AN EXAMINATION OF CYBERCRIME IN GHANA AND ITS IMPLICATIONS FOR THE GHANAIAN IN THE INTERNATIONAL COMMUNITY

BY

ADOMAKO, DOMINIC BAAFI

(10806122)

THIS DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE MASTER OF ARTS DEGREE IN INTERNATIONAL AFFAIRS

JULY 2021

DECLARATION

I, **DOMINIC BAAFI ADOMAKO,** do hereby declare that this dissertation is the result of original research conducted by me under the supervision of DR. FREDERICK BOAMAH and that no part of it has been submitted anywhere else for other purposes apart from other works which have been duly acknowledged.

DOMINIC BAAFI ADOMAKO **DR. FREDERICK BOAMAH**

....

(SUPERVISOR)

DEDICATION

This work is dedicated to the Almighty God the Father, God the Son, and God the Holy Spirit. It is He who gave the inspiration, strength, and resources to complete this study. I am forever grateful to Him.

ACKNOWLEDGEMENTS

The ultimate thanks go to God Almighty for giving me the strength and motivation to write this thesis. I thank Dr. Frederick Boamah for his input, time, and critical review of this research work. I am equally eternally grateful to Christian Pitt for his advice and input in this work, it helped me in the course of this work. Further, I am grateful to all participants interviewed for this work. Without them, this effort would have been much more difficult, and I appreciate all the support and time. I thank all my course mates and everyone at the Legon Centre for International Affairs and Diplomacy. God bless you all immensely.

ABSTRACT

Several studies on cybercrime focus on cybercrime and its consequences on the state, however very little attention has been paid to the impact of cybercrime on individuals and their international engagement. Anecdotal evidence from countries such as Nigeria and Russia suggest that the activities of a few cyber criminals have a grave impact on innocent citizens. The internet is a global community, thus crime in cyberspace is automatically globalized. This has forced policymakers to come up with stringent policies that tackle cybercrime. Using the Theory of Externalities and the Space Transition Theory, this work posits that the internet provides a safe space for people to commit crimes against others they may never interface with. These crimes lead to the innocent public suffering from the activities. This research, therefore, sought to examine the impact of cybercrime on Ghanaians as well as the Ghanaian community abroad. The study employed a qualitative method involving two focus group discussions and in-depth interviews with experts. One of the focus groups involved Ghanaians living abroad, while the other with experts in the field of cybercrime and its associated negative externalities. Further, a one-on-one in-depth interview was conducted among key stakeholders to explore the issue in detail. The findings of the research revealed that cybercrime has a negative externality on Ghanaians living in abroad, as well as on the image of the country. Findings also showed that there was discrimination against Ghanaians due to being perceived as a cybercriminal because of cases blown up in the media involving Ghanaians who had committed cybercrime. The study recommends a deliberate effort by the government in reducing the prevalence of cybercrime by proactively enhancing its cybersecurity framework. This should include the development of comprehensive, locally tailored legislation, widespread public awareness campaign, fostering robust public-private collaborations, crafting unique national cybersecurity strategy, prioritizing international cooperation, making substantial investments in cutting-edge cybersecurity technologies, encouraging indigenous research and innovation in cybersecurity, and implementing a streamlined and accessible reporting system for cybercrime incidents. Further, the Cyber Crime Unit and Digital Forensic Laboratory of the Ghana Police Service should actively promote the reporting of cybercriminal activities and, critically, prioritize expeditious prosecution measures. Ensuring timely and swift legal action not only serves as a deterrent but also enhances the confidence of whistleblowers in the effectiveness of the legal system. These would lead to an improvement of the image of the Ghanaian in the international community.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

RESEARCH DESIGN

1.1. Background of Study

Sir Timothy John Berners- Lee OM an English computer scientist is credited with being the inventor of the World Wide Web (Gandon, 2017). It is imperative to state that two other computer Scientists Vinton Cerf and Bob Kahn are also credited with inventing the internet communication protocol which we use today. The internet provides numerous opportunities for people from all corners of the globe to interact, allowing people to form online social communities, facilitating the smooth sending, and receiving of money, and also allowing people to have access to educational facilities and materials, among other opportunities. The genesis of the internet can be traced to 1st January 1983 under the name "ARPANET." The ARPANET aimed to build and interconnect computer networks to enable the sharing of information and knowledge among users of the networks. The advent of the internet, with its aim in mind, has led to several benefits such as opening up people and also global economies to endless possibilities (Kasraie & Kasraie, 2010). The internet has drawn the global community together, as such it has become a medium for people all over the world to experience other cultures. However, individuals can be judged based on the perceived risk they pose (through cybercrime) to others on the internet (Akgul & Kirlidog, 2015). Although the internet presents many opportunities for remote interpersonal interaction, criminals have taken advantage of the internet to deceive, disinform and defraud the innocent public. The criminal actions of these elements do not only pose a security risk to the public but have serious consequences for others.

The ripple effects of cybercrime are referred to as the negative externalities. This explains the phenomenon whereby others unrelated to the crime suffer physical and emotional consequences

from the action of cybercriminals. To examine the negative externalities of cybercrime on the impact of Ghanaians in the international community, it is important to define cybercrime. Cybercrime has been very difficult to define even among cybercrime experts, however, Shinder (2002) provides an extensive definition of cybercrime as any criminal offenses committed using the internet or another computer network as a component of the crime. Per Shinder's definition, the externalities of cybercrime on Ghanaians living in the international community can be explored through how other Ghanaians use the internet to commit crimes against other nationals. Records by all cybersecurity agencies throughout the world indicate a rise in the prevalence of cybercrime. The rise can be attributed to increased accessibility to the internet. The growth of the internet is intricately linked to the growth and sophistication of cybercrime (Wall 2015). The first reported negative externalities of cybercrimes on the image of a country can be attributed to the first reported case of cybercrime in 1981 committed by a German citizen called Ian Murphy popularly known as Captain Zap (Danquah & Longe, 2011). It involved Ian hacking an American telephone company to make free calls. During that era, Germany was still reeling from the partition of the country. This singular action by Ian led to some people having negative stereotypes of Germans. This happened during a time when there was a rise in negative segments among countries perceived to be socialist.

Cybercrimes have taken on more sophisticated modules such as romance scams (Whitty, 2018), identity theft (Newman, 2006), child pornography (Webb et al., 2007), the spread of hate, and terrorism (Lennings et al., 2010) among others. Recent happenings in Germany, Russia, and China have given credence to the fact that the activities of a few cyber criminals can impact the image of a country thereby leading to negative externalities faced by innocent citizens faced on the internet and in other physical spaces. In the 2016 US elections which saw the election of Donald Trump as

President, Russia was accused of meddling in the democratic process of America through the use of cyber warfare and this led to a further strain on US-Russia relations. Russia, therefore, suffered a very negative image in the global political sphere (Riley & Robertson, 2017). Russians still suffer those negative externalities, especially among their Western peers. This led to other countries adopting a hostile outlook towards people who are deemed as Russians or carry Russian surnames even if they were not Russians.

The lived experiences of Africans regarding the negative externalities of cybercrime are no different from the global picture. The practice of romance scams and identity theft is increasingly becoming a holy ground on the African continent. Popularly called "The Nigerian letter or 419" (Kopp et al., 2015) it is the most common in Africa where a person plays on the romantic emotions of foreigners to steal from them using the internet. A romance scam is one of the reasons why Nigerians experienced various forms of negative lived experiences on the internet. To be a Nigerian became synonymous with being a practitioner of a romance scam. Research by Kshetric (2010) indicates that Africans are comparatively more likely to commit cybercrime than to experience cybercrime. This, therefore, feeds into the narrative that Africans are more likely to commit cybercrime and hence the reason why they receive negative treatment on the internet. It is reported that in 2017, despite Africa being less likely to be at the receiving end of cybercrime, the menace cost the continent over 3.5 billion USD (Serianu, 2017). It is reported that aside from the cost element, cybercrimes have damaged the image of African citizens like Nigeria in the global community (Abdul-Rasheed et al., 2016). This deteriorating image of Africans regarding cybercrimes led the ECOWAS Council of Ministers to adopt "Directive C/DIR.1/08/11" on fighting Cybercrimes at its 66th Ordinary Session in Abuja, Nigeria. The directive included establishing a legal framework to control cybercrime in the West African sub-region; a region

known for higher-than-normal incidences of cybercrimes (Orji, 2019). This legal framework has done very little to reduce cybercrimes in Africa as the increase in cybercrimes can be attributed to several economic underlying conditions that have still not seen improvements (Kigerl, 2012).

Ghanaians also face issues with cybercrimes regarding negative externalities of the impact of cybercrime in the international space. Ghana and by extension, Ghanaians, have a good image of being welcoming, law-abiding, and peaceful. This enviable image is slowly eroding due to the rising cases of cybercrime (Dull 2008). This rising incidence of cybercrime has led to the blacklisting of Ghanaians living in Ghana and also foreigners living in Ghana in enjoying certain economic activities such as the use of PayPal Services, Apple Pay, Cash App, and Zelle among others. The rise of indigenous digital solutions such as MTN Mobile Money, Mobile money payment gateway APIs among others has made it easier to transact online business. Unscrupulous people are using these innovative new ways to use it to commit cybercrime against Ghanaians and other foreign nationals (Akomea-Frimpong et al., 2019). It is also reported that in 2020, the banking sector experienced more than 400,000 incidents of malware, 44 million related spam emails, and 280,000 botnets. The money lost to cybercrime jumped from GH¢115.51million in 2019 to GH¢1.0 billion. (Bank of Ghana, 2020). The increasing cyber-attack can be attributed to vulnerable systems and lax cybersecurity measures.

The government of Ghana in a response to these attacks on cyberspace-initiated measures to curb the menace by the adoption of the National cybersecurity policy and strategy (NCSPS) in 2016, the establishment of the Ghana computer emergency response team (CERT-GH), and the enactment of the data protection Act,2012 (Act 843). Despite these measures, cybercrimes have seen an increase in the number of reported cybercrime spaces. Ghana is listed as one out of four countries (with the others being Nigeria, South Africa, and Ethiopia) with an unfavourable image

of cybercrimes in the international community (Eboibi, 2020). These harms the Ghanaians in several facets of life especially the ease of doing business in the international community.

Most research focuses on cybercrime concerning the image of a country in terms of doing business in the international community. Few studies, however, have focused on the citizen as the unit of analysis and this is what this research seeks to employ.

1.2. Statement of the Research Problem

In international relations, how a nation is perceived by others is of grave importance. The reputation of a country for cybercrimes informs the willingness of international businesses to operate in that country. Ghana is one of the countries noted for a high incidence of cybercrime and this is the reason why companies such as PayPal do not want to operate in Ghana. Other IT giants such as Spotify, Apple, and PayPal among others do not work in the country for the same reason. In the case of PayPal, in African countries where they work, they have very restricted services. The activities of cyber criminals affect other Ghanaians and Ghanaian-owned businesses and the services they can enjoy despite them having no hand in it. A case can be of how this menace has led to the deteriorating image of Nigeria leading to some of their citizens passing themselves off as other West African nations to escape from these negative judgements (Ennin, 2015).

A lot of studies have been done about the impact of cybercrime and its impact on the image of citizens. Research conducted by Oni & Oni (2019) indicates that the activities of cybercrime by a few Nigerians have affected the image of almost all Nigerians. Other studies have been conducted by Ralarala (2020) which concluded that cybercrime affects the image of Kenyans including their dealings with other people from other countries. However, from the Ghanaian perspective, few studies have been conducted about the impact of cybercrime on the image of the Ghanaian in the international community.

The government is aware of the growing menace of cybercrimes and its implication for the lived experiences of Ghanaians in the international community. A report by the cybercrime unit of the criminal investigation department of the Ghana Police Service (2019) indicates that there are yearly increases in the amount of money lost to cybercrime and also the number of people involved. The country lost 105 million USD in the year 2018 as a result of cybercrime, an increase from the figures of 2017 and 2019 which stood at 69 million USD and 35 million USD respectively. These cybercrimes indicate the rather poor and weak security of the cyberinfrastructure and cyberspace of Ghana. Studies by Barfi et al. (2018) indicate that the menace of cybercrime in Ghana has become a canker that has eaten deep into the social fiber of Ghanaian society. Research revolving around cybercrime seeks to focus largely on the country as a unit of analysis (Nayak & Das 2013), on businesses (Paoli et al., 2018), and on the economy (Ibrahim, 2019). However, every country is made up of individuals who make up institutions and society. Despite the importance of the individual, rarely does research focus on them. The lacunae this research seeks to address is to zone in on the Ghanaian and examine how cybercrime impacts their lives and business lives as a whole. Cybercrime has made the Ghanaian worse off in the social services he/she can access online when compared to their African counterparts like Kenyans, South Africans, and Rwandans. The country together with its citizens has been ranked alongside Nigeria and Cameroun among the top 10 countries in the world with very high cybercrime prevalence (Barfi et al., 2018). With these rather disturbing images of Ghanaians on the international front as a hub for cybercrime in Africa, the government of Ghana enacted and implemented the Ghana Electronic Transactions Act 2008 (Act 772). Despite the successful passage of the Act, the issue of cybercrime remains a challenge (Dugle, 2013).

This research, therefore, adds to the body of knowledge regarding the negative externalities of cybercrime on the (Ghanaian) individual on the international scene. It further seeks to examine the effectiveness of cybercrime laws in minimizing the externalities on otherwise innocent Ghanaians. Finally, the research seeks to make recommendations that can be made to reduce the prevalence of cybercrime. This will form a framework through which they can tackle cybercrime and take into consideration how innocent Ghanaians are suffering due to the actions of a few. When issues of cybercrimes are not taken seriously, the Ghanaians suffer more especially those who interface with foreign business partners. They suffer issues of credibility which can impact how businesses will relate to them. This can even be seen in the Nigerian example, where every business that deals with the deals with them on a more scrutinized basis.

1.3. Research Questions

- What are the implications of the rising incidence of cybercrime on the image of Ghanaians in the international community?
- How effective are the laws enacted to deal with cybercrimes in Ghana?
- In what way can the laws that deal with cybercrimes be strengthened to reduce the incidences of cybercrime?

1.4. Research Objectives

- To examine the implications of the rising incidence of cybercrime on the image of Ghanaians in the international community.
- To access the effectiveness of the current laws of cybercrimes in Ghana.
- To examine ways through which the laws that deal with cybercrime be strengthened to reduce the incidence of cybercrime.

1.5. Scope of the Study

The study focused on the implications of cybercrime on Ghanaians in the international community and as such was limited to Ghana and Ghanaians. The study focuses on the various interventions by the government through its relevant key stakeholders to prevent cybercrime. As such it will make use of available data on cybercrime in Ghana focusing on the government of Ghana's interventions in fighting the menace to make recommendations on how best the government can help solve cybercrimes in Ghana drawing on experiences from other countries. The study will focus on reviewing existing research from other countries that have transitioned from being negatively viewed on cybercrimes to them escaping these negative judgments based on certain things their government did. The reason for this was to enable the researcher, the ability to ascertain what Ghanaians go through due to how other countries think of how prevalent cybercrimes is in Ghana. This enabled her to collect accurate data regarding the phenomenon under study. It is expected that the study will be completed within one calendar year.

1.6. The rationale of the Study

At present, there are inadequate empirical studies on the impact of cybercrimes on Ghanaians in the international community. The existing literature does not provide a linkage between cybercrime activities by one Ghanaian and its impact on another unrelated Ghanaian in the international community. (Boateng et al., 2010; Danquah and Longe, 2011; Warner, 2011). This study, therefore, will serve as a useful document for policymakers, government, ministries, and non-governmental organizations among others who are interested in preventing cybercrimes in the country. This study will help the government to detail how the ordinary Ghanaian is suffering due to how the country is perceived negatively about cybercrimes. Although Ghana is viewed as a peace-loving country that was built due to years and years of good hospitality, cybercrimes seek

to undo all these gains. This research will therefore unearth how far the negative perception has gotten and what the government itself can do to help shift back the image of Ghana to its previous peace-loving country the world has known it to be.

The research will help the government again to know how knowledgeable the Ghanaian citizens are about cybercrime prevention strategies that are being spearheaded by the government and the relevant institutions mandated to carry on such an activity. It will also help the government to know how effective these strategies are working since when it works, the prevalence will reduce and once the prevalence is reduced, it will reduce the negative image Ghanaians face in the international community. This study will also help the financial service providers and the telecommunication companies themselves to structure their awareness programs to help minimize incidences of fraud in Ghana. This will in turn build upon the trust foreign institutions will have in Ghana. Recently, Spotify whitelisted Ghana and now their global services can be used in Ghana. This means that our music industry which was otherwise dying could be self-sustaining due to the royalties that Spotify gives to streams. If other companies like Spotify whitelist Ghana, we would have the benefit of an array of services that will make life easier for us. This study will also help stakeholders understand the kind of interventions that are necessary to prevent people from falling victim to cybercrimes and also how to adapt their campaigns when cybercrimes get more sophisticated. This study will also help the government and relevant stakeholders to embark on strategies that will build trust in the people about the government's commitment to the prevention of cybercrimes in the country. Lastly, this research will help the government to come out with strategies to improve its image in Ghana in the international community concerning crimes. When this is done, then it automatically means that the image of Ghanaians will be uplifted.

1.7. Theoretical or Conceptual Framework

The study will adopt two theories: The Space Transition Theory and the Theory of Negative Externalities. The need for this integrated theory is that one theory cannot establish how and why cybercrime occurs and the impact it has on innocent people elsewhere. The Space Transition Theory was developed by Jaishankar in his paper titled, "Establishing a theory of cybercrimes." The theory on Space Transition Theory posits that cybercrime is meant to happen when these three elements are present: anonymity, freedom, and insecurity (Assarut et al., 2019). The theory states that since the internet can offer a sense of anonymity it is suitable for the commitment of cybercrimes since those who commit them go by a pseudonym. According to Jaishankar (2008) who proposed this theory, individuals exhibit unacceptable behaviour using physical and cyberspace. Essentially this theory explains why individuals commit cybercrimes. Jaishankar posits that people in repressed situations look for ways to solve their deteriorating position and hence they use cybercrimes as a means to an end. He argues that since they feel inferior in society, they move to cybercrime. Before they engage in cybercrime, they weigh the magnitude of their current situation of being a law-abiding individual and what they will gain if they break the law by engaging in cybercrime. If they feel the benefits ways, the costs they are likely to transit into cyberspace to commit a crime. He lastly says that those who are shameless are more likely to commit cybercrimes than those who are not.

Cyberspace too provides anonymity for would-be offenders, so they are motivated by it. Anonymity provides a de-individualization; they create a new persona and engage in crime. In their minds, it is not them but rather the new persona that is committing the crime.

Research has applauded Jaishankar for his Space Transition Theory as it is the only theory that adequately addresses cyber-trespassing, cyber-deception, robbery, and cyber-pornography

(Abayomi, 2020). Despite it being one of the best, others argue that the theory is more appropriate for some types of cybercrimes than others, but it gives the basics under which cybercrime occurs and that is the movement of people in different spaces. Cyberspace changes a person's values (Ndubueze, 2017). Warner (2011) argues that Space Transition Theory is best applied to the Ghanaian context because Ghanaians are known globally for their good and hospitable behaviour but the growth of cyberspace in Ghana has led to some Ghanaians living a parallel life as they would have lived if they were in a face-to-face medium. He further argues that space transition theory is important in understanding cybercrimes via an African geopolitical lens, a techno-spiritual lens, and finally a justificatory philosophy of social justice.

Using one theory to delimit cybercrime is extremely difficult as cyber criminology is a multidisciplinary field that encompasses theories from other fields like criminology, victimology, sociology, internet science, computer science, and in this case economics (Jaishankar, 2010).

Externalities are a cost that the action of another imposes on a society (Biglan 2009). The theory of negative externalities is therefore used to explore the negative consequences largely innocent Ghanaians face due to the activities of a few cybercriminals. The theory on externalities largely explains how a third party has no hand in cybercrime but suffers the consequences of an action by someone else. The theory of negative externalities (Smith, 2019) is a concept that sheds light on the effects of cybercrime. This theory emphasises the importance of analysing the external costs imposed on society by cybercriminal actions, emphasising the need for strong cybersecurity measures and international cooperation. When an economic activity generates expenses that are borne by individuals or entities who are not directly involved in the activity, this is referred to as a negative externality. This theory is especially significant in the case of cybercrime since the costs of cybercriminal activities affect a greater spectrum of stakeholders, including enterprises,

governments, and foreign partners (Doe, 2020). Data breaches, identity theft, and ransomware attacks all result in financial losses, compromised privacy, and decreased consumer trust in online platforms.

The theory of externalities is important in this context because, with an estimated population of 31 million, those who commit cybercrime are a very small insignificant number but the impact it has on most Ghanaians is greater than a factor of 100. What is worth knowing is that even those who do not know anything about the internet suffer negative outcomes due to the behaviour of a few cybercriminals. There is a good amount of literature on the profits gained by cybercriminals and the harm suffered by the afflicted but there is inadequate literature on the negative outcomes suffered by the general populace, and this could be best explained and somewhat quantified by the economic theory of negative externalities.

The theory of negative externalities applies in this research due to how other Ghanaians are suffering the impact of the actions of a few cybercriminals. This theory explains more of the impact of cybercrimes on the individual. It explains why they have to suffer negative outcomes, and why they fend off enjoying services like PayPal, and Zelle among others due to the actions of a few cybercriminals. The theory of negative externalities provides a useful framework for comprehending the multiple effects of cybercrime in Ghana and the consequences for Ghanaians in the international community. The digital world's interconnection necessitates collaborative action to counteract cybercriminal actions and their far-reaching implications. Ghana may limit the impact of cybercrime and improve its reputation on the world stage by implementing effective cybersecurity measures, increasing international cooperation, and raising awareness about the negative externalities caused by cybercrime. Investigating cybercrime's impact on Ghana's digital economy and international relations could shed light on the negative externalities associated with

this issue. It may also be beneficial to investigate the efforts adopted by the Ghanaian government and international organisations to combat cybercrime and its consequences. The principle of negative externalities may be applicable to this problem because cybercrime imposes costs on individuals, businesses, and the economy. These consequences may include financial losses, compromising personal information, and reputational harm to the country (Dzogbenuku, 2018). To alleviate the negative externalities associated with cybercrime, both domestic and foreign parties must work together.

Critics of negative externalities view the theory as neo non-classical and as a result, it explains more of issues and effects of issues that happen in the Western world than in the African context. The theory also delimits the impact of personal responsibility in preventing cybercrimes. This is because cybercriminals live in our midst and at times, some people know exactly who they are and what they do but fail to report them to the appropriate quarters.

The Space Transition Theory will therefore be used to explore how cybercrime occurs, which people are likely to commit cybercrimes, and how their actions have Ghanaians. These two theories will therefore be merged to create a unique understanding of how innocent Ghanaians suffer both on the local and international scene due to the actions of others.

1.8. Literature Review

The literature review will focus on two primary areas: the first is the trends in cybercrime and then on the rising impact of cybercrimes on African countries and then citizens.

1.8.1. Trends on Cybercrime

This section of the study presents a thematic review of the impact of cybercrime on Ghanaians in the international community. The literature review will also identify gaps in the existing literature as well as justify the relevance of my study.

According to Morrison (2013), crime is any action or omission that causes harm in a situation that the person or group responsible ought to be held accountable and punished, irrespective of what the law books of a state say. Research by Arora (2018) categorizes crimes into three types. These are Crimes Against Persons, Crimes Against Property, and Crimes Against Society. Cybercrimes, on the other hand, are very difficult to define since defining them can declassify a crime that is supposed to be in that bracket. Many researchers however agree that cybercrimes are crimes that are facilitated using the internet. Cybercrimes can be classified into different categories, including cyber-trespass (e.g., unauthorized system access), cyber-deception/theft (e.g., identity theft, online fraud, digital piracy), cyber-porn/obscenity (e.g., child sexual exploitation materials), and cyber-violence (e.g., cyberstalking; cyber terrorism) (Holt, Bossler, & Seigfried-Spellar 2018). It is nearly impossible to estimate the amount of cybercrime that occurs in most nations across the world because of a lack of standardized legal definitions for these offenses and few valid, reliable official statistics (Holt & Bossler, 2016). Evidence demonstrates, however, that cybercrime rates are increasing as the rates for many forms of traditional street crimes continue to decrease (Tcherni et al., 2016).

Terzi et al., (2017) give a very glaring picture of how prevalent cybercrime is across the globe. In their work, they cited a report by NCSIR (2016) indicating that across the globe, cybercrime victims have spent $126 billion and lost 19.7 hours dealing with cybercrime activities. The number of devices connected to Wi-Fi has seen exponential growth in 2016 and there is a constant need

for connections (NCSIR, 2016). While the internet has many positive aspects, especially in the area of e-business models, cybercrime has become a serious concern for all e-businesses, with a significant impact on Ghanaians. Cybercrime entails criminal activities or crimes in which computing devices or other forms of ICTs are the targets (Pati, 2003). From the perspective of ICT for development, it is not misplaced to say that cyber is a double-edged sword, with both the potential of boosting the image of a nation and its citizens as well as possibly leading to negative outcomes for a country and its citizenry. The internet, by its very design, is an inherently vulnerable network that has enabled cybercrime to flourish in a new virtual environment.

Cybercrime activities differ from continent to continent. In Africa, the practice of romance scams and advance fee fraud is common. It is also ever-increasing due to the growth of the internet coupled with weak internet regulations on the continent. The IC3 for instance states that Africa is ranked as the third-highest continent regarding cybercrime. Nigeria was ranked as the most internet fraudulent country in Africa. Other top destinations include South Africa, Kenya, Ghana, Egypt, South Africa, Zambia, and Cameroon.

Aside from being ranked first on the African continent, Nigeria is ranked the third highest in the world. To solve this negative image, an act empowers the Nigeria Economic and Financial Crime Commission (EFCC) to carry out surveillance responsibilities to regulate industry players, and cyber cafe operators among others to come back to cybercrimes (Adomi, 2007). The act enforces all players to use their systems to keep records of all transactions engaged by users including their home addresses, telephone numbers, and emails.

South Africa despite being one of the most advanced countries even in the world suffers elements of cybercrimes. They have had to deal with fast-paced cybercrime activities which are ever-increasing. Ghana passed the Electronic Communication and Transactions Act to deal with the

menace of cybercrime. The regulation sought to criminalise actions related to the illegal access and unauthorized modification of information as well as the possession and distribution of hardware devices and software programs that serve as accessories to cyber-fraud. The ECT has a specific provision that deliberately deals with cybercrime. Section 86(1) states as illegal all forms of hacking while 88(1) criminalises all forms of an attempt by criminals to gain unauthorized access to any system.

Cybercrime as compared to other crimes is relatively new in Ghana (Warner 2011). It saw jumps between 1999 and 2000: This is particularly interesting as the internet was new and many Ghanaians did not know what it was or its benefits. During this period, the common type of cybercrime was credit card fraud which was started by people who frequented hotels using Western visitors' cards. It was perpetrated by criminals who stole these foreign cards from abroad, shipped them to Ghana, and use it to purchase goods over the internet.

Cybercrime also seeped into the old system of looking for pen pals and using manipulative skills to extort things from them (Burrell 2008). They used pen pal as a point for material gains. It initiated involved the use of the Postal system but when the internet got popular, it was transferred to the internet. Over the years, cybercrimes have gotten more sophisticated so has their prevalence. For instance, between 2016 to 2020 about 161 cases of cybercrime were reported, only 12 of them representing 7.5% were sent to court, the final determination was done, and the suspected criminals were sent to court. A whopping 75% of them were still under investigation during that period. The slow nature of persuasion was a result of the CID's not having the capacity to fully investigate those crimes during that period. The CID now has a better capacity to process such crimes reported to it at a faster rate than before. However, their new capacity is being hampered since the crimes keep getting sophisticated as time goes by.

There are three types of cybercrimes commonly perpetuated in Ghana and these are identity fraud, fake gold dealers, and real estate fraud. In the case of identity fraud, Ghanaians will contact Westerners through social media via a fake identity and try to escort money from them. They mostly do so by passing off as lovers looking for love.

The second type is fake gold dealers. They contact people with the disguise of having gold to sell. The victims fall for it because Ghana is known for its abundance of gold deposits. They offer gold which is way below the world market prices. The criminals are said to generate fake licenses of the Mineral Commission, Precious Minerals Market Company (PMMC), Geological Survey Department, and other documents which are very difficult to verify to dupe the victims (Obiri-Yeboah, 2013).

The third common type is estate fraud. This involves defrauding known people or relatives by telling them they will build houses for them when they send money which they never build or do. The Ghanaians from the diaspora will come to Ghana and realise that there is neither land nor house to their name. The perpetrators do so by creating fake construction companies and sharing fake photos of houses under construction with unsuspecting victims.

1.8.2. Rising incidence of cybercrime and its impact on the individual

While criminality is digitizing, a theory-based understanding of the impact of cybercrime on victims is lacking (Borwell et al., 2021). Research done in the Netherlands indicates that cybercrime impacts the emotional well-being of Dutch citizens. The rising prevalence of an already high rate of cybercrime committed by Nigerian citizens has impacted greatly Nigerians and the Nigerian economy. Nigerians face reputational risk (Ibrahim 2019). Due to this reputation risk, companies are not willing to transact business with them. Business is all about confidence and because companies do not have confidence in transactions from Nigeria, they treat them

harshly. Even when they are willing to transact business with Nigerians, they put higher security measures or interest rates on deals coming in from Nigeria. The major cause of the rising incidence of cybercrime in Nigeria is unemployment. The youth unemployment rate in Nigeria has been pegged at 47% meaning that nearly 1 in 2 youth is unemployed (Ibrahim, 2019). In a quest to better their financial position, some Nigerians resort to cybercrime. However, due to the negative image they have concerning cybercrimes, companies are not willing to invest in Nigeria thereby increasing the unemployment rate in the country on yearly basis.

When it comes to cybercrime, South Africa is an interesting story. The World Bank puts South Africa as the most unequal society in this world. When it comes to cybercrimes, blacks are suffering more than their white counterparts (Omotso & Koch 2018). Cybercrime is high among the black population than in the white population due to high unemployment in the black community. The unemployment rate stands at 39% among the black community as compared to 1.2% among the white community. This differential pushes blacks to engage in cybercrime. The impact of cybercrime in South Africa is hence suffered more among blacks than white. Businesses are therefore more willing to confidently transact more with white South Africans than black South Africans.

In economics, externalities look at a cost or benefit caused by a producer that is not financially incurred or received by that producer. The concept of externalities was first developed in 1920 by Arthur Pigou (Pigou 2017). There are types of externalities but for this research, we will adapt negative externalities to explain the impact of cybercrimes on the Ghanaians in the international community. A negative externality is anything that causes indirect harm or cost or in this case loss of reputation to individuals.

When a country becomes infamous for cybercrimes, those who suffer the most are those who have nothing to do with that crime. Being citizens of countries noted for cybercrimes, they are more likely to be seen in a negative light or denied certain services due to absolutely no fault of theirs. The whole society bears the negative cost of increasing cybercrimes (Anderson et al., 2013). Cybercrimes have internationalized negative externalities; local crimes like burglary do not necessarily cause a negative image of a country or its citizens in the international community but cybercrime does.

Per the literature, it is beginning to suggest that negative externalities associated with the rising incidence of cybercrimes committed by individuals are an African problem. Africans seem to bear the brunt of cybercrimes. Aside from Nigeria, Kenya, South Africa, and also Ghana, Ugandans face negative externalities associated with cybercrimes. In 2017, Uganda reported a loss of $42m to cybercrime. This led to Ugandans facing extra scrutiny when transacting an online business. To combat it, they drafted an Internet Security Framework focused on three sections --- the Electronic Transaction Bill, the Computer Misuse Bill, and the Electronic Signatures Bill (Quarshie & Martin-Odoom, 2012).

1.8.3. Stopping Cybercrimes with legislation

As Jaishankar (2008) posits, people behave differently when they move from one space to another. Cybercrime legislation is enacted to warn people that the cyberspace they are entering is no different from the physical space, they are being watched and there are rules and regulations also available to regulate behaviour. The first discussion on the importance of legislation to deal with cybercrime was held by the United Nations in 1990. It adopted a resolution dealing with computer crime legislation (Gercke, 2010). The early 2000s saw waves of countries enacting legislation to deal with cybercrime and strengthen cybersecurity.

There seems to be a positive correlation between new legislation and the rise of cybercrime. Countries are increasingly drawing up new legislation to combat cybercrime but the rate of growth of cybercrime isn't going down. In 2005, UK's minister for e-government, Jim Murphy, admitted that laws meant to tackle cybercrimes were not working. In UAE, new cybercrime laws are deemed to be effective because of the punitive fines that are imposed on culprits. The stringent legal measures, including longer jail terms, stiffer fines, and deportation of foreigners, have ensured robust deterrence to cybercriminals (Younies & Na, 2020). This means that when cybercrime laws are tougher and well enacted it can turn the positive correlation into a negative correlation. Laws on cybercrime are not enough, it is the enforcement of the law and regulations that bring about the effectiveness of the laws (Watney, 2012).

1.8.4. Theoretical and Conceptual Framework

This section presents the conceptual framework that explains the various aspects of cybercrime about how it damages the reputation of Ghanaians in the international community. Matters of cybercrimes are best explained by criminologists. Felson and Clarke (1998) established 10 principles of opportunities that can be considered criminal behaviour.

Four theories have been modelled to describe the behaviour of cybercriminals. These four theories are Crime Pattern Theory, Routine Activity Theory, Rational Choice Theory, and Differential Association Theory. Crime Pattern Theory (CPT) was proposed by Brantingham and Brantingham in 1993 and it explains that crime has a regular pattern it follows. It further explains that crime is modelled along the life of normal individuals. Perpetrators of crime under the pattern of normal life individual and therefore use the routine or pattern of their life to commit a crime against them.

Rational Choice Theory however takes a different turn; it says that crime is guided by hedonism. Offenders try to maximise their pleasure and reduce pain. They do this by selfishly exploiting the

pain of others. They look at the benefit they would get and the consequences and when they feel the benefits are higher, they commit the crime.

The Routine Activity Theory also factors in the element of the victim. It stipulates that those who have busy activities are easier to be victims of crimes than those who have the luxury of time. The theory stands on three legs: there should be a motivated offender, a suitable target, and a lack of force to prevent the offender from inflicting pain on the target.

The last theory, Differential Association Theory indicates that if you surround yourself with people who have criminal behaviour you are more likely to be one yourself. This theory believes that crime is a learned behaviour. The differential association theory can be applied to cybercrimes as those who engage in cybercrimes are more likely to walk with or know people who engage in cybercrimes themselves.

1.8.5. Theories to be used to explain Cybercrimes

Other cybercrime theories can be used to explain how cybercrime occurs. This research will therefore combine two theories to seek cybercrime and its implication for Ghanaians. The first theory that will be adapted is the Space Transition Theory of Cybercrime. The second theory will be the theory of externalities.

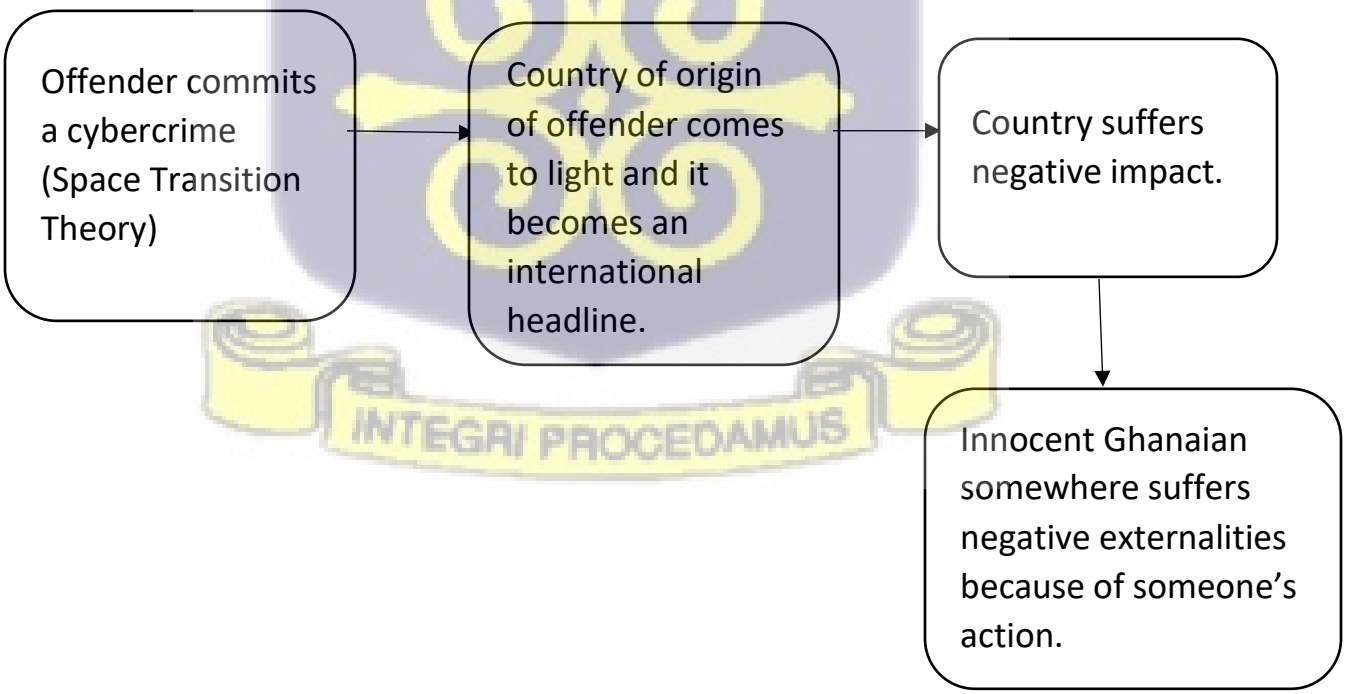
1.8.6. Space Transition Theory of Cybercrime

This theory states that cyberspace serves as a motivation to commit cybercrime, especially for the youth. According to Jaishankar (2008) who proposed this theory, individuals who exhibit unacceptable behaviour use physical and cyberspace. The theory states that individuals who have repressed behaviour commit cybercrimes. Jaishankar posits that people in repressed situations look for ways to solve their deteriorating position and hence they use cybercrimes as a means to an end.

He argues that since they feel inferior in society, they move to cybercrime. Before they engage in cybercrime, they weigh the magnitude of their current situation of being a law-abiding individual and what they will gain if they break the law by engaging in cybercrime. If they feel the benefit outweighs the costs, they are likely to transit into cyberspace to commit a crime. He lastly says that those who are shameless are more likely to commit cybercrimes than those who are not.

Cyberspace provides anonymity for would-be offenders, so they are motivated by it. Anonymity provides a de-individualization; they create a new persona and engage in crime. In their minds, it is not them but rather the new persona that is committing the crime.

Figure 1. Analytical Framework of the study



1.9. Research Methodology

This sector presents the approach adopted to design the study to address the objectives set in the research and to answer the specific research questions stated in the introduction. This section also talks about the research method used, the sampling method, participant selection, sample size, and also how the data was analysed.

1.9.1. Sampling Method

Sampling is the process of selecting members of a population for research. Sampling is the vital stage of every research as it informs validity. Probability and non-probability are the two sampling techniques used in research. This research employed the use of a non-probability sampling technique to select its ten participants for a focus group discussion. The ten were selected based on the characteristics of the population whose experiences fall in line with the objectives of this research. The reason why the non-probability sampling method was used was because of the nature of the information required from participants who have in-depth knowledge of cybercrime and those who have been affected by the negative externalities of cybercrimes. Aside from the focus group discussion, purposive sampling was done to select all the people interviewed. After their selection, they were interviewed using a semi-structured interview guide.

Secondary data was obtained from sources such as journals, books, seminar papers, reports, and other records from the University of Ghana Balme, newspapers, and Legon Centre on International Affairs and Diplomacy (LECIAD) libraries as well as other relevant institutions.

1.9.2. Data Collection Instrument

The most important element in any research is how data is collected (Nurani 2009). How data is collected will inform the validity of the research. To collect data that is of importance to this

research, a focus group interview and in-depth interview were used to gather information about what people think cybercrime has on the image of Ghanaians. A focus group interview is a qualitative method in which the researcher interactively questions a group of participants to test theory-driven hypotheses (Grinn et al., 2006). The sampling method used is the purposive sampling approach. This is a non-probability sampling in which those who will form a part of the focus group will be based on the judgment of the researcher. The purposive sampling approach was used because issues about cybercrimes are a live issue and hence those who have reliable, and knowledge of cybercrimes would be included.

1.9.3. Sources of Data

The research is based on primary and secondary sources of data. The primary source of data includes in-depth focus group discussions conducted using open-ended interview questions. Secondary sources of data comprise autobiographies, books, memoirs, reviews of relevant journals, and other available sources.

1.9.4. Participant Selection

There has been a contested school of thought that qualitative research is less of a research form than its quantitative counterpart. Despite the enormous benefits of quantitative research, it reduces complex phenomena to simple numbers. Qualitative research is more valuable in providing rich descriptions of complex phenomena like cybercrimes (Sofaer, 2000). Cybercrime is a special field in criminology and as such, we need to understand the motive as to why people do what they do and qualitative research is very appropriate in this research that has been undertaken (Weisner, 2014). Qualitative research is also appropriate for this research as interviews benefits from gaining trust from the person you are interviewing and help in unpacking the full extent of a phenomenon (Weisner, 2014) but quantitative research does not have such a luxury.

Respondents selected gave valuable data via surveys, interviews, or other research methods, sharing their insights, experiences, and opinions on many areas of cybercrime in Ghana. Their comments provided researchers with firsthand insight into how cybercrime was hurting individuals, businesses, and the country's broader society. Furthermore, by incorporating a varied set of respondents, the study was able to capture a wide range of perspectives and experiences. This diversity which included people from various professions, sectors, regions, and backgrounds, allowed the researcher to get a more complete view of the way cybercrime affects diverse segments of the Ghanaian community.

The narratives and experiences of respondents offered context for the research findings. The Researcher was able to grasp not only the quantitative features of cybercrime (such as the frequency of assaults) but also the qualitative dimensions (such as the emotional and financial repercussions on victims) through firsthand reports.

The viewpoints of respondents could inform policy suggestions and viable tactics for combating cybercrime. Understanding the issues that individuals and organisations encounter as a result of cybercriminal activity enabled academics to recommend methods that could alleviate the negative consequences and improve Ghana's cybersecurity efforts. Using respondents' feedback helped to situate the study in real-world situations. This grounded approach can make the research more approachable and relevant to Ghanaians' real-life experiences, giving depth and credibility to the study's results and recommendations.

1.9.5. Sample Size

Respondents were selected for both the focus group discussion and the expert in-depth interviews because they hold knowledge and experience in the negative externalities of cybercrimes on Ghanaians. The interviews were based on an open-ended interview questionnaire to get in-depth information and opinion from participants. Interviews were conducted using an interview guide.

The number of people who would be part of the first focus group discussion would be and it will include one security person, one person in the field of IT, one student, one businesswoman, and also one person who has been a victim of a cybercrime. The location for conducting the interview was conducted via zoom since that is where the residents stay and hence might be convenient for them. The total number of people interviewed for this research was twenty-five (25). The first focused group discussion had ten respondents while the second focused group discussion had seven respondents with the in-depth interview.

Respondents are listed in the table below:

Table 1. Respondents of the First Focus Group Discussion

Respondent (R)	Gender	Organisation	Position
FDG1R1	M	University of Ghana	Student
FDG1R2	M	Petroleum Commission	IT Personnel
FDG1R3	M	ReaderApp	Victim of cybercrime
FDG1R4	F	Businesswoman	Sole Proprietor
FDG1R5	M	Agyabeng Akrasi & Co.	Lawyer
FDG1R6	F	Ghana Police Service	Policewoman
FDG1R7	M	University of Ghana	Student

FDG1R8	M	Businessman	Sole Proprietor
FDG1R9	F	Calbank	Banker
FDG1R10	F	National Cyber Security Center	Civil Servant

The second focus group discussion involved Ghanaian citizens living abroad. They were interviewed about their experiences with prejudices resulting from the negative impact of other Ghanaian cybercriminals. The interview was conducted with the help of ZOOM. The respondents are listed in Table 2 below.

Table 2. Respondents of the second Focus Group Discussion

Respondent	Gender	Organization	Position
FDG2R1	M	Affinity Access International	Speech Pathologist
FDG2R2	M	GTC Hub	Product Owner
FDG2R3	M	GTC Hub	Business Analyst
FDG2R4	F	Student	Nantes University
FDG2R5	F	Duensing Law	Lawyer
FDG2R6	F	Brookefield Asset Management	Real Estate Consultant
FDG2R7	F	Homerton University Hospital	Nurse

In addition to the focus group discussion, expert interviews were conducted to solicit their views in line with the set objectives. The respondents are listed below:

Table 3. List of people interviewed for In-depth Expert Interviews

Respondents (IR)	Gender	Organization	Position
IR1	M	Ghana Immigration Service	Officer
IR2	F	National Bureau of Investigation	Intelligence Officer
IR3	M	Express Pay	Research Analyst
IR4	M	e-Crime Bureau Ghana	Security Intelligence Analyst
IR5	M	Cyber Hawk Limited	Cybersecurity Analyst
IR6	M	Cybersecurity Authority, Ghana	Deputy Manager
IR7	M	Africa Digital Rights Hub	Legal Consultant
IR8	M	Public Servant	Former Ambassador

Respondents used in the research improved the research by contributing firsthand information, various perspectives, and contextual insights into the complex subject of cybercrime in Ghana and its international ramifications for Ghanaians. Their contributions served as the foundation for the study's research, results, and recommendations.

1.9.6. Data Analysis

Data collected from the focus group discussion and the expert interview were collected and transcribed verbatim and organized according to the research questions. This kind of thematic analysis is used to analyze, identify, and report patterns within the transcribed data (Braun & Clarke, 2006).

Ghanaians and key people about cybercrimes in Ghana and also it effects Ghanaians in the international community. Data collected from interviews will be analysed through transcription and the commonalities in them in tangent with other literature reviews presented in a non-biased and objective manner.

1.10. Ethical Issues

Ethical considerations were of utmost importance in this research. The questionnaires had no leading questions and also questions that judged the respondents in a negative light. The questionnaires were treated as confidential and were not given to any other third party.

1.11. Arrangement of Chapters

The study is organized into four main chapters. Chapter one talks about the research design. It introduces the subject and gives a brief background to the research area, outlines the research questions and objectives, scope and rationale of the study, the conceptual framework which guides the study, a brief literature review, sources of data, research methodology, as well as limitations of the study. Chapter two provides the global and historic overview and analysis of the growing menace of cybercrime. Chapter three provides an analysis of research findings on cybercrimes and their impact on Ghanaians in the international community. Finally, chapter four presents the key findings of the study, and conclusions, as well as offers some policy recommendations for the way forward for the minimization of cybercrimes in Ghana.

Reference

Abayomi A.A., 2020: Applying Space Transition Theory to Cyber Crime; A Theoretical Analysis of Revenge Pornography in the 21st Century. *International Journal of Innovative Science and Research Technology*

Abdul-Hamid I.K., Shaikh A.A., & Boateng H. & Hinson R.E., (2019): Customers' Perceived Risk and Trust in Using Mobile Money Services – an Empirical Study of Ghana. *International Journal of E-Business Research (IJEBR) 15 (1) 1-19*

Abdul-Rasheed S.L., Lateef I., Yinusa M.A. & Abdullateef R., 2016: Cybercrime and Nigeria's external image: *A critical assessment. Journal of Pan African Studies 9(6), 119-133.*

Afanu E.K. & Mamattah R.S., (2013): Mobile Money Security: A holistic approach.

Akgul M. & Kirlidog M., 2015: Internet censorship in Turkey. *Internet Policy Review 4(2) 1-22*

Akomea-Frimpong I., Andoh C., Akomea-Frimpong A. & Dwomoh-Okudzeto Y., (2019): Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control 22(2):303-317. DOI:10.1108/JMLC-03-2018-0023

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). *"The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region". Library Philosophy and Practice (e-journal). 1715.*

Baumol, W. J., & Oates, W. E. (1988). The theory of environmental policy (2nd ed.). Cambridge University Press.

Boateng R. & Barnor J.N.B., (2020): Unveiling cybercrime in a developing country. *Encyclopedia of Criminal Activities and the Deep Web, 66-92*

Coase, R. H. (1960). The problem of social cost. Journal of Law and Economics, 3, 1-44. Mankiw, N. G. (2014). Principles of economics (7th ed.). Cengage Learning.

Cohen, L., & Felson, M. (1979). *Social Change and Crime Rate Trends. A Routine Theory Approach. America Sociological Review, 44, 588-608.*

Danquah P. & Longe O.B., (2011): Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact 11 (2) 169 - 182*

Dugle, P. (2013). *"Press Coverage of Cybercrime Issues in Ghana: A Content Analysis of the Daily Graphic and Daily Guide". A Dissertation Submitted to the Department of Information Studies, University of Ghana, Legon.*

Dull L.J., 2008: Friendly Africans, Deceptive White Men: Ghanaian Narratives of the Nation.

Eboibi F.E., 2020: Concern of Cyber criminality in South Africa, Ghana, Ethiopia, and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin, 1-32*

Ennin D., Cybercrime in Ghana: A study of offenders, victims and the law. http://197.255.68.203/handle/123456789/8908

Gandon, F. (2017). For everything: Tim Berners-Lee, winner of the 2016 Turing award for having invented… the Web. *1024: Bulletin de la Société Informatique de France*, (11), 21.

Gencer M., (2011): The mobile money movement: Catalyst to jump-start emerging markets. Innovations: *Technology, Governance, Globalization 6(1): 101 - 117*

Holt, T. J., Bossler, A. M., & Seigfried-Spellar., K. C. (2018). *Cybercrime and Digital Forensics: An Introduction. 2nd ed. New York: Routledge.*

Holt, Thomas J., & Bossler, A. M. (2016). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

https://doi.org/10.1111/j.1754-9469.2004.tb00055.x

Kasraie N. & Kasraie E., 2010: Economies of e-learning in the 21st Century. *Contemporary Issues in Education Research (CIER) 3(10), 57-62*

Kigerl A., 2012: Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review 30 (4), 470-486*

Kigerll A., 2012: Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review 30 (4), 470 - 486.

Kopp C., Layton R., Sillitoe J. & Gondal I., (2015): The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology 9(2)*

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198x.2019.1603527

Lennings C.J., Amon K.L., Brummert H. & Lennings N.J., (2010): Grooming for terror: The internet and young people. *Psychiatry, Psychology and Law 17 (3), 424 – 437.*

Leukfeldt E.R. & Yar M., 2016: Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior 37 (3), 263 - 280.

Martin N.& Rice J.,2011: Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security 30(8)803-814*

Matthyssens P., Kirca A.H., Pace S., Moen O., Madsen T.K. & Aspelund A., (2008): The importance of the internet in international business-to-business markets. *International Marketing Review.*

MFWA. (2017a). *Cyber Security in Ghana*. https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf

Ministry of Communication. (2014). *Ghana National Cyber Security Policy & Strategy*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Ghana_2014_NationalCyberSecurityPolicyStrategyFina.pdf

Miroo F., 2014: Routine Activity Theory. The Encylopedia of theoretical criminology, 1-7.

Mowery D.C. & Simcoe T., 2002: Is the Internet a US invention? - economic and technological history of computer networking. Research Policy 31 (8 - 9), 1369 - 1387..

Mukeredzi T., (2017): Uproar over Internet shutdowns: Governments cite incitements to violence, exam cheating, and hate speech. *Journal of Pan African Studies 10 (10), 7*

Newman R.C., (2006): Cybercrimes, identity theft, and fraud: practicing safe internet-network security threats and vulnerabilities. *Proceedings of the 3rd annual conference on information security curriculum development, 68-78*

Nyirenda-Jere T., & Biru T., (2015): Internet development and internet governance in Africa. *ISOC Report 17-53*

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019, April). E-government and the Challenge of Cybercrime in Nigeria. In *2019 Sixth International Conference on EDemocracy & EGovernment (ICEDEG)* (pp. 137-142). IEEE.

Orji U.J., 2019: An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. Computer Law & Security Reviews= 35(6), 105330

Paoli, L., Visschers, J. & Verstraete, C., (2018): The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. Crime, Law and Social Change 70(4), 397-420.

Perman, R., Ma, Y., McGilvray, J., & Common, M. (2011). Natural resource and environmental economics (4th ed.). Pearson Education.

Pratt T.C., Holtfreter K. & Reisig M.D., 2010: Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency 47 (3), 267-296.

Riley M & Robertson J., 2017: Russian cyber hacks on US electoral system far wider than previously known. Bloomberg, June 13, 2017.

serianu. (2017b). *Demystifying Africa's Cyber Security Poverty Line Botswana*. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Thornton A.L., (2001): Does the internet create democracy. African Journalism Studies 22(2), 126 – 147

Twigg C.A., (2002): The impact of the changing economy on four-year institutions of higher education: The importance of the internet. *The Knowledge Economy and postsecondary education. Report of a workshop, 77-104.*

Wall D.S.,2015: The Internet as a conduit for criminal activity. *Information technology and the criminal justice system, Pattavina A., ed 77-98*

Warner, J. (2011). *Understanding Cybercrime: A View from Below. International Journal of Cyber Criminology, 5(1),736-749.*

Webb L., Craissati J. & Keen S., (2007): Characteristics of internet child pornography offenders: comparison with child molesters. *Sexual abuse: a journal of research and treatment 19 (4), 449-465*

Weisner T.S., 2014; Why qualitative and ethnographic methods are essential for understanding family life. *Emerging methods in family research, 163-176.*

Whitty M.T., (2018): Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior and social networking 21 (2), 105-109.*

Wiggins, R. (2000): Al Gore and the creation of the internet. Retrieved on 11th December 2020 https://firstmonday.org/issues/issue5_10/wiggins/index.html

CHAPTER TWO

AN OVERVIEW OF CYBERCRIME FROM A GLOBAL PERSPECTIVE

This chapter reviews existing knowledge on cybercrimes concerning how other nationals perceive Ghanaians. The main purpose of a literature review is to be the building block upon which this research stands. Reviewing the literature enables an understanding of how this research adds to the existing body of knowledge on cybercrimes. The chapter begins with the definition of key concepts, and a review of some concepts related to this study like the need for cybercrimes.

This chapter also explores the conceptual relationship between the independent, dependent, and control variables. Lastly, this chapter discusses the hypotheses for this research.

2.1. An overview of key concepts

2.1.1. Concept of Crime

A crime is any action that causes harm in a situation that the person responsible ought to be held accountable for and be punished regardless of the laws of the country in which that crime was committed says (Morrison, 2013). Morrison further explained that crime can be viewed from the standpoint of being against the laws of God as seen in the Bible, Qur'an, and the Torah. He further stated that even if the country does not recognize it as a crime, once it goes against God, it can be viewed as a sin and therefore a crime. Crime to him is moral and should be seen as such.

Similarly, Reid (2015) agreed with Morrison. He stated that crimes that are not in the laws of a country can be punished by imprisonment and/or a fine. Even when a country does not have a constitution or any law of that sort, "sins" like murder, burglary, rape, and child neglect must be punishable by a required authority.

In Ghana, the Criminal Code of Ghana 1960 (Act 29) makes a clear definition of crime by defining crime as both the act or the action and the intent to commit the act. It further defines it as the breaking of rules or regulations for which a governing authority via mechanisms such as a legal system can ultimately prescribe a conviction (Adinkrah, 2011).

2.1.1. The Concept of Cybercrimes

Cybercrime is a special type of crime. According to NIBRS (2015), there are three types of crimes: crime against the person, crime against property, and crimes against society. Cybercrimes by their nature can fit into one or two or even three categories of crimes. Cybercrime is a very special form of crime as it involves the use of a medium, which is a computer in causing harm to others.

Cybercrime, as defined by Smith et al., (2004), encompasses a variety of terms such as computer crimes, computer-related crimes, digital crimes, information technology crimes, internet crimes, and virtual crimes. Cybercrime has therefore been very difficult to define due to its complexities. The United States Department of Justice (2009) defined cybercrimes in three stage classifications:

The first is in which the computer or its network is the target of criminal activity.

The second is where the computer is used as an accessory to commit a crime; a case in point is child pornography.

Lastly, the computer is used as an incidental aspect of the execution of the crime but may help generate evidence of the crime. For example, the phone records of a suspect who was used as an accessory to a crime could be considered in its terms as cybercrime.

The history of cybercrimes dates as far back as the 1960s (Aidoo et al., 2012) when the first incidence of computer crime was registered. Ever since then, cybercrimes have become commonplace in society (Kabay, 2008). The early cases of cybercrimes involved logging into

telecommunication systems without the right approval or authorization. The reason was mostly to destroy personal data for often financial gains. It aggravated the creation of malware to cause the misfunctioning of computers and servers in the 1980s. Although still happening, the very common form of cybercrimes especially in Ghana is that of identity theft.

2.1.3. Types of Cybercrimes

The 2013 Internet Crime Compliant Centre (IC3) Annual Report lists credit card fraud, bogus business opportunities, identity theft, hacking, phishing, and pharming as types of cybercrimes.

2.1.3.1. Identity Theft

Perhaps the most common type of cybercrime in Africa, involves the use of someone else's information, social security number, date of birth, or residential or office address without someone's knowledge for personal financial gain (Schmalleger & Pittaro, 2009). In Africa, it involves the use of another person's identity for romance scams especially. The social engineer pushes false information to gain the trust of the victim to dupe him for money or vital information. In order not to get caught, the social engineer uses a labyrinth of false information to gain financial rewards through untraceable means.

2.1.3.2. Cyber Pornography and Obscenity

In this type of cybercrime, sexually explicit images of people are used to exploit a person. The pictures may be genuine to a large extent, but the nature of use and extortion is what makes this a cybercrime. Also distributing naked pictures of children is a cybercrime in most jurisdictions in the world. This "illegal" industry is estimated to be a multibillion-dollar industry (Edelman, 2009). The internet is fast becoming a popular venue where sexual predators look or explicit images to satisfy their edges (Olayemi, 2004).

2.1.3.3. Hacking

Hacking is a process where hackers use their sophisticated knowledge of computers and technologies to gain access to a computer system often for malicious reasons (Holt, 2007). The activities of hackers cause economic and personal harm in every economy. The activities of hackers often disrupt the servers of internet providers or companies provide causing widespread economic loss and grievances.

2.1.3.4. Credit Card Schemes

Credit card theft schemes are the biggest cybercrime activity. It is so regular and difficult to solve that it is always been perpetuated. Credit card theft may be deliberately or in- deliberately caused. In the case of romance fraud, a victim may give his or her credit card details to the perpetrator due to the trust s/he has in the person. A credit card theft scheme occurs when a person uses the credit card details for economic activity with the original owner of the card not having any clue about what his or her card is being used for (Jabeen et al., 2023). According to a Eurobarometer survey conducted in 2013, 76% of respondents stated that they believed that they were at risk of being subject to a credit card theft scheme.

2.1.3.5. Merchandise, Auction Fraud, and Online Scams

The IC3 Annual Report (2013) also states that auction fraud involves the misrepresentation of a product by false advertising through the internet. It involves the attempt to make a bad deal appear legitimate. To dupe the victim, the suspect tells the victim to make full payment via a third-party agent before the falsely advertised product is delivered. When payment is made, the offender delivers a fake product while keeping the money.

2.1.3.6. Advance Fee Fraud

This cybercrime is said to have originated in Nigeria, it involves a kind of merchandise and auction fraud, the difference between advance fee fraud and merchandise fraud is that the victim is required to pay a series of fees to process transactions that are supposed to enable a victim to process a large sum of money. It has been nicknamed "YAHOO" in Nigeria; the nickname is a result of the use of the then-popular yahoo mail to engage in this crime. Warnet (2011) explained that this "419" scam began after the fall of the oil prices during the 1990s and since Nigeria is an oil-dependent country, it led to widespread poverty and some of the youth used this means to survive. This led to the blacklisting of Nigerian ISPs and the entire internet to be blacklisted by billion-dollar companies.

2.1.3.7. Fake News

Fake news has become prominent and has become a form of cybercrime against elected public officials. Fake news has become prominent due to the increase in the popularity of internet journalism. The journalism space has seen the highest form of democratization, and this has made the ability to censor news difficult. Although this is a positive thing, the negative aspect is that it has led to the rise of fake news where people deliberately misinform people. Fake news affects the integrity of journalism and makes it difficult for a journalist to create authentic stories for the ability of people to believe it (Pannee, Pattanapong & Titiya, 2021).

2.1.3.8. Deep Fakes

Deepfakes are regarded as one of the most forms of cybercrime and it has become increasingly difficult to deal with them due to their high level of sophistication (Vizoso, Vaz-Alvarez & Lopez-Garcia, 2021). Deep fakes are classified as a set of AI algorithms to synthesize multiple audiovisual products into one manipulated media item (usually videos), for example through face-swap

(Floridi, 2018). The term “deepfake” was first used in a Reddit post to refer to the result of the manipulation is a fake video built through a deep learning algorithm (hence, deepfake) in which a person is seen doing or saying something they never did in real life.

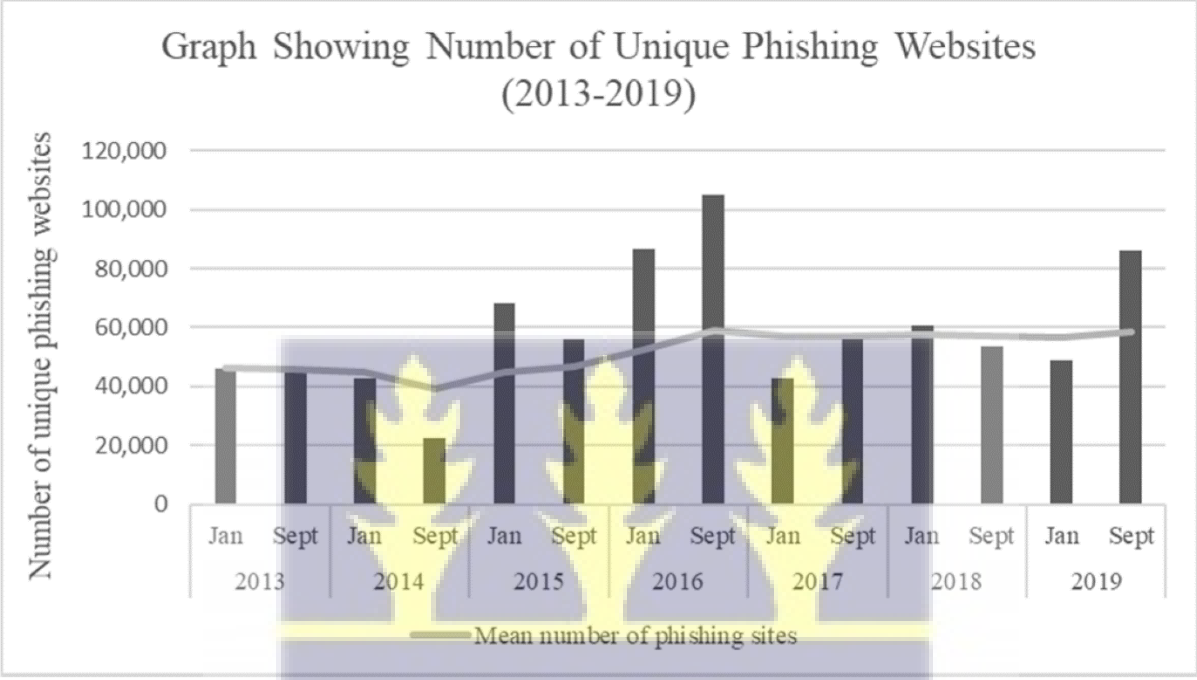
Unsolved deep fake implies that it leads to misrepresentation of what people have said and can cause wrong public disaffection for people. Deep fakes are therefore cybercrime committed against people. Deep fakes as a cybercrime erode public affection in key institutions and against people. Deepfakes recently is being used as a political tool to win elections. There have been several reported incidences of deepfakes in the 2016 US elections, and elections in Malaysia and Gabon (Dasilva, Ayerdi & Galdospin, 2021).

2.1.3.9. Phishing

In recent times, phishing scams have seen rapid growth and hence pose a huge threat to internet security (Alabadan 2020). A phishing attack is regarded as one of the most common and serious threats over the Internet where cybercriminals steal the personal and financial information of people using malware and social engineering. Many cyber security institutions have been working tirelessly to provide software that can detect phishing with a level of high accuracy.

Statistics from McAfee securities indicate that the number of unique phishing websites has increased over the years. The highest incidence of phishing was seen in 2016 when phishing websites rose to more than 120,000 reported cases. The war mounted by cybersecurity companies against phishing seems to have been working. Studies by Alsharnouby, Alaca & Chiasson (2015) indicate that users successfully detected only 53% of phishing websites even when primed to identify them and that they generally spend very little time gazing at security indicators compared to website content when making assessments.

Figure 2. A graph indicating the number of unique phishing websites from 2013 - 2018



2.1.3.10. Social Engineering

Another type of cybercrime is social engineering. Social engineering involves targeting the weakness of a system through various manipulation techniques to elicit sensitive information. The field of social engineering is still in its early stages concerning formal definitions, attack frameworks, and templates of attacks (Mouton, Leenen, & Venter, 2016). Social engineering has become prevalent through social media platforms. Social network sites are critical in weakening one's security and privacy due to a large amount of information available on them, as well as their very large user base. Studies by Irani, Kirda & Pu (2011) show that users of online social networks tend to exhibit a higher degree of trust in friend requests and messages sent by other users. Cybercriminals help use reverse social engineering attacks where the attacker does not initiate contact with the victim. Rather, the victim is tricked into contacting the attacker herself. This

results in a high degree of trust being established between the victim and the attacker as the victim is the entity that established the relationship.

2.1.3.11. Sim card fraud

Sim swap is technically a new form of cyber fraud where hackers gain personal information and does illegal work with a person's bank account, and credit card numbers. Cybercriminals exploit a weak two-factor authentication to swap a sim card. Lately, phone numbers are associated with individuals' phone numbers and information and the ability to swap someone's number indicates that you can have access to their personal information and data (Valentine, 2021). Account changes that involve switching SIM cards can be done in two ways: a SIM swap or port out. A port out transfers the phone number to a new account with a new wireless carrier. In a port out, the SIM cards are from different carriers, whereas a SIM swap retains the phone number and account with the current carrier while transferring the number to a different SIM card only.

2.1.3.12. Ransomware

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands a ransom payment to regain access. Ransomware is a rapidly growing threat to the data files of individuals and businesses. It encrypts files on an infected computer and holds the key to decrypt the files until the victim pays a ransom. This cybercrime is responsible for the annual loss of hundreds of millions. As the amount to be made is large, new versions appear frequently thus allowing the bypassing of antivirus software and other intrusion detection methods (Richardson & North, 2017). Many ransomware operators cashed out using BTC-e, a now-defunct Bitcoin exchange. In total, we can track over USD 16 million in likely ransom payments made by 19,750 potential victims over two years (Huang et al., 2018).

2.1.3.13. Botnet and Free-Wi-Fi

Botnet comprises many compromised hosts under the control of the botmaster remotely (Chen et al., 2017). The architecture of the botnet has evolved to evade detection and disruption. Traditionally, bot programs are constructed as clients which communicate via existing servers. This allows the bot herder (the controller of the botnet) to perform all control from a remote location, which obfuscates the traffic (Schiller, 2007). Accessing suspicious free WiFi may lead you to be hacked by a cybercriminal as your phone or laptop is connected to a botmaster and he can steal and access your device remotely.

2.1.4. Efforts to thwart cybercrime

Since the dawn of cybercrime, there have been several concerted efforts to combat cybercrime. These measures are targeted at making it difficult to commit cybercrime and also reducing the incidence of the menace. Some of the efforts to combat cybercrime include:

2.14.1. Pin Codes and Passwords

A password equally known as a passcode is secret data, typically made up of a string of characters, usually used to confirm a user's identity in a system. A Pin code is numeric data used to authenticate a user. Passwords can be traced to ancient times as it was used as a system of authenticity. In the olden days, only those with a password were entering and exit out of a place. Passwords and pin codes have been used with computers since the earliest days of computing. This old piece of technology remains one of the most relevant tools in preventing cybercrimes (Tran, 2020).

Passwords, therefore, are at the heart of ensuring the security of a system. To combat cybercrime, cyber experts recommend the following:

1. The use of strong Passwords and use different user IDs.
2. Making the password more complicated through the combination of letters, numbers, and special characters.
3. Change password frequently.
4. Keeping passwords only to yourself and not sharing them with anyone.
5. Avoid replying to emails from unknown people and sources.
6. Only log in to trusted websites.

2.1.4.2. The use of face scan

Kaspersky defines a face scan as a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time. The technology is used primarily for security and law enforcement. Face scan/face ID is a new technology used to combat cybercrime (Fahlevi et al., 2019).

The facial recognition market was pegged at 3.97 billion USD in 2018 and is predicted to hit 10.15 billion USD by 2025. Face scan is primarily used for data protection as it is more secure than a regular password. According to Harris & Zagaris (2019), the use of face ID or face scan can reduce the current prevalence of cybercrime.

2.1.4.3. Fingerprint readers and technology

Fingerprint readers have emerged as one of the ways of helping stop the activities of cybercriminals (Shukla et al., 2022). Fingerprint readers have several other important successes as eliminating the need for consumers to remember all their passwords, Fingerprints are harder to hack as it is harder to have the same fingerprint as someone.

Fingerprinting techniques are based on detecting patterns and observing differences in the network packets generated (Suleiman et al., 2020). The two types of fingerprinting technology are active and passive.

Active fingerprinting involves sending TCP or ICMP packets to a system and analyzing the response from the target (Naik et al., 2021). The packet headers contain various flags that cause different operating systems and versions to respond differently. However, active fingerprinting brings with it the risk of easy detection.

Passive fingerprinting techniques are stealthy as they do not involve sending any packets to the target system (Mashima, 2022). They rely on scanning the network as sniffers to detect patterns in the usual network traffic.

Fingerprint technology and scanners are now available on laptops and mobile phones, and it provides safety against illegal access to a device.

2.1.4.4. Firewalls

A firewall is a network security software designed to monitor incoming and outgoing network traffic and permits and certain blocks data packets based on a set of security rules (Krishnan et al., 2022). Firewalls exist to protect a user from the activities of cybercriminals. Firewalls help to enhance privacy by allowing the ability to block or hide the DNS information of all internal hosts (Anwar et al., 2021). It enables only the IP address of the firewall to be available from the internet. Firewalls act as a barrier against trojans directed to computers by cybercriminals. Firewalls prevent the activities of cybercriminals by blocking these viruses directed to a network or a computer by criminals thereby helping to protect the system against potential theft.

2.1.4.5. Anti-virus, anti-hacking, and Phishing Software

Anti-virus and phishing software are equally another way of fighting cybercrime. It works by creating a database of known viruses and spam algorithms for cybercrimes. To maintain the integrity of anti-virus and phishing software, developers of anti-virus and phishing software constantly update the database with new viruses and new algorithms for cybercriminal activities (Al-Asli & Ghaleb, 2019).

Phishing happens when a cybercriminal tries to trick you into giving them your personal information, such as your password or credit card number. They do this by sending you an email that looks like it is from a legitimate website. Phishing attacks can be classified into two categories which are social engineering and malware-based phishing attacks. The anti-phishing solutions can be differentiated into two types which are phishing prevention and phishing detection (Apandi, Sallim, & Sidek, 2020).

What anti-phishing software does is prevent a user from receiving such emails that will lead to a user accidentally clicking on an unsafe link to comprehensive his or her security. A software called "Anti Phishing Simulator" evaluates mail contents and through its database by Bayesian algorithm is provided (Baykara, M., & Gürel, 2018).

Anti-hacking software works like phishing software in the way that it analyses the contents of an email and matches it with its database and blocks a user from accessing certain services and emails. Microsoft has an anti-hacking software named "WINDOWS DEFENDER" which does all three, anti-virus, anti-hacking, and anti-phishing.

2.2. Causes of Cybercrime.

The reason why people commit cybercrime differs from person to person. To some, it may be an economic while to others it may be a form of entertainment. To others, they commit a crime because they want to live a life as portrayed by Hollywood celebrities. It can also be pinpointed to a lack of a good upbringing from parents or guardians (Nayak, 2013). Some also engage in cybercrime as a result of revenge.

2.3. Cybercrime in the West

The recent COVID-19 pandemic which has forced many people to work from home has increased the incidence of cybercrimes as now more people than ever spend a lot of time on the internet (Hawdon et al., 2020). Cybercrime has caused a lot of damage to individuals, organizations, and the government (Ramdinmawii et al., 2014) as the West is often at the receiving end of cybercrimes. Several laws and methods have been enacted to reduce cybercrime in the West yet still cybercriminals are finding newer ways to outsmart the system. For instance, in 2013, nearly $782 million was lost in America due to cybercrime (Ramdinmawii et al., 2014).

To reduce cybercrimes, the United States of America has enacted several acts and created institutions. The National Information Infrastructure Protection Act of 1996 aimed at protecting individuals against various computer-generated offenses. According to this act, anyone who deliberately breaks into a computer to obtain classified or restricted information is subjected to criminal prosecution.

In the UK, they also sort to reduce the incidence of cybercrimes through legislation. The Computer Misuse Act of 1990 was enacted to deter the use of abuse using the computer. This act was to deter people from hacking into other people's computers. The UK also introduced the Privacy and

Electronic Communications Regulations in 2003 and this tried to prevent spam emails aimed at breaking into someone's private affairs using the computer. The UK also adopted the European Convention on cybercrime designed to provide a common international framework to deal with cybercrime.

2.4. Cybercrime in Africa

Cybercrime is not peculiar to the West and the East; Africa has had its fairer share of cybercrime. In Africa, cybercrime is more of an "exported" commodity to the outside world than it is "imported" to Africa. Cybercrime, therefore, differs from that of Europe and Asia. The reason for it being different is that in Africa, there are inadequate regulations and virtually no cross-border collaboration coupled with weak law enforcement (Olowu, 2009).

In Africa, Nigeria holds the title of having the highest prevalence of activities of cybercrime. Indeed, "419" or "Yahoo boy" has tinted the country so much that being a Nigerian often has negative connotations. It holds the record for being the third country globally with the highest incidence of cybercrime to better its image, the government has enacted several laws to make committing cybercrimes in Nigeria difficult. The first of its time was in 2006 when the government passed the Advanced Fee Fraud and Related Offense Act. The act empowered the Nigeria Economic and Financial Crime Commission (EFCC)to clamp down on cybercriminals by regulating industry players such as internet cafes and telecommunication industries not to allow their institutions to be used as a conduit for cybercrimes if they can disallow them. The ineffectiveness of this act, the country through its legislature is seeking to enact laws such as the Cyber Security and Critical Infrastructure Bill, the Electronic Commerce Bill, Computer Security Protection Bill, and the Evidence Act Amendment Bill to help stop cybercrimes. These bills are still in the legislature pending approval.

Aside from Nigeria, the IC3 for instance states that other top destinations include South Africa, Kenya, Ghana, Egypt, South Africa, Zambia, and Cameroon. Despite South Africa being the most advanced country in Africa, it still suffers a high incidence of cybercrimes. The country is also a known destination for cybercrimes in Africa. The level of cyber-attacks on organizations has increased in recent years as more people are getting to the internet (Bouggardt & Kyobe, 2011). They like their Nigerian counterparts have enacted several laws to deal with cybercrimes. The "ECT' act of 2002 was introduced to address the incidence of cybercrimes and although it has been applauded as a landmark law in reducing cybercrime, experts have said it needs improvement to address newer emerging types of cybercrimes (Cassim, 2010). Malware and computer viruses as of 2013 made up the biggest portion of cybercrime (Grobler et al., 2013) and the ECT act was inadequate to reduce those incidences of cybercrimes.

Kenya is known to be highly advanced when it comes to IT in Africa. It is hence not surprising that cybercrime is higher there also. Cybercrime is higher in their capital, Nairobi than anywhere in their country (Magutu, 2011). Cyberbullying is very common in Kenya and is still on the rise. Cybercriminals use social media, emails, blogs, and websites to cause harm to others (Kamau, 2016). Although Kenya has legislation to guard against cybercrime, the Kenya Information and Communications Act and the Cybercrime and Computer Related Crimes Bill of 2014 does not make provision to guard against or punish those who engage in cyberbullying.

2.5. Nigerians and the negative perception as a result of cybercriminals

As of July 2020, official figures indicated that 99.05 million Nigerians were on the internet. This figure represents 46.6% of their total population. More people having access to the internet has translated to higher levels of cybercrime in the country (Izuakor, 2020). The internet has since provided unscrupulous Nigerian fraudsters the platform to reach victims within and across national

borders. Nigerians already have a poor name when it comes to cybercrime. As in other parts of the globe, cybercrime in Nigeria is both internal and international. Internal cybercrime in this context involves cybercrime activities that are committed by Nigerians living in Nigeria to other people living in the same country. International cybercrime on the other hand involves cybercrime activities that are committed by cybercrimes committed by Nigerians living in Nigeria or other countries to other nationals living in other countries.

Nigerians in the international community suffer negative consequences as a result of their country's deteriorating image as a result of cybercrime. Nigeria is consequently regarded as the headquarters of Advance Fee Fraud in Africa. Citizens of the country suffer from a negative image both in Africa and in the rest of the world. The origin of the name "419" which is synonymous with cybercrimes emanates from the Nigerian regulator's attempt to curb the menace (Mba, Stringhini & Cavallaro, 2017). The externalities of the impact of cybercrime can also be seen in how romance scam has been christened "The Nigerian Prince."

2.5.1. Popular Nigerian Cybercriminals

The popular Nigerian cybercriminals include Ramon Olorunwa Abbas popularly known as Hushpuppi, Obinwanne Okeke, popularly known as Invictus Obi, and Ismaila Mustapha (Mompha) have all damaged the reputation of Nigerians.

2.5.1.1. Hushpuppi

Known in real life as Ramon Abbas, Hushpuppi gained public notoriety for his activities in cybercrime. Hushpuppi portrayed himself as a Nigerian Instagram influencer who dealt in real estate. He was arrested by the International Police (Interpol) and Federal Bureau Investigation (FBI) on the count of identity theft and several categories of cybercrimes. His arrest was in connection with a $35 million ventilator scam and also in connection with several laundering

activities worth hundreds of millions of dollars in illicit proceeds from email scams and other cyber-enabled fraud, including a scheme that targeted an English Premier League football club (Ayub, 2021).

Hushpuppi with his accomplice is alleged to have duped nearly two million people who were residents in America, Europe, and Nigeria. Hushpuppi's modus operandi was done through fake websites of well-known banks and companies. Through the cloned websites, he opened the credit card information of his victims and used the stolen credit card to fund his lavish lifestyle.

It has been reported that the investigators of Hushpuppi recovered documents that linked him to a global scale fraud of £352 million. The raid that led to his arrest, as well as 11 other people, led to the seizure of almost $41 million, 13 luxury cars worth $6.8 million including phones and computers containing more than 100,000 fraud files.

2.5.1.2. Naira Marley

Azeez Fashola is a popularly Nigerian musician who was accused of having committed credit card fraud by the Economic and Financial Crimes Commission (EFCC) and arraigned before Lagos Federal High Court. The musician, popularly known as Naira Marley, is famous for heaping praises on cybercriminals in his songs and on social media platforms. The musician is alleged to have used different Access Bank ATM Cards to defraud people for fraudulent financial gains.

The singer was caught in possession of counterfeit credit cards of different cardholders with intent to defraud, which also constituted theft, though, he denied the charges.

2.5.1.3. Invictus Obi

Obinwanne Okeke, popularly known as Invictus Obi was a popular Nigerian businessman who was once featured on the front page of the renowned Forbes magazine, for being a part of the most

influential business- people in Ghana. He has been jailed for 10 years in the USA over a cyber fraud scam in which he admitted to duping people to the sum of $11m (£8m).

It was alleged that he used his Nigerian-based companies to scam people in the US. His company used phishing emails to steal funds from victims. Investigations also revealed that from around 2015 to 2019, he was part of a group that engaged in a conspiracy to conduct various computer-based frauds, including creating fake websites, the US Attorney's Office in the Eastern District of Virginia said in a statement after he was sentenced. His company was at the center of working with conspirators to create profiles of hundreds of victims including people in the US's Eastern District of Virginia.

References

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future internet, 12(10), 168.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.

Al-Asli, M., & Ghaleb, T. A. (2019, April). Review of signature-based techniques in antivirus products. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

Apandi, S. H., Sallim, J., & Sidek, R. M. (2020, February). Types of anti-phishing solutions for a phishing attack. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012072). IOP Publishing.

AYUB, A. O., & RASAKI, A. J. (2021). Modus Operandi and Socio-Demographics of Cybercrimes' Perpetrators and Victims in Nigeria. Gusau Journal of Sociology, 128.

Baykara, M., & Gürel, Z. Z. (2018, March). Detection of phishing attacks. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5). IEEE.

Chen, R., Niu, W., Zhang, X., Zhuo, Z., & Lv, F. (2017). An effective conversation-based botnet detection method. Mathematical Problems in Engineering, 2017.

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. In E3S Web of Conferences (Vol. 125, p. 21001). EDP Sciences.

Haris, A., & Zagaris, B. (2019). Cybercrime. IELR, 35, 455.

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... & McCoy, D. (2018, May). Tracking ransomware end-to-end. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 618-631). IEEE.

Izuakor, C. F. Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context.

Jabeen, U., Singh, K., & Vats, S. (2023, August). Credit Card Fraud Detection Scheme Using Machine Learning and Synthetic Minority Oversampling Technique (SMOTE). In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 122-127). IEEE.

Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing, 12(1), 26.

Mashima, D. (2022). MITRE ATT&CK based evaluation on in-network deception technology for modernized electrical substation systems. Sustainability, 14(3), 1256.

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In Proceedings of the 26th International Conference on World Wide Web Companion (pp. 1301-1310).

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. Computers & Security, 59, 186-209.

Pérez Dasilva, J. Á., Meso Ayerdi, K., & Mendiguren Galdospin, T. (2021). Deepfakes on Twitter: which actors control their spread?

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation, and prevention. International Management Review, 13(1), 10.

Schiller, Craig A.; Binkley, Jim; Harley, David; Evron, Gadi; Bradley, Tony; Willems, Carsten; Cross, Michael (1 January 2007). Botnets. Burlington, Virginia: Syngress. pp. 29–75. doi:10.1016/B978-159749135-8/50004-4. ISBN 9781597491358.

Shukla, V., Deshmukh, A., & Tyagi, A. K. (2022). Role of Artificial Intelligence in Cyber Security: A Useful Overview. In Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks (pp. 92-104). IGI Global.

Suanpang, P., Pothipasa, P., & Netwrong, T. (2021). Policies and Platforms for Fake News Filtering on Cybercrime in Smart City Using Artificial Intelligence and Blockchain Technology. International Journal of Cyber Criminology, 15(1), 143-157.

Schonlau, M., Guenther, N., & Sucholutsky, I. (2017). Text mining with n-gram variables. The Stata Journal, 17(4), 866-881.

Tran, C. (2020). Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. arXiv preprint arXiv:2006.11929

Valentine, J. P. (2021). Sim Card Fraud (Doctoral dissertation, Utica College).

Vizoso, Á., Vaz-Álvarez, M., & López-García, X. (2021). Fighting deepfakes: Media and internet giants' converging and diverging strategies against Hi-Tech misinformation. Media and Communication, 9(1), 291-300.

CHAPTER THREE

ANALYSIS OF CYBERCRIME AND ITS IMPLICATIONS FOR THE GHANAIAN IN THE INTERNATIONAL COMMUNITY.

3.0. Introduction

This chapter was developed from primary data gotten through the two focus group discussions, and expert interviews as well as from secondary data obtained from other researchers conducted by other researchers, recognized institutions, and journals. Primary data were solicited from the person listed under Chapter 1.9. This chapter addresses the objectives of the research based on the research questions and underdeveloped themes from the findings.

3.1. Potential of the internet

The potential of the internet can be seen in how it has changed our communication with people in the outside world. The positive aspect of the internet can be explained through various sectors such as the banking system, and the educational sector among other sectors. The benefits of the internet have been enjoyed by citizens in every country in varying proportions. Through the internet, several Ghanaians are getting access to enjoy banking services. A significant number of Ghanaians have previously been unbanked due to several factors including low wages in the country, and the cost of running a bank account among other reasons (Senyo et al., 2022). Mobile money, an electronic banking service provided by telecommunication networks, allows its subscribers to store funds, send and receive money, make purchases, and do online transactions through mobile money with or without the internet. The popularity of mobile money in Ghana has increased the number of people who now have bank accounts and can transact online services. Payment platforms such as Flutter wave, Hubtel, Paystack, and SlydePay among others have made it easy to access services

that were initially exclusive to credit and debit cardholders. Mobile money has made it possible for users to electronically lend personal and business loans.

The adoption of the use of the internet in the lives of Ghanaians has transitioned companies from physical stores to virtual stores. Rather than queue for food, some Ghanaians rely on food delivery services like Hubtel, Glovo, and Bolt. The growth of online restaurants and food delivery services was necessitated by the COVID-19 pandemic and the lockdown that was instituted to help reduce the spread of the virus.

The respondents in the first focus group discussion noted.

"The internet has gotten big, and the potentials are limitless. It was through the lockdown that I chanced on food delivery apps. I now buy food from Bolt Food…I don't remember the time I went to a restaurant to eat." **(FGD 1, 9th January 2022)**

Another aspect of the potential of the internet can be seen in the transportation industry. The internet has digitized the transportation system through ridesharing apps. It has made it possible for people to order a ride in the comfort of their homes. Aside from this comfort, it has given people both full-time and part-time which was earlier not possible. There has been an increase in the popularity of what is termed "gig jobs."

During the focus group discussion, one of the respondents said,

"*I know a lot of graduates who are operating ride-hailing services. During the banking sector clean-up, many of the bankers I know who got laid off started full-time uber driving. Without the internet and services like Uber or bolt, I have no idea what they would have done."* **(FGD 1, 9th January 2022)**

3.2. The Definition of Cybercrimes according to Ghanaians

The literature indicates that even among experts, cybercrime is puzzling to define as such cybercrime means different things to different people. It is of the essence therefore to know which categories of crime people see as cybercrime. How people understand cybercrime informs their judgment about people they perceive as likely culprits of the act. The average Ghanaian living in Ghana has a limited view of what cybercrime means. This research seeks to explore the negative externalities of cybercrime on Ghanaians living in the international community, however, it is essential to explore what Ghanaians define as cybercrime. One of the respondents in the second focus group discussion summed up cybercrime as:

Cybercrime is the use of the internet to steal from others, especially money. **(FGD 2, 3rd April 2022)**

The businessman said:

I know cybercrime is using the internet to steal money from people. This is what these "sakawa" or 419 boys do. They use their laptop to steal people's valuable goods and services. I know of a certain guy; all he does is stay at home and change cars. They say he is a "sakawa" boy. If you even see his hairdo, you can tell that he does cybercrime…. He is a cybercriminal. **(FGD 1, 9th January 2022)**

Cybercrime is very difficult to define as the dimension of crime keeps changing. In more recent years, cybercrime has come to denote the use of computer technology to commit or facilitate the commission of unlawful acts or crimes. In the expert discussion, one of the experts gave a unique definition of cybercrime which was similar to one of the definitions gotten through the literature guide.

The respondent defined cybercrime as:

'Crimes that are mainly committed through the use of the internet. In my opinion crimes such as wire fraud, spamming, identity theft, and love scams are examples of cybercrime." **(IDI, 10th April 2022).**

Through the focus group discussion, it was apparent that all the participants thought of cybercrime as mainly using the computer and the internet to steal money. Their narratives seem to suggest that cybercrimes deal with the stealing of money. The narratives were confirmed by two people from the focus group discussion. The victim of cybercrime is defined as cybercrime:

as the use of the internet, computer, or phone to steal money or credit card information from people. **(FGD 1, 9th January, 2022)**

Cybercrime, however, goes beyond using the internet to steal money from people. Cybercrime equally involves using the internet to steal valuable information from people. As stated in the literature review, there are other cybercrime acts such as ransomware, the trading of child pornography, and botnets among others. It was apparent from the expert that cybercrime goes beyond what the general Ghanaians seem to view cybercrime to be. The known interpretation of cybercrime is because of the popularity of romance scams in that space. An expert also corroborated this view by saying.

"Ghanaians think cybercrime is all about scamming people out of their money. However, cybercrime goes beyond that. It is using the internet to commit a crime against someone. For example, cyberbullying does not involve stealing money, but it is a cybercrime. I see cybercrime therefore as using the internet and the computer to commit a crime." **(IDI 3, 9th April, 2022)**

The skewed perception of Ghanaians toward cybercrime is due to how fraud has been heavily marketed in our media. The Ghanaian media consumption behaviour has therefore reinforced the narrative of cybercrime as stealing money. The narrative has also been heightened by how we project "419" and romance crime.

3.3. What is the implication of the rising incidence of cybercrime on the image of the Ghanaian in the international community?

The activities of cybercriminals have several negative externalities on citizens of any given country. Firstly, it leads to the deterioration of the image of the Ghanaian in the international community. Ghana is fast losing its image in the world despite the government's best efforts to reduce the prevalence of cybercrime. The country's damaged reputation can be explained through how some Ghanaian use cybercrime to aid corruption, money laundering, military espionage, and terrorism and overall, undermine the technological and socio-economic development of the country (Jackson, Ene & Ene, 2016). As crime becomes globalised, citizens of countries suffer from the impact of cybercrimes committed by nationals of their country. To understand the gravity of cybercrimes, it is essential to note which nationals are likely to commit cybercrime. In Nigeria, cybercrimes in Nigeria are largely perpetrated by young men popularly called yahoo-boys or yahoo-zee millionaires. Unemployed Nigerian youth some of whom are undergraduates of Nigerian universities are (Folashade & Abimbola, 2013) involved in hacking, cloning, and defrauding unsuspecting victims using tools such as password crackers, key loggers, network sniffers, port scanners, vulnerability scanners, exploits, and so on. In Ghana cybercrimes are highly sophisticated, it is committed by those who have some level of literacy.

3.3.1. The perspective of the impact of cybercrime on Ghanaians

The impact of cybercrime on Ghanaians can be explored from two perspectives: The first impact concerns the services freely available to Ghanaian online. The second is the perception of the Ghanaian during a business transaction both online and in person. Today, most Ghanaians and their businesses are registered and can be found on several social networking platforms. Due to the activities of cybercriminals, the country has gained a reputation as a known source of cybercrime. This has led to a negative perception of Ghanaians by the international community.

The participants were asked about the impact of cybercriminals on Ghanaians in the international community. They answered that cybercrimes have an often-negative impact on the Ghanaians, this is what one of the respondents", a businessman, stated:

"Definitely. The activities of cybercriminals have an impact on Ghanaians in the international community. For example, take a look at Nigerians, everyone thinks that they are frauds, due to the action of a few Nigerians. I am not sure that even 5% of Nigerians are bad people but we have negative perceptions about Nigerians due to the actions of a few Nigerians. I believe this is what other citizens see us. They think we are a bunch of cybercriminals, hence when we are doing business with the outside world, it is not conducted in a place of goodwill. This term that you call "externalities" is why stereotypes exist. Someone can commit a crime and then you will hear, "As for Ewes, that is how they are all." I believe that this is the same for cybercrime. A few lazy boys will go and steal from the white man and then I, XXXXX, who is doing his legitimate business in Ghana and Europe will suffer negative consequences from it. I remember the last time, before COVID19 of course, I was in the UK, this white man I was dealing with kept on looking down on me, thinking that I am a criminal. Someone he knew had been duped by a Ghanaian. The thing is that he wasn't even certain if he was a Ghanaian, but you see, he will go around spreading rumors

that Ghanaians are frauds, but he will forget that not all Ghanaians are frauds and that the fraudsters are the minority in the system". **(FGD 1, 9th January, 2022)**

The problem with the impact of cybercrimes on Ghanaians is that it is mostly the innocent who largely suffer its negative consequences (Khan et al., 2015). While the cybercriminal may have scammed one person, often a Western individual, little does he know that his actions have a severe impact on all Ghanaians at home and abroad. Most of the people affected by his actions will never meet in life. The negative impact of cybercrimes on Ghanaians can be observed by most international companies that have blacklisted the country from their services.

In the first focus group discussion, one participant who had been a victim of cybercrime stated that" *she was never going to use Visa cards online again. She felt uncomfortable using her Visa Card for any online transaction".* Apart from this, Ghanaians are not able to use certain international services. Money transfer from Ghana to any other country is very convoluting. It is not possible to send money from Ghana to other countries using Western Union, MoneyGram, and others. This is because Ghana is deemed as one of the hubs for cybercrime, hence allowing people to send money from Ghana abroad maybe enable the activities of cybercriminals.

One of the technology experts on the panel stated:

"At where I work from, I see the direct impact of the Ghanaian deteriorating image due to cybercrime. I remember when we were doing our latest update in our company, we had to talk to a representative of XXX and the kind of stringent rules they gave to us were outrageous. During the series of meetings we had, they always looked suspiciously at us because of the stories of cybercrimes they have heard about Ghanaians." **(IDI 5, 11th April 2022)**

From the expert interview, it was apparent that these activities of cybercriminals have negative externalities on Ghanaians living abroad and Ghana. This shows that issues regarding cybercrime should be of prominent concern to the government. As Ghana wants to promote a pristine image, the country must take a hard stance on cybercrime.

3.3.2. How news about Ghanaians caught in cybercrime has impacted the image of Ghanaians living abroad?

There are numerous examples of Ghanaians who have been caught engaging in cybercriminal activities. For instance, on 7th February 2021, six Ghanaians were arrested and sent to court on the count of stealing $50m through acts of cybercrimes. The six Ghanaians were said to have compromised emails of prominent people, engage in a series of romance scams targeting the elder, and defrauded small businesses in the United States of America (US Department of Justice, 2021). Cybercriminals of Ghanaian origin even commit cybercrime against their countrymen. There is also a reported case of cybercrime that involved a mother and her daughter robbing their victims to a tune of US$6m. They were arrested by America's Federal Bureau of Investigations (FBI) on 21st April 2022. Their cybercriminal activities were said to have happened between July 2018 and April 2022. Their arrest further heightened the negative perception of Ghanaians in that jurisdiction.

These stories have an impact on the lived experiences of Ghanaians abroad. Lived experiences are the experiences of an individual and the knowledge that they gain from these experiences. Experiences are important in evaluating how people relate with others. This can lead to innocent people receiving negative treatment from others (Halana & Smith, 2019). This equally impacts the

confidence of Ghanaians in the international community. Lived experiences of cybercrime suffered by Ghanaians are both internal and external.

3.3.2.1. External Lived Experiences of Ghanaians abroad concerning cybercrime.

The external lived experiences of cybercrime involve negative externalities suffered by Ghanaians abroad as a result of perceived cybercrime risk. Research conducted by Rajan, Ravikumar & Shaer (2017) indicates that the financial implications of cybercrime can lead to citizens of a country facing reputational damages. As more news about Ghanaians caught in cybercriminal activities emerges, other Ghanaians living abroad suffer reputational damage. The research revealed that although Ghanaians have a good image in the international community, the reported incidence of cybercrime is impacting negatively on the previous pristine. One of the Ghanaians in the international community remarked:

*"Ghanaians are generally respected in the international community. I do not know if I should compare us to Nigerians but when we compare Ghanaians to Nigerians, we do not experience so many negative stereotypes regarding cybercrime. Regardless, when you mention the name of Ghana, people link us to cybercrime. People look at you when you say you come from Ghana which is close to Nigeria and they look at you as if you are a cybercriminal…Sometimes, what some of my friends do to escape this…is to lie that they are Americans. "(***FGD 2, 3rd April, 2022)**

Several pieces of research have been done on cybercrime and victimisation. Research by Virtanen (2017) indicates that citizens of countries where cybercrime is prevalent suffer victimisation and vulnerabilities. In the focused group discussion focused on Ghanaians living abroad, they experienced several episodes of victimisation that they suffered as a result of news articles exposing the activities of certain Ghanaians engaged in cybercrimes.

The former ambassador added his views to the conversation by stating:

"During my tenure, there were instances where Ghanaians were arrested for cybercrime offenses. I must say there are a lot of Ghanaians living in the USA, but the activities of these few criminals have an impact on a lot of Ghanaians living in America. When you are in the IT circles and you mention that you are in Ghana, they look at you with suspicion as if you are a cybercriminal! It is not about you; it is always about stories of Ghanaians committing cybercrime that they have heard". **(IDI 8, 29th May 2022)**

3.3.2.2. Internal Lived Experiences of Ghanaians living in Ghana concerning cybercrime.

The internal lived experiences of cybercrime involve cybercrime issues suffered by Ghanaians. In the first focus group discussion, internal lived experiences of cybercrime were discussed.

When asked about some of their lived experiences, these are what some of the participants said:

"At times, I want to subscribe to certain educational materials on the internet but due to my credit card being issued in Ghana, I am unable to do so…. It also extends to entertainment materials; for instance, when you create a Netflix account from Ghana, you are unable to access certain content as they feel that…in Ghana…we are inferior. It took a long time before we were able to use Spotify in Ghana, I think Spotify came to Ghana last year or so. So, imagine being a creative person, you are automatically cut off from one of the world's biggest streaming platforms. Sometimes, we have to use VPN to access certain materials on the internet because if you use your location as Ghana, you are automatically cut off certain services. **(FDG 1, 9th January, 2022).**

The businessman corroborated the story of the student by saying:

What my young brother is saying is very true. You know, as part of my business, I sell African products like shirts, beads, and a host of others online. Sometimes, some of my online customers, especially foreign ones ask if I use PayPal. When I reply that I don't have it, most of them end up not buying my stuff. Although I can accept online payment, most of these foreign customers are not willing to use their Visa and Mastercard to purchase my goods and services because they are afraid of their card details being leaked. The reason why this is so that they are so many "sakawa" boys in the system. Immediately they notice that you are a business based in Ghana, and a red flag is raised. How I wish the government can do something about the "sakawa" menace. Last year too, I heard that PayPal was going to be operational in Ghana, I don't know what happened to it. Does anyone know what happened to it? **(FGD 1, 9th January, 2022).**

On how cybercrime affects the psychological and mental state of those who have directly suffered under cybercrime, a victim who had been duped online stated:

As for me, I have stopped using MoMo (Mobile Money), I don't trust anything on the internet. I prefer to deal with cash instead. You know what they say…Cash is king. I have been directly duped on the internet twice, so I don't trust anything online. These "Sakawa" boys on the internet are very smart. I don't buy anything online. I can like something very much but so far as I would have to pay online, I would not…If the company does not offer "Pay on Delivery" (POD) then I would not buy that thing. **(FGD 1, 9th January. 2022).**

When asked to narrate that he got duped online, he continued:

One day, I saw something online…It was my daughter who saw it. So, I ordered it online with my Visa Card, I think they call the website, All Baba? Yes…Alibaba, they say is Chinese. I don't know what I did wrong, when I ordered the stuff, I was debited, and my bank sent me that bank alert via

SMS. Before I realized it, someone had used my card to buy goods and services worth Ghc8,904. I reported it to my bank, and they were not able to trace the culprit. I thought it was my daughter, but she says she wasn't the one. I ended up losing Ghc8,904. And the second time, it happened, someone sent me Ghc1,000 via MoMo. I saw two text messages. A person later called, and he was panting, he said he had sent Ghc1,000 to my account by mistake and that it was for her mother's medical bill. I sent it to him. Later, I realized that he was a fraud. That day, I cried. That month I virtually starved. I cursed him. I have not used MoMo since then" **(FGD 1, 9th January 2022).**

On MoMo fraud, Akomea-Frempong, & Andoh (2019) have stated that telecommunication networks must intensify their campaign to make sure that the incidence of mobile money fraud is brought to its barest minimum. Their research concluded that the Momo fraud scheme was a syndicated action by certain workers of the telecommunication network and then the Mobile Money agents. This was corroborated by the policeman in the focus group discussion. He stated,

We have traced one of these Momo frauds and realized that sometimes it is these same Momo agents who commit these crimes. I remember a case that happened this year (2021). When the person sent Ghc700 to her customer, the Momo agent went behind his agent and then duped the person who received the money. One of my colleagues too worked on a similar case. So with your case (about the culprit of the cybercrime), it might have been the Momo agent who was behind it. Else who would know someone had sent you Ghc1,000? I think next time you should report the issue to the police station and also never send or refund money to someone you do not know. Tell the person to report the case to MTN if he feels it is a wrong transaction. **(FGD 1, 9th January 2022).**

3.3.3. Discussions on the implications of the rising impact of cybercrime on the Ghanaian in the international community

Regarding the rising impact of cybercrime on the Ghanaian in the international community, the results of the interviews show that cybercrime leads to reputational damage to being a Ghanaian. The activities of cybercriminals linked to Ghana lead to other Ghanaian living in the international community being unfairly labelled as cybercriminals. This negative externality is the underpinning theory for this study. The negative externalities suffered by Ghanaians in the international community constitute being denied a job because of one's nationality. Another example of the negative externalities as a result of cybercrime is the lack of trust of Ghanaians during business meetings in the international community.

The results show that due to the rising incidence of cybercrime by people of Ghanaian descent, other Ghanaians living abroad are generally not trusted. Research by Jakubowicz, Andrew, et al (2017)., shows that people who come from countries noted for the high incidence of cybercrime find it difficult, compared to others, to find accommodation in Australia, Europe, and America due to irrational fear that they may be cybercriminals themselves.

Also, when Ghanaians are online, they experience digital racism and digital stigmatisation. Digital stigmatisation may include not being offered services because of one's name and perceived country of origin. Digital stigmatisation is what seeps into the reason why companies are insecure about offering their services to African countries. Digital stigmatisation has been on the decrease due to globalisation and due to the objectives of companies to reach global dominance. When these companies still come to Africa, they offer Ghanaians very limited services than what they offer to other nationalities and races in Europe, America, Australia, and Asia.

Moreover, using the space transition theory, the impact of cybercrime on Ghanaians is that it makes them predisposed to give out a fake nationality to escape the negative externalities. This is more common among Nigerians, especially who have to claim to be Ghanaians when abroad in a bid to escape the negative social consequences their country has gotten due to cybercrime. When Ghanaians are shopping online, they sometimes have to rely on the use of IP addresses to bypass certain restrictions on the internet. Even in Ghana, to get a PayPal account, people have to misrepresent themselves as other nationalities to get an account to engage in their activities.

Lastly, as a researcher, I agree with research conducted by Thornicroft et al., (2016) which states that people change their cyber behaviour to escape negative externalities. The results show that some Ghanaians lie about their nationalities when they know it is going to lead to negative outcomes.

3.4. How effective are the laws enacted to deal with cybercrimes in Ghana?

3.4.1. Laws on cybercrimes in Ghana

Ghana has enacted various laws to prevent, manage and respond to cybersecurity incidents considering the country's fast digitization. The laws further protect children, women, and marginalized people on the internet from cyberbullying. These laws further provide the consequences of breaking the laws. The legal practitioners interviewed analysed the cybercrime laws on two dimensions.

3.4.1.1. Cybersecurity Act (2020)

The country's cybersecurity act established the Cybersecurity authority in addition to protecting Ghana's critical information. The legal practitioner was asked about why the law was enacted, and he remarked:

The law was passed by parliament in 2020 and essentially it is to deal with most things relating to cybersecurity. Even though it has its provision, if you look at the beginning of the Act, it talks about the fact that it should be read together with other relevant enactments because cybersecurity is a kind of specialized area which bothers other areas. For example, there is the EOCO Act which criminalizes economic crime. Cybersecurity also deals with money laundering and as such you have to look at the Anti-Money Laundering Act as well. The Cybersecurity Act, therefore, was to help other laws to better deal with cybercrime. **(FGD 1, 9th January 2022).**

The country's Criminal Code of Ghana 1960 (Act 29) makes a clear definition of crime by defining crime as both the act or the action and the intention to commit the act. It further defines it as the breaking of rules or regulations for which a governing authority via a mechanism such as the legal system can ultimately prescribe a conviction (Adinkrah, 2011). The cybersecurity act is therefore a built upon the country's criminal code to better deal with this emerging trend. The legal practitioner added:

The first section of the Cybersecurity Act refers to the different acts that the cybersecurity Act should be read in conjunction with. The Act links almost all the acts which criminalise certain acts which people are now doing in cyberspace. We can talk about the Criminal Offences Act, the Anti-Money Laundering Act, the Anti-Terrorism Act, the Electronic Transaction Act, Electronic Communications Act, the Economic and Organised Crime Act, the Data Protection Act, and the Payment System and Services Act. All these acts provide for specific things which tend to easily deal with money and transfer of money. If you do certain things which do things contrary to any of these acts, you would be charged under those acts in conjunction with the Cybersecurity Act. **(FGD 1, 9th January, 2022).**

3.4.1.2. Effectiveness of cybercrime laws

There are several aims of laws in a country, and one of them is to prevent a negative phenomenon from happening. Cybercrime laws are therefore targeted towards preventing cybercrime from happening. Cybercrime laws are also targeted at providing remedies to instances when cybercrime happens. A good law should be effective; however, the effectiveness of laws are vague concept as it is difficult to measure. An effective law looks at "actual observance" as opposed to validity which looks at the "binding force" of law. In one of the key interviews conducted, the legal consultant indicated that cybercrime laws in Ghana are valid:

Laws in cybercrime are both valid and effective. The laws are valid because they followed the right procedural method before the laws were passed. When I say this, I mean the laws were passed following the laws of Ghana. **(FGD 1, 9th January 2022).**

Research conducted by Djanggih et al., (2018) indicates that laws on cybercrimes are ineffective due to the failure of policy implementation to solve the root causes of cybercrimes. One of the root causes of cybercrime in developing countries is attributed to high graduate unemployment in the country (Ampong, 2020). Hence, to prevent cybercrime and make the laws effective, the government has to fix the causes of cybercrime. It has been argued in some quarters that when the government can fix cybercrime laws to be effective, it needs to incorporate elements of evidence-based policing. In an evidence-based policing approach, police officers and staff create, review and use the best available evidence to inform and challenge policies, practices, and decisions.

For a law to be effective, the law and its enforcers have to identify two groups: technical and non-technical people. Non-technical people employ social engineering technics to defraud their clients while technical people employ a very complex web of coding to steal from people. For non-technical cybercriminals, the citizens believe that it is the job of the Ghana Police Service to fight

this kind of cybercrime (Ennin & Mensah, 2019). For technical cybercriminals, the citizens believe that it is the job of EOCO.

To measure, how effective the law is, the people interviewed were asked to give their own opinion on the effectiveness of the law, this was what it was deduced.

The legal consultant said:

The cybercrime laws in Ghana are very effective because when someone is caught abusing the cybercrime space, the person will be dealt with. What makes people think that the laws are not effective is not because they have not seen people being caught and the laws applied. **(FGD 1, 9th January 2022).**

The police officer, in the focus group discussion, confirmed what the legal practitioner said:

Ghanaians misunderstand the effectiveness of the law. To them, they think the law is not effective. But trust me, when the law catches up with you, it will deal with you. At my unit, I have seen several people being prosecuted for cybercrime. I will have to admit, that cybercrime keeps getting sophisticated day in and day out. **(FGD 1, 9th January 2022).**

During the in-depth interview, the lawyer bemoaned how the vast nature of the cybercrime space makes it hard to catch and tackle people who commit cybercrime. The lack of effective reporting of cybercrime has resulted in the lack of sufficient data/statistics relating to cybercrime. The non-availability of data regarding cybercrime suggests that many of these offenders may not be caught by the legal net making it difficult for cybercrime law enforcement policymakers to draw up long-term plans for dealing with cybercrime.

The student, however, had a contrary view regarding cybercrime. He stated:

For me, I would say the law is not effective. I see a lot of 'fraud' boys on campus. Since the law hasn't caught up with them, I would not say the laws are effective. Their unexplainable wealth is motivating others too to engage in cybercrime. They are making in life and people who I know who have master's degrees can't even find jobs to do. For me, until I find or hear someone being jailed for cybercrime, I do not think that the laws are effective. **(FDG 1, 9th January, 2022).**

The perception of the student regarding cybercrime is due to how he has not seen cybercrime laws at play. This is because people believe cybercriminals benefit from ineffective law enforcement amid growing economic difficulties. The perception is also influenced by the media consumption behaviour of how cybercrimes are reported. When cybercrime cases that have been successfully trailed are reported in the media, the perception of people regarding the ineffectiveness of cybercrime laws would change.

3.4.1.3. Institutions mandated to fight cybercrime.

At the forefront of ensuring the effectiveness of law are the institutions mandated to enforce those laws. Institutions are the built structures that matter most in the social realm: they make up the stuff of social life and in essence, they are what is needed to fight cybercrime (Hodgson, 2006). Institutions are therefore the humanly devised constraints that structure political, economic, and social interaction.

During the focus group discussions and the various in-depth interviews, the respondents were asked whether they knew the institutions that have been mandated to enforce the effectiveness of cybercrime laws. The police officer stated:

In fighting cybercrime, it is eminent for all and sundry to be a part of the fight. Yes, they are key institutions to fight cybercrime that without the general public reporting the crime, most of the

cybercrime will go unreported. The fight against cybercrime, therefore, requires a coordinated effort among all stakeholders such as us (the police officers), government bodies, educational institutions, business organizations, and law enforcement authorities. **(FDG 1, 9th January, 2022).**

The Intelligence Officer at the National Bureau of Investigation was able to list some regulatory institutions that are to make sure that the cybercrime laws are effective. He stated:

In Ghana, the institutions that are mandated to find cybercrimes in Ghana are the National Cyber Security Centre, the Cybercrime Unit of the Criminal Investigations Department (CID) of the Ghana Police Service, and sometimes us (the National Bureau of Investigations). **(IDI 2, 17th April, 2022).**

The participant from Express Pay also added:

Apart from these institutions, players such as those of us in the FinTech space have the responsibility to report cases of cybercrime to the police and other institutions. Sometimes we see our platforms being used to perpetrate cybercrime. Therefore, it is also our responsibility to make sure that we report these cases to these institutions. When people know that suspicious transactions committed on our platform will be sent to regulatory institutions, cybercrimes will reduce. We are part of the institutions that should make sure that laws on cybercrimes are effective. **(IDI 3, 9th April 2022).**

3.4.1.4. Evidence of Cybercrime law enforcement

It was evident through the interviews conducted that evidence of cybercrime law enforcement can both reduce the incidence of cybercrime in Ghana and equally improve the image of the Ghanaian in the international community. The justice and security system plays an integral role in the

enforcement of cybercrime. Cybercrime enforcement is a coordinated effort between the citizenry, various security agencies, and also the judiciary. Evidence of law enforcement starts from the general public reporting cybercriminals to the security agencies. It is a well-known fact that people know the criminals in society. People can have faith in the cybercrime laws when there is much media coverage of large numbers of cybercriminals being reported and jailed.

Enforcement of cybercrime law, therefore, starts with people reporting the activities of cybercrimes to the right authorities. Once it is reported and the issue is not taken up, it can be deduced that the law is not effective. Various newspaper report suggests that the incidence of cybercrime report seems to be on the increase.

When asked how the normal Ghanaian can help in reporting cybercriminals to the right authorities for prosecution.

The policeman who was part of the first focus group discussions stated:

"People know the criminals in society. They live with us. If people want to get rid of cybercrimes and cybercriminals, they have to report them to the police. People live in the same community as these thieves. Sometimes you see someone who does not work but drives an expensive car. I don't want to be stereotypical, but do you ask yourself, what work he or she is doing? For all the successful cybercrime cases that have been tried, it started with the general public reporting the cases to us. At my office, I can tell you that we see people reporting perpetrators of cybercrimes daily. Just last week, someone reported another person who committed mobile money fraud, as we speak currently the case is still in court. I also know of a case where a businessman reported a cybercriminal to our station. There are a lot of cybercrime cases that are currently being

prosecuted. There are also a lot more that have been tried and the cyber criminals sent to jail." **(FDG 1, 9th January, 2022).**

The legal consultant reiterated the point that was raised by the police officer. He stated how he has handled cybercrime cases in the past. He made it known that there is evidence of cybercrime reports but because the ordinary citizens are not "*close to the issue"* they are oblivious. He said:

"I am handling a case on cybercrime, and I can tell you that cybercrime laws are being enforced and people are going to jail as a result of cybercriminal activities. As I said earlier, until you are caught in the web of the law, you may think that the laws are ineffective or there is no evidence of cybercrime reporting in Ghana. **(FDG 1, 9th January, 2022).**

The student disagreed with the police by giving a contrary view.

"*Even on campus, there are guys who are suspected cybercriminals, but we are afraid to report them because we have no proof. They also have money so if you report them, they will target you and harm you in a kind of negative way. So, in my view, I am yet to see evidence of cybercrime laws being enforced. When you have people, who can buy their way out, you cannot say you have seen evidence of cybercrimes being prosecuted."* **(FDG 1, 9th January, 2022).**

3.4.2. Discussions on the effectiveness of laws of cybercrime in Ghana

The effectiveness of law deals with how laws are enforced and their consequences because of their enforcement. The cybercrime law was implemented to deter acts of cybercrime. Its effectiveness can therefore be measured by how it has been able to deter acts of cybercrime and how it has been able to lead to a reduction in the prevalence of the menace.

Cybercrime becomes difficult to curb due to its transnational nature making it very difficult to deal with (Nguyen, 2017). At times cybercrime is committed using infrastructure by foreign-owned

companies and these foreign-owned companies are not willing to cooperate with the local police institution because they want to protect their image by not reporting these crimes. When these crimes are reported by this international cooperation, it may send a signal to users of their services that their platforms are not safe. When these foreign institutions are not willing to work with local enforcers, it becomes difficult to tackle cybercrime.

Using the yardstick of cybercrime laws not being able to deter cybercriminals, we can defer that the cybercrime laws in Ghana have been ineffective in dealing with acts of cybercrime. Reported cases of cybercrime keep increasing year on year and cybercrime keeps getting sophisticated. The legal consultant held the opinion that the laws are effective because he has seen them being tested in his field of work. However, using the theory of media consumption behaviour, it is hard to agree with his position. In the media, there are increasing reported cases of Ghanaians both living in Ghana and living abroad engaged in certain cybercriminal acts ranging from romance scams to phishing among other types. One can argue that there has been an increase in reported cases since the media is now shedding light on this menace. Even if this was the case, Ghanaians still perceive cybercrime as rising despite the passage of all these laws stated in the study.

Some Ghanaians are of the view that law enforcers are complicit in helping cybercriminals escape the legal justice system. Again, due to the slow nature of the legal proceeding in Ghana, people generally lose interest in cybercrime cases, and often they do not hear about the outcomes of such cases. This makes them perceive the law as ineffective. The local police force is integral to making the cybercrime laws effective and they are complicit as stated. The police know their community because they were part of it. In Ghana, there is a general distrust of the Ghanaian police, and as such cybercrime cases are less likely to be reported to them (Boateng et al., 2019).

The law is therefore not very effective as it does not motivate people to report acts of cybercrime activities to the police for onward prosecution because there is a general belief that even if they report the criminals, it will be inconsequential and once the case is over, they are going to be attacked by cybercrime mobs and gangs.

3.5. In what way can the laws that deal with cybercrimes be strengthened to reduce the incidence of cybercrime?

3.5.1. Recommendations to reduce the incidence of cybercrimes in Ghana.

Cybercrime laws regardless of how well written and effective they are, need frequent improvement to tackle new and emerging trends in cybercrime. The activities of cyber criminals in Ghana have negatively impacted the image of other Ghanaians in international communication. The current laws are meant to tackle the menace of cybercrime in Ghana, the laws have also set up institutions to enforce these laws among other reasons. Despite these frameworks, Ghana is fast losing its prestige image in the international community space. Reports from the National Cybersecurity Advisor, Dr. Antwi-Bosiako indicate that cybercrime is increasing geometrically and if it is not reduced, it will impact greatly the image of the Ghanaians in Ghana and abroad.

Through the in-depth interviews, it is evident that Ghanaians are suffering from the activities of cybercrime. These include access to certain services on the internet, how the Ghanaian is perceived during international conferences, and also how Ghanaians are received in jobs and other international circles. The personnel from Ghana Migration Service indicated:

"Through the activities of cybercriminals, Ghanaians are fast losing their respect in international circles. In the past, when Ghana is mentioned, people happily welcome you. When you mention Ghana, they immediately ask you about Kwame Nkrumah, Asamoah Gyan, and Kofi Annan. These men made Ghanaians respected. Cybercriminals are making Ghanaians lose their respect and

value in the international community. Now if you say you are from Ghana, people look at you as if you are part of those who commit cybercrime. To improve the image of Ghanaians in the international community is to reduce the incidence of cybercrime." **(IDI 1, 10th April, 2022).**

Against this backdrop, the participants in the focus group discussion and the in-depth interviews were asked to give recommendations to reduce the incidence of cybercrime. Some of the recommendations, respondents in the focus group gave were similar. The student said:

"The first thing that can be done is to change how the activities of cybercriminals can be reported. It is alleged that cybercriminals have linked in the security. So, if it is possible to report the activities of cyber criminals online without going to the Police station. This will encourage more people to report these criminals as it will ensure confidentiality. These fraud boys are dangerous and well connected so if you report them to the police and they get to hear of it, they may negatively harm you." **(FDG 1, 9th January, 2022).**

The police officer added to the discussion:

"The Police is your friend, if we want to solve cybercrime, we need to report whoever we think is engaged in cybercrime. Until the police get wind of it, we will not be able to know who is engaged in cybercrime. The police do surveillance once in a while, but the citizens can best help us." **(FDG 1, 9th January, 2022).**

As a victim of cybercrime, he suggested:

"I think the security services must tell us what to do when we fall victim to cybercrime. You know cybercrime differs from the crime that we know. So, if not for today, I never knew if I had reported it and through the help of the telcos, they could have gotten the culprit arrested. I believe if all this information is in the public domain, more cases will be reported. Sometimes people do not know

what to do when they are victims of cybercrimes….in my case, I kept blaming the wrong people rather than reporting the culprits to the right authorities." **(FDG 1, 9th January, 2022).**

3.5.2. Role of law enforcement in the prevention of cybercrime

Law enforcement is important in making sure that negative behaviour is changed. Law enforcement in the prevention of cybercrime makes people feel confident in safely conducting their businesses. Cybercrime laws, when enforced, will reduce the incidence of cybercrime. It is believed that enforcement of the law can act as a deterrent to cyber misbehaviour and criminal activities (Travis & Coon, 2005). Despite the great importance of law enforcement, various governments have paid little attention to enforcement, hence why the incidence of cybercrime has been on the ascendency. One of the ways to reduce the incidence of cybercrime is to fund the agencies that battle cybercrime. However, historically budgetary allocations for security services have been consistently low (Jachmann, 2008). There are hence regulatory challenges faced by the Police and legal and financial institutions in addressing cybercrime. (Boateng et al., 2011). With this constraint in mind, the success of law enforcement agencies in reducing cybercrime lies on the citizenry in reporting suspicious behaviour to the authorities Internet service providers operating in the country should also be mandated to report suspicious traffic going through their networks. Many legal theorists posit that the effectiveness of the law is based on how we internalize them, obeying even when not compelled to do so.

Concerning the role of the law in preventing cybercrime, the police officer who was part of the first focus group discussion said:

The cybercrime laws can lead to a reduction in cybercrime. The laws are largely effective and if implemented will solve their purpose. But as I always say, if the citizens will help us, it will be better. The laws of cybercrime only work when want to collaborate with us. If citizens don't help

us to arrest the criminals, then there is nothing, we can do about law enforcement. **(FDG 1, 9th January, 2022).**

The legal consultant reiterated:

"Generally, there is a misconception about the effectiveness of the law in Ghana. Laws are effective, they might be slow, but it is very effective. Just like all other laws, I know; I believe strongly that the cybercrime laws in Ghana can help reduce the cases of cybercrime in Ghana. I have every faith in its abilities." **(FDG 1, 9th January, 2022).**

3.5.3. Discussions on what way can the laws that deal with cybercrimes be strengthened to reduce the incidence of cybercrime.

There are so numerous reports and research on Ghana's cybercrime situation and how it is contributing to citizens of other countries responding negatively to well-meaning Ghanaians. These reports indicate that cybercrime is a cancer to the image of the country as well as its citizens. A reduction in the incidence of cybercrime has a direct correlation with improving the image of Ghanaians in the international community. There is distrust among people who come from countries where the incidence of cybercrime is high. The participants were asked if a reduction in cybercrime will improve the image of Ghanaians in the international community.

The participant from the e-Crime Bureau Ghana stated:

"If cybercrime is reduced, it will improve Ghana's image. In our line of work, we see how companies want to invest in Ghana, but they are skeptical due to cybercrime. The love of Ghana is out there but these cybercriminals are enabling distrust in the Ghanaians. You can see clearly that when cybercrime started to grow, the respect people have for us is going down. If the

government should fund these agencies to tackle cybercrime, the image of the Ghanaians in the international community will improve." **(IDI 4, 9th April, 2022).**

A major way of ensuring the effectiveness of cybercrime laws is their enforcement. The laws on cybercrime must be enforced swiftly to serve as a deterrent to others. This can be done by setting up specialised fast-track courts to deal with people who are standing trial for cybercrime-related infractions. A fast and effective cybercrime trial will serve as a deterrent to others. Reports indicate that when court proceedings are long and winding, people generally lose interest in the case. An expedited cybercrime trial will deter people from committing cybercrime and hence lead to a reduction in the prevalence of cybercrime.

Similarly, the government can set up an online portal where people can easily report the activities of cybercriminals without having to go to the police station. This faceless portal will encourage more Ghanaians to report people who are perceived to be engaging in cybercrime. One of the major obstacles to cybercrime is the belief that when a cybercriminal is reported their gang will harm the reporter. An online reporting system will solve this issue by providing anonymity to the reported and also tell the international community that the country is interested in fixing the growing menace of cybercrime in the country.

In conclusion, Ghana has adequate laws that can deal with cybercrime. What is lacking is the will to enforce the law to the latter. Our lack of urgency can be attributed to institutional challenges and the overburden of our judiciary institution.

3.8. Conclusion

This chapter has achieved the task of examining the menace of cybercrime in Ghana and its implication for Ghanaians in the international community. The research through the focus group discussion and also the in-depth interviews discussions helped to build a new perspective of cybercrime according to the Ghanaians, and how these externalities affect the Ghanaians in the international community. Globally, cybercrime is becoming a worrying phenomenon and it also impacts the image of citizens making them unable to access certain services due to how that country is perceived to have a high incidence of cybercrime in that country.

Reference

Akomea-Frimpong, I., Andoh, C. & Akomea-Frempong, A. (2019): Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control. Vol 22, No 2.

Boateng, F. D., Makin, D. A., Abess, G., & Wu, G. (2019). Speaking out: Officers speaking about police misconduct in Ghana. The police journal, 92(2), 121-135.

Hartford Court and: Arrest Warrant Details Charges Against East Hartford Businessman. https://www.courant.com/breaking-news/hc-br-manchester-cyber-hack-300k-retirement-funds-warrant-20180831-story.html Accessed on 20th June 2022.

Djannggih, H., Thalib, H., Baharuddin, H., Qamar N. & Ahmar, A.S. (2018): The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia. Journal of Physics: *Conference Series, Volume 1028, 2nd International Conference on Statistics, Mathematics, Teaching, and Research 2017 9–10.*

Ennin, D. & Mensah, R.O. (2019): Cybercrime in Ghana and the reaction of the law. *Journal of Law, Policy, and Globalization. Vol 84. DOI: 10.7176/JLPG*

Folashade B.O & Abimbola K.A (2013): The Nature, Causes, and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research. Vol. 3 No. 9; September 201

Ghana Chamber of Telecommunications. https://www.telecomschamber.com/news-media/industry-news/ghana-records-over-11-000-cybercrime-cases-since-2019 Retrieved on 8th January 2022.

Halana, V. & Smith, N. (2019): School-going teenage mothers in an under-resourced community: lived experiences and perceptions of support. Journal of Youth Studies. V*olume 22, 2019 - Issue 9*

Thornicroft, G., Mehta, N., Clement, S., Evans-Lacko, S., Doherty, M., Rose, D., ... & Henderson, C. (2016). Evidence for effective interventions to reduce mental-health-related stigma and discrimination. The Lancet, 387(10023), 1123-1132.

Hodgson, G.M. (2006): What Are Institutions? *Journal of Economic Issues. Volume 40. Pages 1-25. https://doi.org/10.1080/00213624.2006.11506879*

Jackmann, H. (2008): Monitoring law-enforcement performance in nine protected areas in Ghana. *Biological Conservation. Volume 141, Issue 1, Pages 89-99. https://doi.org/10.1016/j.biocon.2007.09.012*

Jakubowicz, A., Dunn, K., Mason, G., Paradies, Y., Bliuc, A. M., Bahfen, N., ... & Connelly, K. (2017). Cyber racism and community resilience. Cham: Palgrave Macmillan.

Jackson, T.C.B., Ene, J. & Ene, R.W. (2016): CYBERCRIME AND THE CHALLENGES OF SOCIO-ECONOMIC DEVELOPMENT IN NIGERIA. JORIND 14(2)]. ISSN 1596-8303. www.transcampus.org/journal; www.ajol.info/journals/jorind

Khan M.T., Huo X., Li Z. Kanich C. (2015): Every second counts: Quantifying the negative externalities of cybercrime via typosquatting. 2015 IEEE Symposium on Security and Privacy 135 – 150.

McClean, D. Zhang, T. & Zhao, M. (2012): Why Does the Law Matter? Investor Protection and Its Effects on Investment, Finance, and Growth. https://doi.org/10.1111/j.1540-6261.2011.01713.x

Nguyen, H.V. (2019): Cybercrime in Vietnam: A critical analysis of its regulatory framework.

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017, June). UAE cybercrime law and cybercrimes—An analysis. In 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1-6). IEEE.

Saroha, R. (2014): Profiling a Cyber Criminal. ***International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 253-258***

Travis, L.F. & Coon, J.K. (2005): The Role of Law Enforcement in Public School Safety: A National Survey.

US Department of Justice (2021): https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting Retrieved on 19th June 2022.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. Psychiatry, Psychology and Law, 24(3), 323-338.

Ward S. & Vedel, T. (2006): Introduction: The potential of the internet revisited. Parliamentary affairs 59(2), 210 – 225.

CHAPTER FOUR

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATION

4.0. Introduction

This chapter presents a summary of the research findings based on the objectives set in Chapter 1. This chapter provides inferences, conclusions, and recommendations from both primary and secondary data.

4.1. Summary of Findings

This research was to examine the implication of cybercrime on the image of Ghanaians in the international community. The study was premised on the context that cybercrime could lead to negative externalities on innocent Ghanaians in the international community. The pre-emptive conclusion was based on the literature which suggests that the Nigerians in the international community are suffering negative consequences due to the activities of cybercriminals perceived to be Nigerian. The Nigerian image has been damaged by a form of cybercrime called "advance-fee scam" known as "The Nigerian Prince" or "419." The research employed a qualitative study to explore the set objectives.

4.1.1. To examine the implication of the rising incidence of cybercrime on the image of the Ghanaian in the international community.

- The focus group discussions and the expert interviews revealed that cybercrime has a scathing impact on Ghanaians in the international community. The focus group discussion among people in the international diaspora indicated that although Ghanaians when compared to other African counterparts like Nigerians receive less unfavourable perception due to the high incidence of cybercrime, they still face negative lived experiences in which

they have no hand in. Ghanaians are seen as hardworking and friendlier in the international community, but cybercrime is affecting this pristine image that the country once had. These negative externalities reflect in how many services the Ghanaians both in Ghana and abroad on the internet. Ghanaians, for example, in the international community cannot freely send money to relatives in Ghana which falls above a certain threshold. This is a result of perceived cybercrime and perceived risk. Equally, credit and debit cards such as Visa and Mastercard from Ghana are restricted in the international community. Certain banking apps cannot be used in Ghana due to how negatively Ghanaians are perceived due to cybercrime.

- Payment services such as PayPal and Zelle among others are equally restricted in Ghana due to the perceived risk associated with cybercrime in Ghana. According to PayPal, Ghanaians were using their services as a conduit for internet fraud, hence the decision to blacklist Ghana. The study further discovered that some Ghanaians have reported being victimized due to the high incidence of cybercrime Ghanaians. Aside from this, Ghanaians have gathered an unnecessary rumour of using "fetish" to voodoo innocent people into committing cybercrime.
- People in the outside world think that Ghanaians employ "spiritual" elements in other to dupe people for their hard-earned money. This negative view is held largely by other Africans in sub-Saharan Africa and other Africans in the diaspora. Being called or known as fetish or voodoo carries a negative image among their sub-Saharan African peers.

4.1.2. To access the effectiveness of the current laws of cybercrimes in Ghana

- The study provided evidence through the expert interviewed that although the laws are readily available it has been ineffective to deal with issues of cybercrime. The reason for

the ineffectiveness can be associated with institutional challenges and the unwillingness of Ghanaians to report friends, family, and other relatives involved in the menace.

- Another reason is that there is a low education on cybercrime in general and the various legislations that are available to combat it. Enacting a law to combat a problem is not enough. The institutions mandated to curb cybercrime should educate people on ways in which they can report people engaged in cybercrime. Citizens should know which institution they have to first contact when they have reasonable suspicion on friends and relatives who are committing cybercrime.

4.1.3. To examine ways through which the laws that deal with cybercrime be strengthened to reduce the incidence of cybercrime.

- There should be a new reporting system to cybercrime where people can report people engaged in cybercrime by filling an online system. This online system will encourage citizens to report those they suspect are engaged in cybercrime. There is the belief that the security service is complicit in cybercrime and by reporting such people, your security may be at stake. An online system will remove this perceived risk.
- There should be a fast-track court which is set up to prosecute cybercrime. This court should expedite on cybercrime cases. When cybercrime cases are fast tracked, it will serve as a deterrent to those engaged in the act.
- There should be a campaign on educating people on the law and what to do to seek redress when they are subject to cybercrime. The first point of call should be an education to sensitize Ghanaians on what really is cybercrime. The study revealed that Ghanaians perceive cybercrime as crimes that involve the use of the internet to steal money.

- Cybercrime is a broad concept but aside from the experts, the ordinary Ghanaian see cybercrime as any crime involving monetary theft on the internet. The perception of cybercrime as the use of the internet to steal money is because the advanced-fee scam is the most popular scam that Ghanaians know about. The Ghanaian cybercriminal is rarely interested in stealing information. Despite the sophistication of cybercrime in Ghana, the main focus is using the internet to steal money from people; where the stealing of money is not possible, they use credit calls of people to buy goods and services online and they later sell these things in Ghana.

4.2. Conclusions

In the league table of nations, image is everything. Many countries both in the East and West, invest copious resources in ensuring that they have an admirable image on the international scene. A country's worth does not consist only of its mineral, human and financial resources. It also consists of the perceived image, and the esteem with which it is regarding by the international community.

Thus, it is imperative that the image of nations states be safeguarded. While the good image of a country may take years to build, it only takes the publicised activities of a few unscrupulous citizens to destroy that image. The image of a country takes a while to build but it can take a few unscrupulous people for it to be destroyed. When the image of a country is soiled, it negatively impacts its citizens everywhere, as they are representations and symbols of that particular country. A classic example is Nigeria: Its citizens are regarding with suspicion and mistrust the world over, due to the notorious activities of Nigerians "419" online scammers over of the years. As a results, Nigeria and by extensions Nigerians, have become synonymous with online fraud. The fairness or unfairness of this global judgement of Nigerians, is not the focus of this study. Instead, this

investigation seeks to measure the impact of cybercrime on nation states, with particular reference to Ghana. Despite the growing incidence of cybercrime in Ghana via internet fraud or "sakawa", the image of the Ghanaian is not irreparably damaged. The government must therefore devise innovative ways to enforce existing the laws in order to reduce this menace.

The study concludes that the activities of cybercriminals present negative externalities to innocent Ghanaians living both home and abroad. The negative externalities include the non-availability of certain business and financial opportunities to them, as well as their chances of being hired in jobs requiring a high level of trust. Even online dating sites tend to bar internet traffic from Ghana and Nigeria. By and large, this study examines the negative effects on Ghanaians home and abroad, as a result of the activities of cybercriminals. It also accesses the behaviour of foreigners citizens towards Ghanaians in general, as a result of media reportage of cybercrime in Ghana.

The study further concludes that the laws regarding cybercrime in the country are not effective in dealing with the challenges of cybercrime. The ineffectiveness comes from the opinion that cybercriminals are not arrested and prosecuted by the regulatory authorities. Although there are several documented instances where people have been trialled and jailed, the numbers are minimal to change people's opinion on the effectiveness of the law.

Moreover, the study concludes that ways in which the ways can be made effective are to educate people on what to do to report people they suspect engaging in cybercrime. Mass education can be in the form of social media campaigns, radio, and TV campaigns on what to do when you are a victim of cybercrime like how it was done by MTN to combat Mobile Money fraud.

4.3. Recommendations

The research proposes recommendations grounded on the findings and inputs from respondents interviewed.

4.3.1. Reduction of unemployment

Recognizing that a significant proportion of cybercriminals turn to illicit activities due to limited employment opportunities, it is imperative for the government to adopt a proactive approach to mitigate unemployment in the country. Reducing unemployment is not only a key societal goal but also an effective means to curtail cybercrime. The strong correlation between low cybercrime rates and higher employment levels has been consistently established through extensive research. To address this issue comprehensively, the government should particularly target graduate unemployment, a segment of the population facing unique challenges. While the introduction of initiatives like "NABCO" is commendable, a more multifaceted approach is necessary. Furthermore, considering the adverse impact of the COVID-19 pandemic on unemployment, the government should explore options such as providing tax exemptions and stimulus packages to companies. These measures will incentivize businesses to create more job opportunities, thus reducing unemployment and, concurrently, diminishing the incidence of cybercrime. By pursuing these strategies, the government can foster both economic growth and a more secure digital landscape for its citizens.

4.3.2. Educating people on the cybercrime laws

It is crucial to instil in Ghanaians the importance of promptly reporting cybercrimes to the police as their first course of action. Building on the success of MTN's fraud detection education campaign, which has substantially reduced Mobile Money (MoMo) fraud, the government should expand such initiatives to address other forms of cybercriminal activities. Furthermore, a comprehensive education program should be implemented to familiarize Ghanaians with cybercrime laws, empowering them with knowledge about their rights in the digital realm. When citizens are well-informed about their cyberspace rights, they are far less vulnerable to online fraud and cybercrime.

4.3.3. Expediated justice system

Ghana's justice system has been consistently criticized for its lack of efficiency and timeliness. When it comes to addressing cybercrimes, a rapid and decisive response is paramount. Timely prosecution not only acts as a strong deterrent but also ensures the protection of individuals' hard-earned assets from cybercriminals. To effectively tackle this challenge, the establishment of specialized courts exclusively dedicated to adjudicating cybercrimes emerges as a proactive and strategic solution. Such specialized courts would not only expedite the legal process but also demonstrate the nation's commitment to combating cyber threats.

4.3.4. Implementation of existing legislation on cybercrime

For a more effective response to cybercrime, the Ghanaian government should prioritize and actively champion the comprehensive enforcement of its existing legal framework and policies dedicated to combating cyber threats. Collaborating closely with critical stakeholders, including internet cafes, internet service providers, and telecommunication networks, is imperative to ensure strict adherence to cybercrime laws. This collaborative approach will not only fortify the efficacy of the legal apparatus but also cultivate a robust cybersecurity ecosystem, safeguarding the digital landscape for all Ghanaian citizens.

4.3.5. Encouraging people to report acts of cybercrimes.

To combat cybercrime effectively, it is imperative to encourage individuals to report any acquaintances, including friends, family, and relatives, who are involved in such activities. This initiative should encompass community leaders, including religious figures, who can play a pivotal role in promoting awareness and reporting. Religious leaders must actively engage in condemning cybercrime and its glamorization, drawing from the Holy Scriptures to reinforce the message that such activities run counter to divine principles. This concerted effort will help create a society that is more vigilant and morally resistant to the allure of cybercrime.

4.3.6. Enactment of a cybercrime policy

The government must enact a cybercrime policy to deal with the growing menace of cybercrime. The cybercrime policy aims to give remedy to the cybercrime menace not provided for in the existing cybercrime laws. The policy would give direction to the government can follow to properly tackle this growing menace.

4.3.7. Encouraging research into cybercrime to identify new trends.

The Government of Ghana should actively promote and facilitate collaborative research, forums, and workshops dedicated to addressing cybercrime. These initiatives should bring together a diverse array of stakeholders, including law enforcement, academia, businesses, civil society, and end users, both domestically and among Ghanaian communities abroad. This collective effort will be instrumental in identifying emerging cybercrime trends within the nation and beyond, fostering a comprehensive approach to combatting this multifaceted issue.

BIBLIOGRAPHY

A. Books

Afanu E.K. & Mamattah R.S., (2013): Mobile Money Security: A holistic approach.

Chen, R., Niu, W., Zhang, X., Zhuo, Z., & Lv, F. (2017). An effective conversation-based botnet detection method. Mathematical Problems in Engineering, 2017.

Haris, A., & Zagaris, B. (2019). Cybercrime. IELR, 35, 455.

Pérez Dasilva, J. Á., Meso Ayerdi, K., & Mendiguren Galdospin, T. (2021). Deepfakes on Twitter: which actors control their spread?

Travis, L.F. & Coon, J.K. (2005): The Role of Law Enforcement in Public School Safety: A National Survey.

B. Journal Articles

Abayomi A.A., 2020: Applying Space Transition Theory to Cyber Crime; A Theoretical Analysis of Revenge Pornography in the 21st Century. *International Journal of Innovative Science and Research Technology*

Abdul-Hamid I.K., Shaikh A.A., & Boateng H. & Hinson R.E., (2019): Customers' Perceived Risk and Trust in Using Mobile Money Services – an Empirical Study of Ghana. *International Journal of E-Business Research (IJEBR) 15 (1) 1-19*

Abdul-Rasheed S.L., Lateef I., Yinusa M.A. & Abdullateef R., 2016: Cybercrime and Nigeria's external image: *A critical assessment. Journal of Pan African Studies 9(6), 119-133.*

Akgul M. & Kirlidog M., 2015: Internet censorship in Turkey. *Internet Policy Review 4(2) 1-22*

Akomea-Frimpong I., Andoh C., Akomea-Frimpong A. & Dwomoh-Okudzeto Y., (2019): Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control 22(2):303-317. DOI:10.1108/JMLC-03-2018-0023

Akomea-Frimpong, I., Andoh, C. & Akomea-Frempong, A. (2019): Control of fraud on mobile money services in Ghana: an exploratory study. Journal of Money Laundering Control. Vol 22, No 2.

Al-Asli, M., & Ghaleb, T. A. (2019, April). Review of signature-based techniques in antivirus products. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE.

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.

Apandi, S. H., Sallim, J., & Sidek, R. M. (2020, February). Types of anti-phishing solutions for phishing attack. In IOP Conference Series: Materials Science and Engineering (Vol. 769, No. 1, p. 012072). IOP Publishing.

AYUB, A. O., & RASAKI, A. J. (2021). Modus Operandi and Socio-Demographics of Cybercrimes' Perpetrators and Victims in Nigeria. Gusau Journal of Sociology, 128.

Barfi, K. A., Nyagorme, P., & Yeboah, N. (2018). *"The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region". Library Philosophy and Practice (e-journal). 1715.*

Baykara, M., & Gürel, Z. Z. (2018, March). Detection of phishing attacks. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5). IEEE.

Boateng R. & Barnor J.N.B., (2020): Unveiling cybercrime in a developing country. *Encyclopedia of Criminal Activities and the Deep Web, 66-92*

Cohen, L., & Felson, M. (1979). *Social Change and Crime Rate Trends. A Routine Theory Approach. America Sociological Review, 44, 588-608.*

Dadson, M. (2019): Examining the perceived vulnerability and experiences of inbound tourists on cybercrime in Ghana. URI: http://hdl.handle.net/123456789/4820

Danquah P. & Longe O.B., (2011): Cyber deception and theft: An ethnographic study on cyber criminality from a Ghanaian perspective. *Journal of Information Technology Impact 11 (2) 169 - 182*

Djannggih, H., Thalib, H., Baharuddin, H., Qamar N. & Ahmar, A.S. (2018): The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia. Journal of Physics: *Conference Series, Volume 1028, 2nd International Conference on Statistics, Mathematics, Teaching, and Research 2017 9–10.*

Dull L.J., 2008: Friendly Africans, Deceptive White Men: Ghanaian Narratives of the Nation.

Eboibi F.E., 2020: Concern of Cyber criminality in South Africa, Ghana, Ethiopia, and Nigeria: rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin, 1-32*

Ennin D., Cybercrime in Ghana: A study of offenders, victims and the law. http://197.255.68.203/handle/123456789/8908

Ennin, D. & Mensah, R.O. (2019): Cybercrime in Ghana and the reaction of the law. *Journal of Law, Policy, and Globalization. Vol 84. DOI: 10.7176/JLPG*

Fahlevi, M., Saparudin, M., Maemunah, S., Irma, D., & Ekhsan, M. (2019). Cybercrime Business Digital in Indonesia. In E3S Web of Conferences (Vol. 125, p. 21001). EDP Sciences.

Folashade B.O & Abimbola K.A (2013): The Nature, Causes, and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research. Vol. 3 No. 9; September 201

Gandon, F. (2017). For everything: Tim Berners-Lee, winner of the 2016 Turing award for having invented… the Web. *1024: Bulletin de la Société Informatique de France*, (11), 21.

Gencer M., (2011): The mobile money movement: Catalyst to jump-start emerging markets. Innovations: *Technology, Governance, Globalization 6(1): 101 - 117*

Halana, V. & Smith, N. (2019): School-going teenage mothers in an under-resourced community: lived experiences and perceptions of support. Journal of Youth Studies. V*olume 22, 2019 - Issue 9*

Hartford Court and: Arrest Warrant Details Charges Against East Hartford Businessman. https://www.courant.com/breaking-news/hc-br-manchester-cyber-hack-300k-retirement-funds-warrant-20180831-story.html Accessed on 20th June 2022.

Hodgson, G.M. (2006): What Are Institutions? *Journal of Economic Issues. Volume 40. Pages 1-25. https://doi.org/10.1080/00213624.2006.11506879*

Holt, T. J., Bossler, A. M., & Seigfried-Spellar., K. C. (2018). *Cybercrime and Digital Forensics: An Introduction. 2nd ed. New York: Routledge.*

Holt, Thomas J., & Bossler, A. M. (2016). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

https://doi.org/10.1111/j.1754-9469.2004.tb00055.x

Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., ... & McCoy, D. (2018, May). Tracking ransomware end-to-end. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 618-631). IEEE.

Izuakor, C. F. Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context.

Jackmann, H. (2008): Monitoring law-enforcement performance in nine protected areas in Ghana. *Biological Conservation. Volume 141, Issue 1, Pages 89-99. https://doi.org/10.1016/j.biocon.2007.09.012*

Jackson, T.C.B., Ene, J. & Ene, R.W. (2016): CYBERCRIME AND THE CHALLENGES OF SOCIO-ECONOMIC DEVELOPMENT IN NIGERIA. JORIND 14(2)]. ISSN 1596-8303. www.transcampus.org/journal; www.ajol.info/journals/jorind

Kasraie N. & Kasraie E., 2010: Economies of e-learning in the 21st Century. *Contemporary Issues in Education Research (CIER) 3(10), 57-62*

Khan M.T., Huo X., Li Z. Kanich C. (2015): Every second counts: Quantifying the negative externalities of cybercrime via typosquatting. 2015 IEEE Symposium on Security and Privacy 135 – 150.

Kigerl A., 2012: Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review 30 (4), 470-486*

Kigerll A., 2012: Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review 30 (4), 470 - 486.

Kopp C., Layton R., Sillitoe J. & Gondal I., (2015): The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles. *International Journal of Cyber Criminology 9(2)*

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198x.2019.1603527

Lennings C.J., Amon K.L., Brummert H. & Lennings N.J., (2010): Grooming for terror: The internet and young people. *Psychiatry, Psychology and Law 17 (3), 424 – 437.*

Leukfeldt E.R. & Yar M., 2016: Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior 37 (3), 263 - 280.

Martin N.& Rice J.,2011: Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security 30(8)803-814*

Matthyssens P., Kirca A.H., Pace S., Moen O., Madsen T.K. & Aspelund A., (2008): The importance of the internet in international business-to-business markets. *International Marketing Review.*

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017, April). Flipping 419 cybercrime scams: Targeting the weak and the vulnerable. In Proceedings of the 26th International Conference on World Wide Web Companion (pp. 1301-1310).

McClean, D. Zhang, T. & Zhao, M. (2012): Why Does the Law Matter? Investor Protection and Its Effects on Investment, Finance, and Growth. https://doi.org/10.1111/j.1540-6261.2011.01713.x

Miroo F., 2014: Routine Activity Theory. The Encylopedia of theoretical criminology, 1-7.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. Computers & Security, 59, 186-209.

Mowery D.C. & Simcoe T., 2002: Is the Internet a US invention? - economic and technological history of computer networking. Research Policy 31 (8 - 9), 1369 - 1387..

Mukeredzi T., (2017): Uproar over Internet shutdowns: Governments cite incitements to violence, exam cheating, and hate speech. *Journal of Pan African Studies 10 (10), 7*

Newman R.C., (2006): Cybercrimes, identity theft, and fraud: practicing safe internet-network security threats and vulnerabilities. *Proceedings of the 3rd annual conference on information security curriculum development, 68-78*

Nyirenda-Jere T., & Biru T., (2015): Internet development and internet governance in Africa. *ISOC Report 17-53*

Olubukola, S.A., (2017): Cybercrime and Poverty in Nigeria. *Canadian Social Science. Volume 13. No 4*

Oni, S., Berepubo, K. A., Oni, A. A., & Joshua, S. (2019, April). E-government and the Challenge of Cybercrime in Nigeria. In *2019 Sixth International Conference on EDemocracy & EGovernment (ICEDEG)* (pp. 137-142). IEEE.

Orji U.J., 2019: An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. Computer Law & Security Reviews= 35(6), 105330

Paoli, L., Visschers, J. & Verstraete, C., (2018): The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. Crime, Law and Social Change 70(4), 397-420.

Pratt T.C., Holtfreter K. & Reisig M.D., 2010: Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency 47 (3), 267-296.

Rajan, A. V., Ravikumar, R., & Al Shaer, M. (2017, June). UAE cybercrime law and cybercrimes—An analysis. In 2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security) (pp. 1-6). IEEE.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation, and prevention. International Management Review, 13(1), 10.

Riley M & Robertson J., 2017: Russian cyber hacks on US electoral system far wider than previously known. Bloomberg, June 13, 2017.

Rufai, M.O. (2018): Nigerian newspapers' coverage of crime and the gratification of readers' safety information need 2010-2014

Saroha, R. (2014): Profiling a Cyber Criminal. ***International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 3 (2014), pp. 253-258***

Schiller, Craig A.; Binkley, Jim; Harley, David; Evron, Gadi; Bradley, Tony; Willems, Carsten; Cross, Michael (1 January 2007). Botnets. Burlington, Virginia: Syngress. pp. 29–75. doi:10.1016/B978-159749135-8/50004-4. ISBN 9781597491358.

Schonlau, M., Guenther, N., & Sucholutsky, I. (2017). Text mining with n-gram variables. The Stata Journal, 17(4), 866-881.

serianu. (2017b). *Demystifying Africa's Cyber Security Poverty Line Botswana*. https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Suanpang, P., Pothipasa, P., & Netwrong, T. (2021). Policies and Platforms for Fake News Filtering on Cybercrime in Smart City Using Artificial Intelligence and Blockchain Technology. International Journal of Cyber Criminology, 15(1), 143-157.

Tade, O. (2013): A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *HUMAN AFFAIRS 23, 689–705.* DOI: 10.2478/s13374-013-0158-9

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, *33*(5), 890–911. https://doi.org/10.1080/07418825.2014.994658

Thornton A.L., (2001): Does the internet create democracy. African Journalism Studies 22(2), 126 – 147

Tran, C. (2020). Recommendations for ordinary users from mitigating phishing and cybercrime risks during COVID-19 pandemic. arXiv preprint arXiv:2006.11929

Twigg C.A., (2002): The impact of the changing economy on four-year institutions of higher education: The importance of the internet. *The Knowledge Economy and postsecondary education. Report of a workshop, 77-104.*

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. Psychiatry, Psychology and Law, 24(3), 323-338.

Vizoso, Á., Vaz-Álvarez, M., & López-García, X. (2021). Fighting deepfakes: Media and internet giants' converging and diverging strategies against Hi-Tech misinformation. Media and Communication, 9(1), 291-300.

Wall D.S.,2015: The Internet as a conduit for criminal activity. *Information technology and the criminal justice system, Pattavina A., ed 77-98*

Ward S. & Vedel, T. (2006): Introduction: The potential of the internet revisited. Parliamentary affairs 59(2), 210 – 225.

Warner, J. (2011). *Understanding Cybercrime: A View from Below. International Journal of Cyber Criminology, 5(1),736-749.*

Webb L., Craissati J. & Keen S., (2007): Characteristics of internet child pornography offenders: comparison with child molesters. *Sexual abuse: a journal of research and treatment 19 (4), 449-465*

Weisner T.S., 2014; Why qualitative and ethnographic methods are essential for understanding family life. *Emerging methods in family research, 163-176.*

Whittakker, J.M. & Button, J. (2018): Understanding pet scams: A case study of advance fee and non-delivery fraud using victims' accounts. https://doi.org/10.1177/0004865820957077

Whitty M.T., (2018): Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior and social networking 21 (2), 105-109.*

C. Internet Sources

Ghana Chamber of Telecommunications. https://www.telecomschamber.com/news-media/industry-news/ghana-records-over-11-000-cybercrime-cases-since-2019 Retrieved on 8th January 2022.

US Department of Justice (2021): https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting Retrieved on 19th June 2022.

Wiggins, R. (2000): Al Gore and the creation of the internet. Retrieved on 11th December 2020 https://firstmonday.org/issues/issue5_10/wiggins/index.html

D. Reports

MFWA. (2017a). *Cyber Security in Ghana*. https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf

Ministry of Communication. (2014). *Ghana National Cyber Security Policy & Strategy*. https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Ghana_2014_NationalCyberSecurityPolicyStrategyFina.pdf

E. Interviews

1. Interview with Akua Nyarko Asamoah, National Bureau of Investigation, 20th March, 2022.
2. Interview with Kevin Nii Gator, Ghana Immigration Service, 20th March, 2022.
3. Interview With George Owusu Oduro, Express Pay, 20th March, 2022.
4. Interview with Eric Mensah, E Crime Bureau Security, 20th March, 2022.

5. Interview with Elikplim Kuma Cyber hawk, 20th March, 2022.
6. Interview with Jemima Owusu Yeboa Cyber Security Authority, 22nd March, 2022.
7. Interview with Teki Akuetteh , Africa Digital Rights Hub, 22nd March, 2022.
8. Interview with Ambassador Baffour Adjei Bawuah Former Ghana Ambassador to USA, 25th March, 2022.

F. Focus Group

FOCUS GROUP 1, 9th January 2022

1. Nana Kwame Owusu, Level 300, University of Ghana.
2. Adam Samed, Petroleum Commissions, Accra.
3. Joseph Yaw Frimpong, ReaderApp, Accra.
4. Juliana Marfo, Makola Market, Accra.
5. Lawyer Akrasi Agyabeng, Osu.
6. Ernest Nyame, Ghana Police Service.
7. Kofi Mensah, Madina Market.
8. Mr. Charles Kwame Addo, Calbank Accra.
9. James Inkoom, Civil Servant, Accra.
10. David Kissi Amoako, Level 400, University of Ghana.

FOCUS GROUP 2, 3rd April, 2022

1. Krobea Asante Adomako, Speech Pathologist, Seattle Washington, USA
2. Isaac Nyame, Product Owner, Maryland, USA
3. Michael Kwabena Amoah, Business Analyst, Florida, USA
4. Brenda Afful, Student, Nantes University, France
5. Maame Nhyira Inkoom, Duensing Law, Canda
6. Nana Inkoom, Brookefield Asset Management, Canada.
7. Nana Kwame Ansah, Nurse, Washington, USA

G. Theses

Dugle, P. (2013). *"Press Coverage of Cybercrime Issues in Ghana: A Content Analysis of the Daily Graphic and Daily Guide". A Dissertation Submitted to the Department of Information Studies, University of Ghana, Legon.*

Valentine, J. P. (2021). Sim Card Fraud (Doctoral dissertation, Utica College).

APPENDIX

INTERVIEW GUIDE

TOPIC: ***An Examination of Cybercrimes in Ghana and its implications for the Ghanaian in the international community***

My name is Dominic Baafi Adomako. I am an M.A Student from Legon Centre for International Affairs and Diplomacy (LECIAD), University of Ghana. I am conducting research on the above topic for the purpose of my dissertation.

OBJECTIVE: The purpose of this study is to examine the implication of the rising incidence of cybercrime on the image of the Ghanaian in the international community. The knowledge and relevant information which scholars and policymakers could utilize to reduce the negative externalities suffered by Ghanaians due to activities of a few cybercriminals. This exercise is solely for academic purposes and is a requirement for awarding a master's degree in international Affairs. Data gathered through this interview will be treated with strict confidentiality and used solely for the purposes of this study. Thank you for your assistance. I am very grateful.

Can you please introduce yourself?

……
……
……

Objective 1: Implication of the rising incidence of cybercrime on the image of Ghanaians in the international community?

a) What do you understand by the term cybercrime?
b) In your opinion do the activities of cybercrime have any impact on Ghanaians in the international community.

c) What are some of the implications of cybercrime on Ghanaians in the international community?
d) Have you personally been a victim of cybercrime in form?
   - If yes, kindly share your experience.
   - If not, kindly give an account of issues of cybercrime you have witnessed or heard from friends.

Objective 2: Effectiveness of the laws that were enacted to deal with cybercrimes in mitigating the rising prevalence of cybercrimes?

Do you know of any cybercrime laws in Ghana? Yes / No, if yes, can you tell us some of the cybercrime laws you know?

a) Do you think these laws are effective in dealing with incidence of cybercrime?
b) Do you know of any institutions that is mandated to enforce these laws?
c) Do you know of any instances where these laws have been applied to perpetuators of cybercrimes?

Objective 3: Recommendations can be given to the government and stakeholders in their quest to reduce the incidence of cybercrimes?

a) What recommendations can you give that can help reduce activities of cybercrime in Ghana?
b) What role can enforcement of the law play to make sure that these cybercriminals are brought to book?
c) Can you think of other examples from other jurisdictions that have helped reduce cybercrime in those countries?
d) Do you believe that legislation is enough to reduce incidence of cybercrime?
e) Do you think that the image of the Ghanaian can be improved when the prevalence cybercrime is reduced?