by Al-Zoubi (2013) reveal that relative advantage has a positive significant relationship with e-business adoption in fighting against physical theft. Financial resources have a positive and insignificant relationship with e-business adoption in fighting against physical theft (Al-zoubi, 2013). Technology capability has a positive and significant relationship with e-business adoption in fighting against physical theft. Government has a positive and significant relationship with e-business adoption in fighting against physical theft (Al-zoubi, 2013). Top Management Support has a positive and insignificant relationship with e-business adoption. Legal framework has a positive and insignificant relationship with e-business adoption in fighting against physical theft (Al-zoubi, 2013). The study used structural equation

method to meet the study objectives (Al-zoubi, 2013).

The study conducted by Chong and Olesen (2017) legal framework has a positive and significant relationship with Fighting Cybercrimes in Africa (Chong and Olesen, 2017). Compatibility) has significant positive relationship with Fighting Cybercrimes in Africa. Complexity has a positive significant relationship with Fighting Cybercrimes in Africa (Chong and Olesen, 2017). Financial resources have a positive significant relationship with Fighting Cybercrimes in Africa. Regulatory support has a positive significant relationship with Fighting Cybercrime in Africa (Chong and Olesen, 2017). The study used a quantitative method to meet the study objectives.

The study conducted by Lin (2013) reveals that legal framework has a positive and significant relationship with the rapid growth of cybercrimes affecting information systems in the global. Government support has significant positive relationship with the rapid growth of cybercrimes affecting information systems in the global (Lin, 2013). Financial resources have a negative significant relationship with the rapid growth of cybercrimes affecting information systems in the global (Lin, 2013). Technology Compatibility has a positive and insignificant relationship with the rapid growth of cybercrimes affecting information systems in the global. Regulatory support has a positive and significant relationship with the rapid growth of cybercrimes affecting information systems in the global. The data to test were obtained by using a mail survey of large Taiwanese companies to meet the study objectives (Lin, 2013).

The study conducted by Chong and Olesen (2017) legal framework has a positive and significant relationship with Fighting Cybercrimes in Africa (Chong and Olesen, 2017). Compatibility) has significant positive relationship with Fighting Cybercrimes in Africa. Complexity has a positive significant relationship with Fighting Cybercrimes in Africa (Chong and Olesen, 2017). Financial resources have a positive significant relationship with Fighting Cybercrimes in Africa. Regulatory support has a positive significant relationship with Fighting Cybercrime in Africa (Chong and Olesen, 2017). The study used a quantitative method to meet the study objectives

The study conducted by Kuan et al (2021) reveals that budget has a positive and significant relationship with cybercrime security in Tanzania. Government support has significant and negative relationship with cybercrime security in Tanzania. Complexity has a positive significant relationship with cybercrime security in Tanzania (Kuan et al, 2021). Financial resources have a positive and insignificant relationship with cybercrime security in Tanzania. Regulatory support has a positive and significant relationship with cybercrime security in Tanzania (Mayunga, 2013). The study used a survey method to meet the study objectives.

The literature review has revealed various studies across the world that has conducted by researchers across different geographic location in the field of cybercrime. But there are very few studies that address the Challenges of preventing and combating cybercrime in Dar es salaam, Tanzania specifically in cybercrime investigation unit within Tanzania Police Force.

Therefore, this study targeted to bridge the gaps by examine the challenges facing Tanzania Police Force in preventing and combating cybercrimes in Dar es salaam, Tanzania specifically in cybercrime investigation unit within Tanzania Police Force. It is a motivating research area in Tanzania where by many cases of such crimes have been reported, since establishment of cybercrime investigation unit hence it provides a room for research to find out the challenges for this social problem.

Material and Methods

The study on Tanzania Police Force on preventing and combating cybercrimes in Tanzania was conducted at the cybercrimes investigation unit of Tanzania Police Force with the aim of investigating the current situation of Tanzania Police Force on combating and preventing cybercrimes and examine the effect of the current legal framework governing the

force on preventing and combating cybercrimes in Tanzania.

Area of the Study

The study was conducted in Dar es Salaam City. Specifically, the researcher obtained data from the cybercrimes investigation unit of the Tanzania Police Force (TPF). The choice of this area is because it is a public agency which is responsible for detecting, preventing, combating and liquidating cybercrime in Tanzania (Liu et al, 2018).

Research Design

The current study used exploratory sequential design to study the challenges facing Tanzania Police Force in preventing and combating cybercrimes. In an exploratory sequential design, qualitative data collection and analysis occurs first, followed by quantitative data collection and analysis. The researcher first of explored initial question for the first objective and develop hypotheses for the second, third and fourth hypothesis.

Research Approach

This study used mixed research approach. Mixed methods research combines elements of quantitative research and qualitative research in order to answer the research question or hypothesis. Mixed methods can help to gain more complete picture than a standalone quantitative or qualitative study, as it integrates benefits of both methods (Sausi et al, 2021). The mixed methods approach was used in this study because of two reasons; first, it is because the nature of the objectives of the current study involves one qualitative objective and quantitative objective. Second, the mixed approach was used because the researcher wanted to gain more complete picture that standalone quantitative or qualitative study cannot.

Targeted Population

The targeted population of this study comprised of Tanzania Police Officers who are currently employed and working at the cybercrimes investigation unit. The target population size was 110 Police officers (Officer Commanding CID) in the cybercrimes investigation unit in Dar es Salaam City.

Sample Size

A sample size of 86 Police officers from the cybercrimes investigation unit will be selected to participate in this study. Yamane's mathematical formula was used to determine the sample size. The formula has been commonly and widely applied by other researchers. Yamane's formula has been stated below where "n" represents the sample size, "N" represents the population of the study and "e" represents the margin of error = 0.05.

Yamane's formula:

$$n = \frac{N}{(1+Ne^2)} \quad (1)$$

$$n = \frac{110}{(1+110*0.05^2)} = 86.275$$

$$n = 86$$

Therefore, a sample size of 86 Police officers from the cybercrimes investigation unit was selected to participate in this study. Since this study is mixed, from the sample size of 86 respondents, 10 respondents were interviewed to respond to questions under objective one.

Sampling Strategies

According to Bryman (2016) sampling is a systematic process of choosing a sub-group from a population to participate in the study. It is the process of selecting several individuals for a study in such a way that the individuals selected represent the large group from which they were selected (Nord, 2020). This study used a simple random sampling to obtain respondents from the population (Bryman, 2016)

Data Collection Tools

Questionnaire

The study used an online administered close-ended questionnaire to collect data for objective two to four. The close-ended questionnaire involves questions that require the respondent to

respond to the questions by using a certain scale of measurement (Kumar, 2018). The first part of the questionnaire gathered details about the demographic characteristics of the respondents; gender, age, experience. The second part of the questionnaire solicited information relating to the specific objectives of the study. This involved the use of the measurement statements based on prior literature that capture (operationalize) the studied constructs.

Interview Guide

In this study, the interviews were conducted to answer objective one. The main aim was to extract main themes from the interview, these themes were discussed in relation to the objective.

Data Analysis

This study collected both qualitative and quantitative data**.** The collected quantitative data were analyzed by using multiple linear regressions under statistical package for social science (SPSS). This research used two-step analytical procedure, which include assessment on the validity and reliability of the measurement model and the linear regressions which analyzed the hypotheses relationships established in the study model. Qualitative data was analysed by using thematic analysis**.** In the study, the researcher followed all procedures of analyzing qualitative data through thematic analysis.

Validity and Reliability

Validity measurement was performed to determine the degree at which measurement instruments are measuring what is supposed to be measured in the study, the test was performed through Kaiser-Mayer Olkin (KMO) and Bartlett's Test to assess the proportion of variance in the variables that might be influenced by the underlying factor in the research model. The Kaiser-Mayer Olkin (KMO) and Bartlett's Test is based on assumption that the result score closer to 1 or 100% implies that variables are valid and good measure of data and appropriate for analysis. According to table 2, the gathered data have Kaiser-Mayer Olkin (KMO) and Bartlett's Test have score of 0.851 (85.1%) which means there is good measurement of data and Chi-Square of 858.825 with significant values of 0.000 that less than P-Values 0.05 indicating statistically significant for the data.

On the other hand, data reliability shows the degree to which an instrument measures accurately what it claims to measure. The researcher analyzed the data by using SPSS tool where reliability of data was assessed based on Cronbach's alpha value which its cut point is > 0.7 (Lwoga & Komba, 2015). A Cronbach's Alpha test was applied to test the internal consistency of measurement instruments, the test was conducted to assess the ability and accuracy of information gathered to provide answers toward the challenges faced by Tanzania Police Force in preventing and combating cybercrimes. According to the results in Table 1, Cronbach's Alpha test based on standardized Items is 0.798 that is 79.8% which is above 75% and close to 100% implies that there is greater consistency internally among the variable in the scale of measurement suggested by (Cronbach, 1955). And this means the gathered information was good for further analysis.

Table 1. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0.851
Bartlett's Test of Sphericity	Approx. Chi-Square	858.825
	Df	153
	Sig.	0

Source: Data Analysis.

Table 2. Reliability Statistics

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.791	0.798	18

Source: Data Analysis.

Trustworthiness of the Interview Guide

Credibility, transferability, dependability, and confirmability are the four primary criteria, according to Creswell (2012) that qualitative researchers must demonstrate in order to guarantee the reliability of the study's findings. In this study, the researcher guaranteed the reliability of the interview guide through multiple viewpoints throughout the data gathering process to verify that the qualitative data were adequate. This was accomplished by member or participant validation, rigorous data collection methods.

Ethical Consideration

The participants were allowed to freely withdraw from the research without any obligations and all information acquired from the respondents was treated with confidentiality without disclosure of the respondents' identity. In ensuring the privacy of respondents, the names were not disclosed. Additionally, there was no information modified. Information acquired, were presented as collected and all the literatures collected and reviewed for this study purpose were all cited and appreciated in the reference list.

Results

Demographic Data

In assessing the magnitude of challenges faced by Tanzania Police Force in preventing and combating cybercrimes, the study took into consideration characteristics of respondents such as their rank, age, gender, education level and working experience as summarized in Table 3 and results was presented as follows:

The findings in table 3 shows the ranks of the respondents, 6 (7%) respondents were Gazetted officers, 37 (43%) respondents were Inspectors while Rank and File were 43 (50%) respondents. This diversity in ranks of the respondents helped the researcher to collect responses from different respondents basing on their experience in Tanzania Police Force especially the cybercrimes investigation unit**.** The results in table 3 shows that 12 (14%) respondents were in 26-35 age group, 42 (49%) respondents were in 36-50 age group while 32(37%) respondents were in 50 and above age group. This indicates that all respondents had diversity in ages, this was beneficial to the current study as they gave responses according to their level of understanding basing on their level of understanding which in fact is always different from one person to another.

The study assessed gender of respondents to indicate inclusiveness of gender in the study, Male are 66 (76.7%) respondents and female are 20 (23.3%) respondents as shown in table 3, this indicates that this diversity in gender has brought constructive diversity in responses.

Respondents was asked to share their education level with questionnaire, according to finding of the study that presented in table 3; 13 (15.1%) respondents had secondary education, 21(24.4%) had diploma level of education, 45 (52.4%) respondents had bachelor's education, and 7 (8.1%) had master's degree and above. The findings suggest that the findings of the current study were from people with diversity in education level.

According to table 3 more than 9 (10.5%) respondents had 1 to 5 years of working experience, 22 (25.6%) had 6 to 10 years of working experience and 55 (64%) respondents had more than 10 years of working experience. With these findings on working experience, the responses of respondents on the objectives of the study were from people with enough experience in cybercrimes matters.

Table 3. Demographic Characteristics

Rank	Frequency	Percent
Age of respondents		
Gazetted Officer	6	7

Inspector	37	43
Rank and file	43	50
Total	86	100
Age of respondents		
26-35	12	14
36-50	42	49
50 and above	32	37
Total	86	100
Gender of respondents		
Male	66	76.7
Female	20	23.3
Total	86	100
Education level of respondents		
Secondary education	13	15.1
Diploma level	21	24.4
Bachelor degree	45	52.4
Master's degree and above	7	8.1
Total	86	100
Working experience of respondents		
1 to 5 years	9	10.5
6 to 10 years	22	25.6
more than 10 years	55	64
Total	86	100

Source: Interview Data (2023)

Current Situation of Tanzania Police Force on Combating and Preventing Cybercrimes in Tanzania

The first objective of the current study focused on exploring the current situation of Tanzania Police Force on combating and preventing cybercrimes. The data for this objective were collected by using interview guide from the field. The analysis of this objective was based on content or thematic analysis. Content or thematic analysis focuses on extracting main themes from the interview transcripts or quotations. Table 4 shows the main themes extracted after the interview was conducted with respondents.

Table 4. Main Themes Extracted during an Interview Concerning the Current Situation of Tanzania Police Force on Combating and Preventing Cybercrimes

Verbatim Quotes	Themes	Code
The cybercrimes is currently a burning issue in Tanzania, this is proved by the high rate of reported cases in Police stations in Dar es Salaam	**High rate of cybercrimes cases in Dar es Salaam**	MT1
It is true that we have demonstrated our endless effort to prevent and control cybercrimes by educating the public through mass media and arresting those involved in these crimes. We have been using online patrol and human intelligence to identify and arresting suspects of cybercrimes.	**Endless efforts in preventing and combating cybercrimes**	MT2
Despite of having cybercrimes act and other related laws there is need close and promptly cooperation from MNO's on providing personal information of their customers suspected to commit cybercrimes. Also currently in Tanzania there is implementation of personal data protection Act, this in other hand can cause some interruptions to Police Force Tanzania on obtaining personal information of the suspects during investigation.	**Legal framework is not supportive**	MT3

Source: Interview Data (2023)

Table 4 shows verbatim quotes, main themes and the codes assigned to the main themes. The analysis shows that there are three main themes that were identified during an interview. They are discussed below;

High Rate of Cybercrimes Cases in Dar es Salaam (MT1)

The respondents argued that the current situation of cybercrimes in Dar es Salaam is characterized by high rate of cybercrimes in Dar es Salaam city. This is witnessed by the number cybercrimes cases reported in Police stations in Dar es Salaam. One of the respondents in Dar es Salaam had this to say;

> **"***The cybercrimes is currently a burning issue in Tanzania, this is proved by the high rate of reported cases in Police stations in Dar es Salaam" – a respondent during an interview in Dar es Salaam, August, 2023.*

Endless Efforts in Preventing and Combating Cybercrimes (MT2)

The current situation of the cybercrimes in Tanzania especially in Dar es Salaam is dominated by endless efforts shown by Tanzania Police Force. Although there are so many challenges but one of the respondents said that, Tanzania Police Force is battling the problem of cybercrimes endlessly. There was a respondent who said that;

> *"It is true that we have demonstrated our endless effort to prevent and control cybercrimes by educating the public through mass media and arresting those involved in these crimes. We have been using online patrol and human intelligence to identify and arresting suspects of cybercrimes." – a respondent in Dar es Salaam, August 2023.*

Legal Framework is Not Supportive (MT3)

This was another main theme identified during an interview, the current legal framework was evaluated by the respondents that it is not supportive. The current legal framework impinges with personal data protection Act. With this situation, the access for information regarding the cybercrimes is very challenging. The respondent had this to say;

> *"Despite of having cybercrimes act and other related laws there is need close and promptly cooperation from MNO's on providing personal information of their customers suspected to commit cybercrimes. Also currently in Tanzania there is implementation of personal data protection Act, this in other hand can cause some interruptions to Police Force Tanzania on obtaining personal information of the suspects during investigation." – One of respondents in Dar es Salaam, August, 2023.*

Effect of the Current Legal Framework Governing the Police Force on Preventing and Combating Cybercrime in Tanzania

The second objective of the current study focused on examining the effect of the current legal framework governing the Police Force on preventing and combating cybercrime in Tanzania; according to MLR in table 5, the current legal framework governing the Police Force has slope coefficient *(β)* of -0.537with its P-Value (Sig.) of 0.000 that is less than 0.05 level of significance. The second null hypothesis was rejected at p-value 0.000 that is less than the level of significance (0.05). This indicates that, other things remain constant, a unit increase in the current legal framework governing the Police Force lead to significant decrease of effort on preventing and combating cybercrimes in Tanzania by 0.537.

The effect of current legal framework governing the Police Force on preventing and combating cybercrimes in Tanzania, was also measured by using the mean value of the Likert scale, the five level Likert scale measurement with a decision matrix where 1=strongly disagree (1.00-1.80), 2=disagree (1.80-2.60), 3=Undecided (2.60-3.40) 4=agree (3.40-4.20), 5= strongly agree (4.20-5.00). according to the result as indicated in table 6 respondents disagreed that the current legal framework governing the Police Force is not a challenge on preventing and combating cybercrimes in Tanzania, because its mean value was 3.0 found on the range of 3 = undecided (2.60-3.40). These descriptive data conquer with the regression results which have shown negative relationship between the current legal

framework of the Tanzania Police Force and prevention of cybercrimes in Tanzania.

Table 5. Multiple Regression Model Results

	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	4.715	0.378		12.467	0
LEGAL FRAMEWORK	-0.537	0.145	-0.465	-3.715	0

Table 6. Mean Value for 5 - Point Likert Scale Responses

Item Statistics		
	Mean	N
Available laws governing cybercrimes is not enough in preventing and combating cybercrimes.	3.4419	86
Difference in legal systems between countries is not a challenge in preventing and combating cybercrimes in Tanzania.	2.4302	86
Stakeholder's legal compliance in providing on time information concerning their customers who suspected to commit cybercrimes is not enough in preventing and combating cybercrimes.	4.4186	86
Court Jurisdiction in cybercrimes prosecution is not a challenge in preventing and combating cybercrimes in Tanzania.	2.2442	86
Cybercrimes act and other related cyber laws awareness to society is not a challenge in preventing and combating cybercrimes in Tanzania.	2.6279	86

Source: Survey Data, 2023

Discussion of Findings

The current study based on examining the Tanzania Police Force on preventing and combating cybercrimes in Tanzania: a case of cybercrimes investigation unit of Tanzania Police Force. The first objective of this study was based on exploring the current situation of Tanzania Police Force on combating and preventing cybercrimes in Tanzania. The findings of the first objective suggest that, the government of Tanzania through responsible law enforcement agent is showing effort to battle this problem. On the other hand, cybercrimes in Tanzania is on high rate as this was justified by the respondents that, the reported cases on cybercrimes in Dar es Salaam Police stations are many. With this increase, still the infrastructures to support the cybercrimes investigation unit are still not enough. The issue of high increase in the rate of cybercrimes is not reported only in Dar es Salaam in Tanzania, the same issue was also reported by Datta, Panda, Tanwar and Kaushal (2020) in India that the ratio of cyber-crime in India is constantly rising due to various reasons. Cyber-criminals are very difficult to trace and this advantage is fully utilizing by scammers. Furthermore, it has been established by Sviatun, Goncharuk, Roman, Kuzmenko and Kozych (2021) that the level of cybercrime in the world and the economic consequences of its impact tend to increase. It is estimated that in 2020 the total cost of cybercrime and cybersecurity will exceed one trillion US dollars, which is more than 1% of world gross domestic product. The reasons have been determined why the number of cybercrimes are increasing (electronization and computerization of most industries, public sector; low level of operational cooperation; inconsistency of legal policy with the realities of cybercrime; development of cyber-attack mechanism; modernization of cybercrime; obstacles to international cooperation and so forth).

During an interview, more than three main themes were extracted; these include, High rates

of cybercrimes in Dar es salaam, Endless efforts in preventing and combating cybercrimes and also legal framework governing Police Force in preventing and combating cybercrimes was found to be a problem. The findings on objective one are supported by what Van Nguyen, Truong and Lai (2022) who explored the legal challenges of combating cybercrime in Vietnam. They reveal that Vietnam's fight against cybercrime still faces legal challenges, including traditional and novel ones. Moreover, active and flexible approaches within Vietnam's cyberspace management can increase the effectiveness of combating cybercriminal activities; however, they can cause concerns in balancing cybercrime control and human rights protection.

In objective two, the researcher targeted to determine the effect of current legal framework governing Tanzania Police Force on preventing and combating cybercrimes. The findings have shown that the current legal framework has negative relationship with preventing and combating cybercrimes. This means that, the current legal framework is reducing the efforts done to prevent and combating cybercrimes. The legal framework has been witnessed in other countries to be a challenging factor in preventing and controlling cybercrimes. For example, a study by Van Nguyen, Truong and Lai (2022) in Vietnam found that despite positive results, Vietnam's fight against cybercrime still faces legal challenges, including traditional and novel ones. Moreover, active and flexible approaches within Vietnam's cyberspace management can increase the effectiveness of combating cybercriminal activities; however, they can cause concerns in balancing cybercrime control and human rights protection. Another study by Siddik and Rahi (2020) in Bangladesh found that, the government enacted Information and Communication Technology Act to prevent the possible cybercrimes. But this legislation was not enough to combat with increasing cybercrimes committed by offenders. As such the government in 2018 enacted another piece of legislation namely the Digital Security Act. But to combat cybercrimes in social media especially in Facebook how much effective is this Digital Security Act and ICT Act is a great concern. The study revealed that the legal framework regulating cybercrime in Bangladesh is wide but technically hazardous and complicated.

Conclusion

Basing on the findings of the current study, the researcher makes the following conclusions; government of Tanzania is currently doing a good job in combating cybercrimes. The rate of cybercrimes is increasing day by day. The current legal framework brings difficulties in handling cybercrimes issues. The researcher recommends the following;

- There is need for the government of Tanzania to make collaboration with other countries so that our laws can be recognized and implemented in various countries; this will help the criminal to be arrested anywhere with our laws and brought to the country.

- Furthermore, a law should be made to allow the Police Force to access the customers' communication that they do through communication networks in the country. This will be done for the purpose of helping investigators to implement their responsibilities successful. Also, there should be no court jurisdiction to prosecute cases of cybercrimes.

- It is also recommended that, the Tanzania cybercrime act of 2015 should be reviewed and some offenses that are described in our penal code should be added in Tanzania cybercrime act of 2015. The cybercrime unit should be allocated enough budget to carry out its duties. Also funds for on-job training and education for the public should be allocated to build the capacity of detectives and deliver education to the public.

Acknowledgement

This study is the result of guidance and support from many individuals. Firstly, we thank God for the gift of life and health and for guiding me throughout the process of this study and for granting us wisdom, strength, and indeed to him,

everything is possible. Secondly, we take this opportunity to express a special thanks to all Staff, friends and colleagues at Institute of Accountancy Arusha - Dar es Salaam Campus who offered encouragement and support. Special thanks to Tanzania Police Force and their cybercrimes investigators who responded and supported us throughout the data collections process.

References

Al-zoubi, M. I. (2013). Predicting E- Business Adoption through Integrating the Constructs of the Rogers's Diffusion of Innovation Theory Combined with Technology- Organization-Environment Model. *IJACR, 3*(4), 2249-7277.

Bakar, I.H. (2016). *Social engineering tactics used in mobile money theft in Tanzania.* Dissertation. The University of Dodoma.

Bryman A. (2016). *Social Research Method,* fifth edition. UK: Oxford University Press.

Chong, J. L. L., & Olesen, K. (2017). A Technology-Organization Environment Perspective on Eco-Effectiveness: A Meta-Analysis. *Australasian Journal of Information Systems, 21,* 1-26. https://doi.org/10.3127/ajis.v21i0.1441

Cross, C. (2021). Dissent as cybercrime: social media, security and development in Tanzania. *Journal of Eastern African Studies, 15*, 442-463. https://doi.org/10.1080/17531055.2021.1952797

Datta, P., Panda, S.N., Tanwar, S. & Kaushal, R.K. (2020). A technical review report on cyber crimes in India. In *2020 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 269-275). IEEE.

INTERPOL. (2021). National Cybercrime Strategy Guidebook. Retrieved from https://www.interpol.int/content/download/16455/file/Cyber%20Strategy%20Guidebook.pdf

Klassen, A. C., Creswell, J., Plano Clark, V. L., Smith, K. C., & Meissner, H. I. (2012). Best practices in mixed methods for quality of life research. *Quality of life research : an international journal of quality of life aspects of treatment, care and rehabilitation*, *21*(3), 377–380. https://doi.org/10.1007/s11136-012-0122-x

Kshetri, N. (2017). Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy. *Telecommunications Policy, 41,* 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kuan, K.K., & Chau, P.Y. (2001). A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework. *Inf. Manag., 38*, 507-521. https://doi.org/10.1016/S0378-7206(01)00073-8

Kumar, R. (2018). *Research methodology: A step-by-step guide for beginners.* SAGE Publications Ltd.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

LinH. (2013). Technological Forecasting & Social Change Understanding the determinants of electronic supply chain management system adoption. Using the technology–organization-environment framework. *Technological Forecasting & Social Change, 86,* 80-92. https://doi.org/10.1016/j.techfore.2013.09.001

Lwoga, E. T. & Komba, M. (2015). Antecedents of continued usage intentions of web-based learning management system in Tanzania. *Education and Training, 57*(7), 738–756. https://doi.org/10.1108/ET-02-2014-0014

Mayunga J. (2013). *Cybercrime And Criminal Investigation: Challenges Within The Tanzania Police Force Forensic Laboratory: The Case Tanzania Police Force Head Quarters, Dar Es Salaam.* Dissertation. Mzumbe University Dar es- Salaam Campus College in Partial Fulfilment of the Requirements for the Award of the Degree of Master of Public Administration (MPA) of Mzumbe University.

Magalla, A. (2017). Magalla, Asherry, Human Rights Protection in Tanzania as Described by

the Cyber Crime Act, No.13. http://dx.doi.org/10.2139/ssrn.4134618

Mhina, J. R. A. (2020). Social Media and Government Employees in Tanzania'. In *Global Encyclopedia of Public Administration, Public Policy, and Governance,* pp. 1–15. https://doi.org/10.1007/978-3-319-31816-5_3688-1

Mphatheni, M.R. & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science (2147-4478), 11*(4), 384-396. https://doi.org/10.20525/ijrbs.v11i4.1714

Nfuka, E. N., Sanga, C., & Mshangi, M. (2020). The Rapid Growth of Cybercrimes Affecting Information Systems in the Global : Is this a Myth or Reality in Tanzania. I*nternational Journal of Information Security Science, 3*(2), 182–199.

Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. H. (2020). Information security policy compliance: Leadership, trust, role values, and awareness. *Journal of Computer Information Systems, 60*(1), 1–8. https://doi.org/10.1080/08874417.2019.1668738

Kiwango, T. A., & Omar, H. . (2021). Challenges Confronting Implementation of Electronic Human Resource Information System in Public Institutions. *The Accountancy and Business Review*, *13*(2), 51–63. https://doi.org/10.59645/abr.v13i2.28

Pallanyo H. J. (2022). Cyber Security Challenges, its Emerging Trends on Latest Information and Communication Technology and Cyber Crime in Mobile Money Transaction Services. *Tanzania Journal of Engineering and Technology, 41*. https://doi.org/10.52339/tjet.v41i2.792

Richard, M. (2022). Research in Business & Social Science Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *Tanzania Journal of Engineering and Technology, 11*(4), 384–396.

Semlambo, A. , Mfoi, D. and Sangula, Y. (2022) Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computer and Communications, 10,* 29-43. https://doi.org/10.4236/jcc.2022.1011003

Sausi J. M., Mtebe, J. & Mbelwa J. (2021). Sausi, John & Mtebe, Joel & Mbelwa, Jimmy. (2021). Evaluating user satisfaction with the e-payment gateway system in Tanzania. *SA Journal of Information Management, 23*(1), 1-9. https://doi.org/10.4102/sajim.v23i1.1430

Schjølberg S. (2017). *The History of cybercrime: 1976-2016*. Books on Demand.

Siddik, M.A.B. & Rahi, S.T. (2020). Cybercrime in Social Media and Analysis of Existing Legal Framework. Bangladesh in context. *BiLD Law Journal*, *5*(1), 68-92.

Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O. & Kozych, I.V. (2021). Combating cybercrime: economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751-762. https://doi.org/10.37394/23207.2021.18.72

Symantec. (2016). Cybercrime & Cybersecurity Trends in Africa. Retrieved from https://thegfce.org/cybercrime-and-cybersecurity-trends-in-africa/

TCRA Statistics report. (2021/2022).

Van Nguyen, T., Truong, T.V. & Lai, C.K. (2022). Legal challenges to combating cybercrime: An approach from Vietnam. *Crime, Law and Social Change*, pp.1-22.