Impact of Telecommunications Technology on Human Security: A Case of Tanzania

By
Einot Zablon Moses[1], *Darius Mukiza*[2] *& Albert Memba*[3]

Abstract
This paper examines the impact of telecommunications technology to human security of Tanzania. The study employed a cross- sectional research design, and the sample size of the study was 120 respondents. Data were collected through open and close-ended questionnaires and semi-structured interviews administered to staff from Tanzania Communications Regulatory Authority (TCRA), the police, selected mobile operators as well as mobile phone subscribers. Descriptive statistical analysis was applied for quantitative data while content analysis was adopted for qualitative data. Results revealed that identity theft, terrorism, money laundering, online money theft, human trafficking and drug trafficking were security threats aggravated by telecommunications technology. Also, the motivation factors for committing cybercrimes include poverty (financial gain), religious and political ideologies, and violent extremism. It is concluded that telecommunications technology aggravates security challenges, and it is suggested that the government should take institutional measures in developing cyber security culture in the fight against security threats.

Keywords: human security, securitization, telecommunications.

1.0 Introduction

Development in the telecommunications industry has brought many blessings in sectors like transport, education, health, finance and businesses. Telecommunication services are key to national economies and critical to national security (EC-RRG, 2014). However, these benefits are facing many risks. For example, a survey conducted among banks in Kenya, Rwanda, Uganda, Tanzania and Zambia revealed that banks were at high risks of being hacked by their own employees and other malicious insiders (Kshetri, 2019). In Ghana, the major issues confronting the banking industry were data safety and lack of trust

[1] PhD Candidate, The Open University of Tanzania (OUT) (einotm27@yahoo.com)
[2] University of Dar es Salaam, School of Journalism and Mass Communication (rugalama@gmail.com)
[3] The Open University of Tanzania (OUT) (almemba@gmail.com)

especially in Internet Banking. Fraudulent transactions and data robbery lead to perception and reputational problems (Ohene, 2015). Also, telecom networks which provide services integral to other sectors like finance, health and education are vulnerable to some risks (Bears, 2021). Increasingly, interconnected global supply chains make cyber-attacks and digital failures an ever present set of risks to business integrity (Adonis, 2018). Indeed, the world is depending on internet of things to meet different demands ranging from businesses, health, education and finance; however, as people and institutions go more 'online' the higher the risks they encounter.

2.0 Background to human insecurity in the digital age

Telecommunications infrastructure that provides the necessary backbone for information exchange such as voice, video, data, and Internet connectivity have been found to be vulnerable to various forms of attacks like denial of service, loss of integrity and lack of confidentiality of network services (Chukwudebe & Nosiri, 2015). For instance, countries such as Nigeria, India, Iraq, Syria, Nepal and Columbia experienced telecommunications infrastructural destruction due to insurgency or military conflicts. In 2012, Boko Haram (a terror group) in Nigeria destroyed about 530 base stations and killed staff (Agubor, et al., 2015).

The development of new accessible technologies and the expansion of the Internet have resulted in new forms of criminal behaviour. For example, Tropina (2016) stated that digital technologies facilitate the migration of traditional organised crime online and provide a number of opportunities for fraud, corruption, tax evasion and other criminal activities. It is easy to launch money laundering activities with the assistance of new technologies to include online banking and money transfers provided the criminals have all the necessary credentials to execute the transactions, and this is also possible for people or institutions with the intent of terrorist financing.

Also, gaining access to network databases containing customer information becomes a compelling target for cyber-criminals or insiders, whose aim may be to steal money, conduct identity theft, blackmail customers, or launch any other form of attack (Chukwudebe & Nosiri, 2015). Despite the intentions of the attackers, generally, cybercrimes cause vast damage to essential infrastructure. Gandhi et al. (2011) remarked that politically motivated cyber-attacks may be

carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate terrorist activities. On the other hand, perpetrators of organised crime are typically focused on control, power and wealth (Gragido et al, 2012). According to Harshé (2021), the Al Qaeda and the IS extended their terrorist activities from the west Asian region (Afghanistan and Pakistan) to African countries like Mali, Nigeria, Somalia and Mozambique contributing to security threats to civilians and security agencies. For instance, in Africa, in 2015, there were 381 terrorist attacks targeting civilians with 1394 fatalities while in 2020 there were 7,108 attacks with 12,519 fatalities. Plotted crimes like terrorist activities in many countries impede national security as essential infrastructures are vulnerable to damage, and national demographics decrease leading to obstruction of national economy. It is costly to replace the essential infrastructure that can be destructed by cybercriminals.

DFID (2017) reported that failed and fragile states are home to more than 900m people, half of whom live in severe poverty, posing a significant threat to international security as states like DR Congo, Sudan, Chad, Central Republic of Africa and Somalia offer a safe haven for illicit trade, drugs-production and weapons-smuggling. Lack of governance in some African countries contributes to political instability, in turn, rebel groups establish strong networks, which are necessitated by communications services. These networks are used especially in getting new recruits and funding for aggravating internal conflicts through illegal transactions like human and drug trafficking, as well as kidnapping. Also, drug abuse affects the youth as they develop health problems and become unproductive. It is costly to the government to provide them medical treatment.

Worcester (2015) stated that strong presence of radical Islamic groups in Somalia and the growing presence of Iranian-backed groups tied to Hezbollah, at times cooperating with Al Qaeda in West Africa poses security threats in Africa. For instance, from the Sudanese province of Darfur in the east, across the Central Africa Republic, southern Chad, northern Cameroon, Mali and Niger are at risk of developing into a zone of entrenched social conflicts. Terrorist groups, which are present in West Africa, Central Africa and East Africa become much stronger due to networks with other rebels outside Africa, and pose security threats in neighbouring countries impeding foreign direct investments (FDIs)

which could boost national economies. It is remarked that causes of human trafficking in Africa include, but are not limited to, poverty, political instability, greed, peer pressure, and lack of legitimate and sustainable employment opportunities and corruption leading to enormous threats to peace and security on the African continent (Bello, 2015; Mollema, 2013; Bello & Olutola, 2020).

Human trafficking poses economic challenges as it affects the ability of countries to engage their citizens, especially the youth, to participate in economic and social development as this active group is exploited in other places or countries. Although empirical studies indicate a number of factors which lead to organised crimes like terrorism, human and drug trafficking, as well as extremist violence. Few researches have been conducted on the impact of telecommunications technology on national security of Tanzania, and the motivations for committing such crimes. Therefore, this study set out to examine the impact of telecommunications technology on human security of Tanzania focusing mainly on the influence of telecommunications technology on security threats like identity theft, money laundering, online money theft, human trafficking and terrorism.

3.0 Theoretical Framework

This study was guided by securitisation theory developed by the Copenhagen School in the mid-1990s. The theory assumes that securitization is evident when (i) the security character of public problems is established, (ii) the social commitments resulting from the collective acceptance that a phenomenon is a threat are fixed and (iii) the possibility of a particular policy is created (Balzacq et al., 2016). For example, human trafficking in Africa poses security threats. In this regard, each state should first consider and find a solution to the underlying or root causes of the crime as these factors are embedded in the countries' socio-economic, political, and cultural milieus (Bello & Olutola, 2020).

The problem of weak and failing states is significantly more dangerous than is generally understood as these unstable regions are a breeding ground for organised crime and terrorism. In order to avoid weakness in the face of security threats, states need strong and effective legal institutions. These institutions will help in building a cyber-security culture within the states. Indeed, the world cannot stop from using ICTs because many sectors are well networked to enable easy access to variety of services and products. But lack of cyber-security culture

gives criminals opportunities to launch crimes. This study used the securitisation theory because it contributes to the understanding of the threats, which have not been given much attention by the government institutions despite to be salient and posing security challenges such as identity theft and spam mails.

In practice, the theory focuses on stable and effective institutions. Taking the example of the greater Horn of Africa which includes Sudan, Ethiopia, Djibouti, Somalia, Kenya and Uganda, conflict emanating from specific states continues to destabilise the region. The interlocking rebellion in Sudan affects northern Uganda, eastern Chad and north-eastern Central African Republic (Worcester, 2015). Political institutions, which are government policies, should ensure stability in the society. Governments should put in place and initiate legal frameworks which aim to control threats impeding national security. In this case, the underlying factors for terrorism should be identified and intervening strategies be sought by the relevant authorities like policy makers of the individual countries and international community by establishing regulatory and legislative measures that intend to prevent such security challenges.

In addition, the established institutions should be able to cope with advances and changes in technology. For example, the advent of wireless mobile technologies has driven packet-based switching technology, which provides the type of network suitable for triple-play communications such as voice, data and video (Sif & Newell, 2004). Though, data centres as critical infrastructure are vulnerable to criminals, yet, they have not received much attention (Balzacq et al, 2016).

Notwithstanding its high value, the securitisation theory has limits. For instance, politicians who have authoritative power may use the theory to brand migrants as security threats instead of refugees, which may lead to racism (Gutierrez, 2018). For example, migrants crossing Mediterranean Sea to Europe have been framed as security threats in some European countries simply (Howell & Richter-Montpetit, 2019). In this case, politicians are likely to use securitisation to create difficult political environment for opposition parties for matters which do not pose security threats in order to keep such political parties outside the public sphere of influence. Nevertheless, the theory is important for this study as

it suggests that government institute regulations that lead to cyber security culture.

4.0 Methodology

4.1. Study Area and Study Approach

This study was conducted in Kinondoni district, Dar es Salaam region, in Tanzania. Kinondoni district is located in northwest of Dar es Salaam region. The district has a large number of reported crimes (Tanzania Police Force & National Bureau of Statistics, 2017). Also, the headquarters of the selected mobile phone companies (Airtel, Tigo, and Vodacom) are located in the district. The study employed a cross - sectional research design. Data were collected through open and close-ended questionnaires administered to 100 mobile phone subscribers from Airtel, Tigo and Vodacom networks.

Semi structured interviews were prepared for face-to-face interviews with twenty (20) key informants from Tanzania Communications Regulatory Authority (TCRA), mobile operators and the police for the purpose of getting insights on crimes committed through telecommunication services and the strategies being used to fight them. Review of documents on government legislative and regulatory frameworks as well as incidents of crimes was also conducted. Document review assisted the researcher to get insights on the effect of telecoms technology and factors influencing crimes. Descriptive statistical analysis was applied to quantitative data while content analysis was used for qualitative data.

4.2 Demographic characteristics of respondents

a. Gender of Respondents

Gender was included in this study so as to determine whether both categories of gender participated in the study to provide their views regarding to the impact of telecommunications technology to the national security of Tanzania.

Table 1: Respondents by gender

Variable	Frequency	Percentage
Male	70	58.3
Female	50	41.7
Total	**120**	**100**

Source: Filed work, 2023

The study findings indicated that 70(58.3%) out of 120 respondents were males while 50 (41.7%) were females. Table 1 gives the summary of results.

4.3 Age of Respondents

Age was included in this study. Out of 120 respondents, 15(12.5%) were in age group of 20-25 years; 43(35.8%) were aged between 26-30 years and 20(16.7%) were aged between 31-40 years. In addition, 22 (18.3%) were aged 41-50 years and the rest 20(16.7%) were aged between 51-60 years. Table 4.2 summarises the above data.

Table 2: Respondents by age

Variable	Frequency	Percentage
51 – 60 years	20	12.5
20 -25 years	15	35.8
26 - 30 years	43	16.7
31 – 40 years	20	18.3
41 – 50 years	22	16.7
Total	**120**	**100**

Source: Field work, 2023

4.4. Education of Respondents

Table 4.1 Respondents by education

Variable	Frequency	Percentage
Illiterate	5	4.3
Primary	50	41.7
Secondary	35	29.1
College	30	25.0
Total	**120**	**100**

Source: Field work, 2023

In this category of social demographic characteristics of respondents, the level of education of respondents assisted the researcher to determine the degree of understanding of study population regarding the impact of telecommunications technology to national security of Tanzania. Results showed that 5(4.2%) out 120 of respondents did not have formal education and 50(41.7%) out of 120 respondents attained primary education. Moreover, 35(29.1%) out of 120

respondents completed secondary education while 8(6.7%) out 120 of respondents were diploma holders, 12(10%) out of 120 respondents had bachelor degree, 6(5%) had master degree, and 4(3.3%) out of 120 respondents were holders of PhD. Summary of findings is shown in Table 4.3.

5.0 Findings and disussion

In this objective, the respondents were asked to mention threats which are aggravated by telecommunications technology. Findings from questionnaires and interviews indicate that security threats resulting from telecommunications technology include theft of identity, online theft of money, money laundering, and human trafficking and terrorism.

5.1. Identity theft

Sahin et al (2017) asserted email and SMS phishing acquires unsuspecting subscriber's personal information such as usernames, passwords, credit card account information, and other sensitive information through the Internet. Many mobile subscribers have been vulnerable to cybercrimes through blackmail, in turn they fall in loss of money or become bankrupt as well as their reputation is tarnished by criminals. Preece (2014) established that fat finger attack occurs where devices are left in an insecure default state or configured insecurely by mistake. Since some enterprises like banks outsource services, human errors may cause unintentional attack because the system or database is vulnerable to criminals.

Moreover, findings from in-depth interviews with TCRA and police indicated that 14 out of 20 respondents mentioned identity theft as a security threat posed by telecommunications technology. In detail, one key informant said:

> *Criminals tend to steal personal information through emails for conducting unlawful acts like making unauthorized transactions and the victims are left with damage to their finance or reputation.*

Another key informant pointed out that:

> *Criminals use high-technological methods to steal critical information for tarnishing a victim's reputation or stealing money.*

Furthermore, another key informant said that:

> *Criminals commit crimes like financial identity theft and social security identity theft*

> *to obtain credit or goods and services without knowledge of the victim. Sometimes, cybercriminals can obtain social security numbers of victims for receiving free medical care or applying for loans or combing fake data with stolen data to create a new identity for fraudulent acts like stealing money from credit cards.*

In collecting data on identity theft, respondents were asked to provide their views to what extent identity theft is a security threat caused by telecommunications technology. Questionnaire responses were rated using a five-point Likert scale ranging from strongly disagree to strongly agree. In the research findings, 7(7%) out of 100 respondents strongly disagreed, 5(5%) disagreed and 11(11%) were neutral on identity theft as a security threat caused by telecommunications technology. Moreover, 45(45%) out of 100 respondents agreed and 32(32%) strongly agreed that identity theft is a security threat resulting from telecommunications technology. Summary of the findings is illustrated in Figure 1.

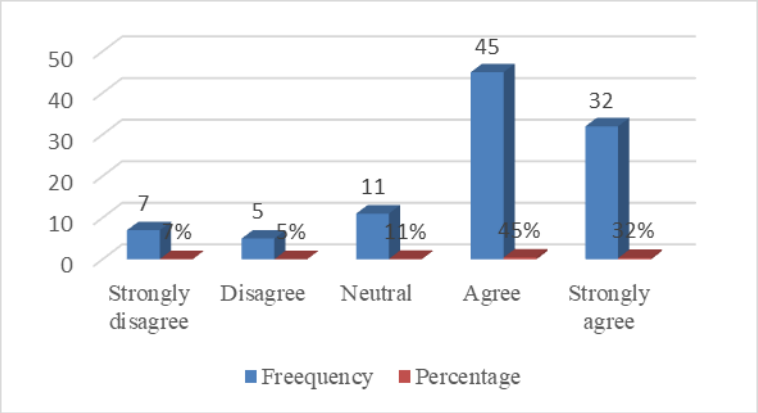

Figure 1: Identity theft
Source: Field work, 2023

The above findings on identity theft can be interpreted that, although telecommunications technology has brought blessings in many sectors like education, health and financial sectors; yet, the telecommunications technology causes security threats. It implies that telecommunications services can be misused by criminals to commit crimes. The findings are in line with Chukwudebe & Nosiri (2015) who said gaining access to network databases

containing customer information becomes a compelling target for cyber-criminals. Before the introduction of modern telecommunications systems Tanzanians experienced traditional crimes like mugging, armed robbery and burglary but today technology has enabled criminals to conduct cybercrimes from different parts of the world.

5.2. Online theft of money

Before the introduction of the new technologies people did not experience cybercrimes which are currently taking a rapid pace. Warner (2011) found that electronically based crimes were primarily related to credit card fraud. Karambu (2011) revealed only 40% of banks in Kenya, Uganda and Tanzania were prepared against cyber threats. A survey conducted among banks in Kenya, Rwanda, Uganda, Tanzania and Zambia revealed that banks were at high risk from threats, such as hacking and malicious insiders (Kshetri, 2019). Internet of things has prompted individuals and institutions to constantly use online transactions like internet banking, online marketing, and mobile money transactions; however, lack of security alert or cyber security preventive measures has given room to cybercrime.

Data collected through in-depth interviews with TCRA and the police revealed 18 out of 20 respondents viewed online theft of money as a security threat posed by telecommunications technology. Explicitly, one of the respondents stressed that:

> *Online theft of money is a criminal activity involving gaining illegal access to bank cards and personal identity through emails and filling in data on fake websites.*

Another key informant commented that:

> *Cybercriminals tend to create and distribute Trojan spy programmes that collect data like passwords for stealing money from personal accounts.*

Another respondent mentioned that:

> *Lack of proper cyber security practices, and lack of skills among Internet users, makes people victims to scam software and compromised websites which enable criminals to steal passwords and credit card numbers. Sometimes criminals intercept information exchanged with a victim's bank to commit unlawful acts.*

Respondents were asked to determine to what extent online theft of money is security threat emerging from telecommunications technology. Questionnaire responses were rated using a five-point Likert scale ranging from strongly disagree to strongly agree. Research findings established 18(8%) out of 100 respondents strongly disagreed, 12(12%) disagreed and 7(7%) were neutral that online theft of money is a security threat resulting from telecommunications technology. Moreover, 20(20%) out of 100 respondents agreed while 43(49%) strongly agreed that online theft of money is a security threat caused by telecommunications technology. Figure 2 provides the summary of the findings.

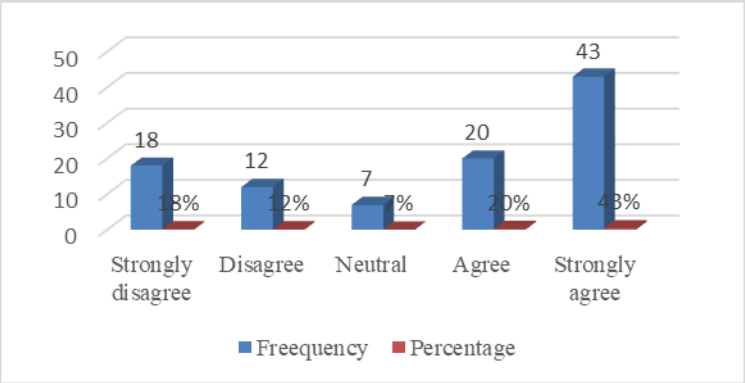

Figure 2: Online theft of money
Source: Research Findings, 2022

The above mentioned findings can be described as testifying that telecommunications technologies contributed to online theft of money. This implies that as mobile phone users go online the more vulnerable they become to cybercrimes. It can be stated that cybercrimes like online theft of money have been fuelled by modern telecommunications technologies. With regard to online theft of money, Mostay (2010) remarked that people and institutions lost around USD 40 billion annually in online activity through ID theft and communication fraud.

5.3. Money laundering

Studies by Johari et al., 2016 and Friedrich & Quick, 2019, indicated that while laundering of criminal proceeds is mainly done through the banking and financial institutions and businesses, in some incidents non-financial entities,

intermediaries and professionals are used or facilitate money laundering. Previously, crimes experienced by people were mainly traditional ones like mugging, burglary and armed robbery; however, modern telecommunications technologies have changed the techniques launderers apply to plot cybercrimes like money laundering.

On the other hand, data collected through in-depth interviews with TCRA and the police revealed that 18 out of 20 respondents viewed money laundering online as a security threat posed by telecommunications technology. Explicitly, one of the respondents stressed that:

> *Money laundering impedes national security as it involves criminal activities like drug trafficking or corruption.*

Another key informant said that

> *Money laundering is experienced in Tanzania through dishonest use of political power and influence.*

Yet another key informant mentioned that:

> *Money laundering is a serious criminal activity involving tax evasion and corruption in the public sphere, and sometimes it is conducted through illegal financial transactions like drug and weapon smuggling, piracy, poaching as well as cyber terrorism involving insiders and outsiders.*

Respondents were asked to estimate to what extent money laundering is a security threat emerging from telecommunications technology. Questionnaire responses were rated using a Likert scale of five-points ranging from strongly disagree to strongly agree. Findings revealed 14(14%) out of t 100 respondents strongly disagreed 10(10%) disagreed and 8(8%) were neutral on the money laundering as a security threat caused by telecommunications technology. Likewise, 38(38%) out of 100 respondents agreed and 40(40%) strongly agreed that money laundering is a security threat caused by telecommunications technology. Figure 3 illustrates the findings.

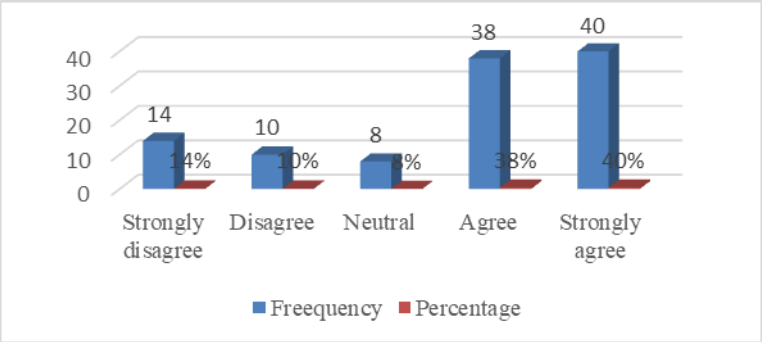

Figure 3: Money laundering
Source: Research Findings, 2022

Findings on money laundering outlined above explain that telecommunications technology supports money laundering countries. Tanzania is also exposed to transnational money laundering threats arising from smuggling of goods, drug trafficking, human trafficking, and the criminal proceeds are suspected to be channeled through hospitality industry and real estate sector. Also, the country is used as a transit route for drugs to and from Asia, Latin America, Europe and Southern Africa (The Eastern and Southern Africa Anti-Money Laundering Group, 2021).

5.4. Human trafficking

Fourteen sources reviewed make reference to internal trafficking in Kenya, ten in Tanzania, and eight in Uganda. Certainly, before the development of modern telecommunications technologies, it was hard to conduct this illicit activity of human trafficking due to difficulties in communications and processing of travel documentation.

Data collected through in-depth interviews with TCRA and the police revealed 15 out of 20 respondents viewed human trafficking as a security threat caused by telecommunications technology. For example, one key informant among them stressed that:

> *The traffickers exploit marginalized groups like children by compelling them to perform labour or engage in commercial sex*",

Another key informant stated that

Human trafficking is involuntary and victims bear life threatening risks like paying smuggling debts or face slavery.

Likewise, one key informant pointed out that:

Tanzania is considered as a source, transit and destination country for men, women and children being trafficked for the purposes of forced labour and sexual exploitation, but trafficked girls and women are sent to Gulf countries like Oman and others for domestic works.

Respondents were asked to determine to what extent human trafficking is a security threat emerging from telecommunications technology. Questionnaire responses were rated using a Likert scale of a five-points ranging from strongly disagree to strongly agree. Findings illustrated that 15(15%) out of 100 respondents strongly disagreed, 10(10%) disagreed and 5(5%) were neutral that human trafficking is a security threat caused by telecommunications technology. Furthermore, 30(30%) respondents agreed and 40(40%) strongly agreed that human trafficking is a security threat. Summary of the findings is shown in Figure 4 below.

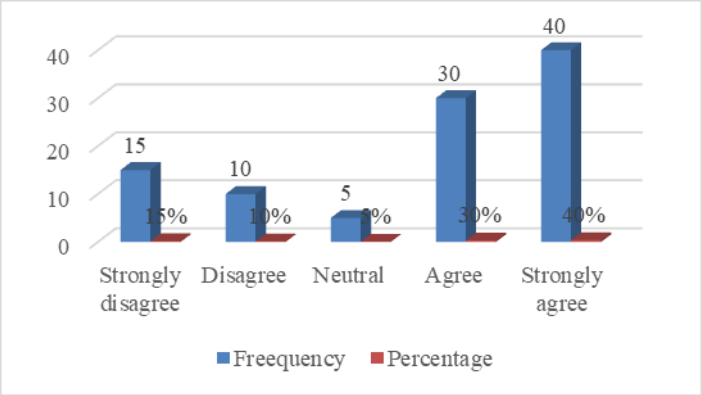

Figure 4: Human trafficking in persons
Source: Research Findings, 2022

In line with the above findings, it can be said that human trafficking has gained pace due to telecommunications technology. United States Department of State (2020) reported that human traffickers exploit domestic and foreign victims in Tanzania, and traffickers exploit victims from Tanzania abroad. Daghar (2020)

reported that Eastern Africa, Tanzania inclusive, was affected by both internal and international trafficking.

5.5. Terrorism

According to EAPCCO (2023), in Eastern Africa, the challenges that continue to perpetuate terrorism include the continued spread of religious fundamentalism and extremism; the growing threat of home grown terrorism; the existence of porous borders; inadequate sharing of intelligence among countries; and inadequacies in addressing radicalisation and violent extremism. Explicitly, ideology and radicalization have fuelled transnational terrorism which affects many countries, Tanzania inclusive. But one additional facto could be found in the use of new technologies, particularly telecommunication.

Data collected through in-depth interviews with TCRA and the police revealed that 15 out of 20 respondents viewed terrorism as a security threat supported by telecommunications technology. For instance, one key informant stated that:

> *Terrorism causes security challenges as the unlawful acts conducted by terrorists may cause risks to both the targeted victims and innocent civilians, especially when the attackers target crowded areas like markets or transport points.*

In interview with one key informant from the police, it was noted that:

> *Terrorism is one among the security threats in many countries which evoke much fear and emotion to both security institutions and civilians as it is not easy to predict effectively the time the terrorists may launch a particular terrorist attack.*

Respondents were also asked to determine to what extent terrorism is a security threat emerging from telecommunications technology. Questionnaire responses were rated using a Likert scale of five-points ranging from strongly disagree to strongly agree. Findings indicated 10(10%) out of 100 respondents strongly disagreed, 15(15%) disagreed and 5(5%) were neutral that terrorism is a security threat caused by telecommunications technology. Furthermore, 35(35%) respondents agreed and 35(35%) strongly agreed that terrorism is a security threat resulting from telecommunications technology. Summary of the findings is shown in Figure 5 below.

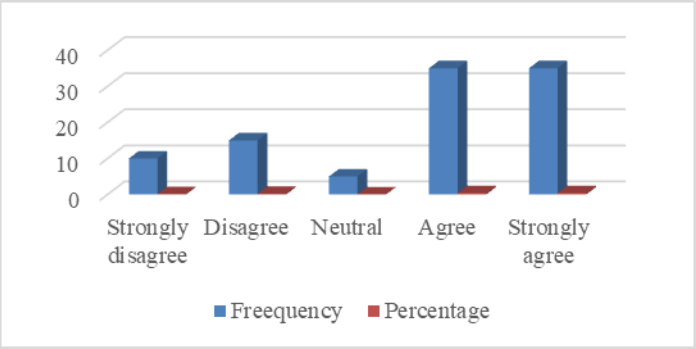

Figure 5: Terrorism
Source: Research Findings, 2022

It can be interpreted that modern telecommunications technology contributed to the emerging new techniques which accelerate terrorism. UNODC (2012) found that the Internet might be used for propaganda in the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. OCBA (2010) reported that terrorist groups like Al Qaeda use different online techniques to launch unlawful acts. Also, terrorist groups steal IDs and fake passports to open bank accounts in which terrorist supporters are transferring money (Arterberry, 2005). In today's digital world, personal data are largely collected and shared online platforms leading to vulnerability, especially when criminals who use the stolen data to commit cyber terrorism.

6.0 Conclusion and Recommendations

Telecommunications technology has aggravated some crimes, which have impact on human security. Indeed, many people and institutions like banks have become victims of cybercrimes due to lack of cyber security among users of telecommunications services and products. The techniques being used by cybercriminals have transformed the traditional crimes to online crimes, which make the fight against cybercrimes to be difficult among individuals and institutions and governments. National governments and other institutions using telecommunication technology in offering their services are required to build a cyber-security culture by institutionalizing, not only legal regulations but also best practices in cyber security.

References

Adonis, Dennis (2018). *The 10 major threats to global supply chains.* Available at: http://www.whispir.com/en-us/blog/the-10-major-threats-to-global-suplly-chains. (Accessed 13 July 2022.)

Agubor, C.K, Chukwudebe, G.A. & Nosiri, O.C. (2015). *Security Challenges to Telecommunication Networks: An Overview of Threats and Preventive strategies.* Conference paper, 4-7 November 2015. Abuja, Nigeria.

Arterberry J.D (2005). *Identity theft: trends, techniques, and responses.* Washington, DC: The United States Department of Justice. Available at: www.nacrc.org (Accessed 10 June 2021).

Bears, J. (2021). *White Paper: Telecom Sites Physical Security.* Asentria. Available at: https://www.asentria.com/blog/telecom-sites-physical-security-white-paper/#modal-close474 (Accessed 13 July 2022).

Bello, P. (2015). Examining human trafficking and the response of the South African criminal justice system. PhD thesis. Pretoria: Tshwane University of Technology.

Bello, P. & Olutola, A. (2020). The conundrum of human trafficking in Africa. IntechOpen

Chukwudebe G. A. and Nosiri, O.C (2015*). Security Challenges to Telecommunication Networks: An Overview of Threats and Preventive Strategies.* International Conference On Cyberspace Governance – Cyberabuja held from 4-7 November, 2015 Abuja, Nigeria.

Daghar, M. (2020). *Evidence suggests that trafficking from the region to the Middle East is being run entirely by East Africans.* Nairobi: Institute of Security Studies. Available at: https://issafrica.org (Accessed 10 May 2022).

DFID (2017). *DFID spend on fragile states and regions: Percentage of DFID's budget spent on fragile states and regions.* London: Department for International Development.

Friedrich, C. & Quick, R. (2019). An analysis of anti-money laundering in German

non-financial sector. *Journal of Management and Governance*, *23* (4), p. 1099-1137.Available at: DOI: 10.1007/s10997-019-09453-5 (Accessed 12 February 2022).

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28-38. DOI: 10.1109/MTS.2011.940293 (Accessed 9 January 2022).

Gragido, W., Molina, D., Pierce, J., & Selby, N. (2012). *Blackhatonomics: an inside look at the economics of cybercrime.* In C. Han & R. Dongre. Q &A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10), 40–42. Available at: http://timreview.ca/article/838 (Accessed 10 June 2021).

Harshé, R. (2021). *Burgeoning Terrorism in Africa: A Critical Overview.* Available **at:** https://www.orfonline.org/expert-speak/burgeoning-terrorism-in-africa-a-critical-overview (Accessed 13 July 2022).

Johari, Z.A., Mohamed, I.S. & Omar, N.B. (2016). A review of the role of designated non-financial business and professions as preventive measures in mitigating money laundering. *International Scientific Researches Journal*, *72* (7), p.93-105. Available at: DOI:10.21506/j.ponte.2016.7.6 (Accessed 12 May 2021).

Kshetri, Nir (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77-81. Available at: DOI: 10.1080/1097198X.2019.1603527 (Accessed April 20021)

Mollema N (2013). *Combating human trafficking in South Africa: A comparative legal study.* (*PhD thesis*) Pretoria: University of South Africa.

Ohene, R.K. (2015). *Evaluation of Cybercrime and Information Security Breaches in Financial Institutions in Ghana: A Customer Perception. Report for the Advanced Programme in Risk Management.* Pretoria: University of South Africa

Preece, Carline (2014).*Cyber Security Courses.* London: Dennis Publishing Limited.

Sahin, M., Fancillon, A, Gupta, P & Ahamad, M. (2017). *SoK: fraud in telephony.* 2017 IEEE European Symposium on Security and Privacy.

The Eastern and Southern Africa Anti-Money Laundering Group (2021). *Anti-money laundering and counter –terrorist financing measures, Tanzania: Second round mutual evaluation report.* Dar es Salaam. ESAAMLG. Retrieved from the Eastern and Southern Africa Anti-Money Laundering Group website: https://www.esaamlg.org/report/me.php.

Tropina, T. (2016). *Do digital technologies facilitate illicit financial flows?* New York: The World Bank.

US Department of State (2020). *2020 trafficking in persons report: Tanzania.* Washington, DC: United States of America. Available at: https://www.state.gov (Accessed 10 January 2021).

UNODC (2013). *Report on the meeting of the expert group to conduct a comprehensive study on cybercrime.* Vienna. Office on Drugs and Crime. Available at: https://www.unodc.org (Accessed 12 November 2022)

Worcester, M. (2015). *Combating Terrorism in Africa.* Berlin: Institute for Strategic, Political, Security and Economic Consultancy (ISPSW).