

The “Sakawa Boys”: A Critique of the Policing of Cybercrime in Ghana.

Edward Akuako

MA in Critical Sociology

Submitted in Partial Fulfillment of
The requirements for the degree of
Master of Arts

Faculty of Social Sciences, Brock University
St. Catharines, Ontario

© Edward Akuako 2022

Abstract

Cybercrime, especially cybercrime related to online romance scams has increased exponentially in Ghana (Alhassan & Ridwan, 2021; Baylon & Antwi-Boasiako, 2016). As a result, the government of Ghana has deployed various traditional policing strategies to control this form of crime. However, this traditional policing strategies remains repressive and reactive and are unable to control Sakawa- related activities effectively in the country. This paper draws upon a Human Security framework as a reflective of non- traditional policing strategy to tackle the root form of this crime which is mainly poverty created by the country's implementation of Structural Adjustment Program (SAP) and neoliberal economics.

Acknowledgments

Dr. Ifeanyi Ezeonu, my supervisor you welcomed me with open arms and supported me through out my program. You have contributed to my academic and professional experience. Thank you for your commitment in this cause.

Professor Jane Helleiner, my committee member, you displayed your dedication and commitment to the well-being of your students to me. Your nourishment kept me going even when the going became daunting. I am forever grateful to you.

Professor Thomas Dunk, my Graduate Program Director, thank you for the good work you do for the cohort and the program, you were there for me anytime I called on you for assistance. I am very thankful to you for all your help.

Dr. Lauren Corman, Dr. Murray Smith, Dr. Hijin Park, Dr. Trent Newmeyer, and Dr. Andrea Doucet, I want you to know that your respective courses and diverse teaching styles have left indelible mark on my academic and professional progress. I appreciate your contributions towards my overall experience and success at Brock University.

Dedication

I dedicate this project to God for strengthening and carrying me through this piece. To my late uncle Joseph Yeboah, thank you for the immeasurable and invaluable roles you played in my life, may you rest in peace.

To my father, Frank Yeboah Koranteng, my mother Reginal Sarpomaa, grandmother Comfort Ayensu and my dear beloved Rebecca Boahemaa Yeboah, I could not have come this far if not for your unflinching and unconditional support and love for my progress. I love you always!

Table of Contents

	Page
Abstract.....	ii
Acknowledgement.....	iii
Dedication.....	iv
Chapter One.....	1
Introduction.....	1
Relevance of the Study.....	3
Research Questions.....	3
Accessing Relevant Sources.....	3
Theoretical Framework.....	4
Definition of Terms.....	6
Chapter Two.....	7
Literature Review.....	7
Online Scams in Africa.....	7
Organized Cybercriminal groups in Ghana.....	10
Structural Adjustment Programme in Ghana.....	12
Negative Impact of SAP in Ghana.....	13
Human Security as a Policing Strategy.....	18
Human Security versus State-Centric Security.....	19
Human Security and Policing of Cybercrime in Ghana.....	22
Chapter Three.....	24
Cybercrime in Ghana.....	24
Historical Development of Cybercrime in Ghana.....	24
Nature of Online Scams in Ghana.....	26
Forms of Online Scams in Ghana.....	28
Gold Fraud and Sakawa Boys.....	28
Online Estate Scam and Sakawa Boys.....	29

Credit Card Fraud and Sakawa Boys.....	30
Malware and Sakawa Boys.....	30
Online Romance Scam and Sakawa Boys.....	31
Chapter Four.....	34
Cybercrime: Organization, Growth, and the Challenges on Ghanaian Society.....	34
Introduction.....	34
How Sakawa Boys Organized their Activities.....	34
Online Romance Scam in Ghana.....	36
Challenges Imposed by Cybercriminal Activities on Ghanaian Society.....	39
Challenges to Individual Victims.....	40
Challenges to the Government and Corporate Institutions.....	40
Chapter Five.....	43
A Critique of the Traditional Policing of Cybercrime in Ghana.....	43
Introduction.....	43
Traditional Policing Strategies Against Cybercrime in Ghana.....	43
Electronic Transaction Act.....	44
Data Protection Act.....	45
National Information Technology Act.....	46
Criminal Offense Act.....	47
Ghana National Cyber Security Policy and Strategy.....	48
Cyber Security Act.....	49
Non- Traditional form of Policing Strategy.....	52
Human Security as Non- Traditional Policing Strategy.....	53
Policing of Cybercrime in Ghana using Human Security Architecture.....	54
Unemployment Benefits.....	56
Job Creation Opportunities.....	58
Regulation of Labour.....	59
Chapter Six.....	62
Summary and Conclusion.....	62

References..... 66

Chapter One

Introduction

Cybercrime, especially cybercrime related to online romance scams, gained prominence in Ghana in the late 1990s (Warner, 2011; Ennin, 2015). In Ghana, this form of cybercrime is popularly known as “Sakawa,” and it involves primarily poor young men using unscrupulous tactics to defraud both local and international victims with whom they established fraudulent romantic relationships in cyberspace (Amstrong, 2011; Barnor et al., 2020; Duah & Kwabena, 2015). Those involved in perpetuating these crimes are often referred to locally as “Sakawa Boys.” Scholars such as Aning (2007), Baylon and Antwi-Boasiako (2016), and Mohammed et al. (2019) trace the development of Sakawa to the high rate of unemployment and poverty created by the country’s adoption of neoliberal economics in 1983. The neoliberal economics, ushered in by the Structural Adjustment Program (SAP) in 1983, caused massive retrenchment (Obeng-Odoom, 2012; Oduyayo, 2015), leaving many young adults to find unconventional ways to survive the economic pressures. According to Overa (2007), Baah-Boateng (2004), and Akonor (2006), the SAP neoliberal policies were due to the pressure from the Bretton Woods institutions—i.e., World Bank and the International Monetary Fund (IMF), which situate the private sector at the heart of a country’s economic development.

The job losses brought by neoliberal economics led many young men to turn to Sakawa, and this in turn led to repressive and reactive policing of Sakawa-related activities by the Ghanaian government. The Ghanaian government has deployed various policing strategies to control this form of crime (Ennin & Mensah, 2019; Eboibi, 2020). These strategies include the Ghana National Cyber Security Policy and Strategy and Cyber Security Awareness Month (Ministry of Communications, 2015). The government has also enacted legislative Acts such as the Electronic

Transaction Act, Data Protection Act, and the Criminal Code Act 29/60 section 131 to control cybercrime (Ennin & Mensah, 2019; Eboibi, 2020). The National Cyber Security Policy and Strategy was established to prevent cyber fraud and find ways to enforce laws on cybercrime (Ministry of Communications, 2015). Also, the Electronic Transaction Act, Data Protection Act and the Criminal Code Act 29/60 section 131 were used to investigate and prosecute cybercrime perpetrators and these acts are still active (Eboibi, 2020). From the accounts of Baylon and Antwi-Boasiako (2016), Mohammed et al. (2019), and Eboibi (2020), these strategies and acts have not been effective in controlling the spread of this form of crime.

Given the premise (Ennin & Mensah, 2019, Eboibi, 2020) that the traditional policing strategies and acts remain repressive and reactive in addressing the problem of cybercrime in Ghana, this paper draws upon a Human Security framework to explore alternative, non-traditional policing strategies. The Human Security framework is built on meeting people's social and economic needs as a blueprint for crime prevention and control (United Nations Development Program, 1994; Hanlon & Christie, 2016). This non-traditional strategy recognizes the fact that cybercrime in Ghana results from the expanding ecology of poverty created by the country's implementation of the SAP and neoliberal economics.

This paper contributes to the knowledge of market political economy as a criminogenic force by situating the growth of cybercrime in Ghana within the devastating effects of the country's adoption of neoliberal economics. The findings of my paper highlight how the expanding ecology of poverty associated with this economic framework produces the increase in cybercrime and "Sakawa" more particularly in the country and limits the efficacy of traditional policing methods aimed at curbing this form of crime. This paper also contributes to the literature by exploring how

state efforts at cybercrime control might be more effective if a “Human Security” framework was adopted.

Relevance of the Study

Eboibi (2020) argues that in 2016, the Ghanaian government approved and implemented the Ghana Cyber National Security Policy and Strategy and acts to control the proliferation of cybercrime and reduce its impact on internet users. Unfortunately, the strategic policy and related Acts have not been as effective as expected. Eboibi (2020) reports that as a result of its failure to control the cybercrime menace, the government of Ghana has recorded an approximate \$299.9 million domestic economic loss due to cybercrime cases between the year 2016 and 2018 (p. 87). The victims of this loss include individuals, groups, and corporate bodies. There is therefore a need for a new policing strategy which addresses the economic challenges at the root of the crime.

Research Questions

This paper will address the following questions:

1. What is the nature of cybercriminal activity associated with the “Sakawa Boys”?
2. How have the neoliberal policies implemented in Ghana contributed to the emergence of the Sakawa Boys criminal group?
3. How could a policing strategy based on the “Human Security” framework help in tackling this form of crime?

Accessing Relevant Sources

This paper will rely mainly on a wide range of secondary sources, including books, journal articles, government reports and policies, IMF and World Bank documents, and other media sources. These

sources will be analyzed to achieve the objectives of the paper. Fortunately, there are reputable and informative secondary data sources available for this study.

Theoretical Framework

This paper uses the “Human Security” framework to evaluate alternative ways to tackle cybercrime in Ghana. The Human Security framework used in this context, draws upon scholarship on non-traditional form of policing best articulated in the works of Kempa (2008, 2010) and Neocleous (2000, 2008). These scholars, among other criminologists and exponents of critical security studies, conceptualize policing broadly as the “entire domain of what the government does to ensure what it considers to be the integrity of the polity and the well-being of the people” (Kempa, 2010, p. 108). Neocleous (2000) particularly promotes this expansive framing of policing to account for a range of institutions and mechanisms through which the state shapes and stabilizes civil society.

The broad conception of policing thus goes beyond a more narrow understanding focused only on institutional police forces. It is presented as most appropriate for the “holistic ways of thinking and examining human safety and well-being” (Kempa, 2010, p. 107). This expansive framework borrows from the earliest European idea of policing as the use of different mechanisms and social policies to maintain order (Neocleous, 2000, 2007; Kempa 2010; Foucault, 1979, 1965). Policing therefore comprises the totality of government policies, structures, and institutions used to organize and promote conformity to the social order and dominant norms.

In line with the works of Kempa (2008, 2010) and Neocleous (2000, 2008), the Human Security framework has been used by a growing number of Critical Criminologists such as Kim and Cho (2013), Benedek (2010), and Adesina (2017) in the context of exploring other forms of crime such as drug trafficking, terrorism, and organized crime. The Human Security framework

was espoused by the United Nations Development Program (UNDP) in its Human Development Report of 1994. In this report, Human Security was conceptualized as a people-centred alternative way of thinking about public security. It defines public security threats more broadly to highlight the underlying ecology of poverty and inequality, which creates different kinds of threats to society. In this context, the major security threats in society are commonly economic, and manifest as poverty, diseases, and different forms of crime (Reveron & Mahoney-Norris, 2011; Okubo & Shelly, 2011). As Okubo and Shelly (2011) argue, human security – i.e., the social welfare of the people - must be at the centre of any effort to tackle these crimes. The concept of Human Security for developing countries stresses the protection of people from the threat of poverty, unemployment, chronic diseases, hunger, crime, political repression, social conflicts, and environmental hazards (United Nations Development Program, 1994).

Further, Human Security emphasizes two major components: “freedom from want” and “freedom from fear.” The freedom from want means that individuals in developing countries should be able to take good care of themselves and have the opportunities and privileges to meet their essential needs (United Nations Development Program, 1994). On the other hand, freedom from fear means that there should be mechanisms and strategies put in place to protect people in developing countries from the fear of losing their jobs, the threat of crime, the spread of deadly diseases such as HIV/AIDS, and other social and economic challenges that may emerge in the future (United Nations Development Program, 1994).

I consider this theory to be most relevant to this paper because the policing of this criminal group (i.e., Sakawa Boys) should be situated within the context of the devastating effects of Ghana’s adoption of neoliberal economics. The implementation of neoliberal economics created a crisis of economic survival, affecting poor young men in significant ways. Unemployment and

debilitating poverty among this population are intolerably high; thus, creating the drive for alternative means of living. With greater access to the internet, cybercrime has become one of these alternatives (Baylon & Antwi-Boasiako, 2016; Duah & Kwabena, 2015). To effectively tackle this form of crime, policing strategies should address its economic origin to achieve any meaningful form of policing.

Definition of Terms

In the context of this paper, the following terms have the meanings set forth below:

Sakawa: This is a term synonymous with cybercrime in Ghana. It is used to describe all the unscrupulous tactics used by poor young men to defraud victims in cyberspace.

Sakawa Boys: This is a term used in Ghana to describe a group of poor young men who are involved in perpetuating internet-based crime.

Policing: This is defined as the totality of government policies, structures, and institutions used to organize and promote conformity to the social order and dominant norms.

Neoliberal Policies: These involve the 10 principles of the Washington Consensus which sums up the conditions attached to the financial aid advanced to the government of Ghana by the Bretton Woods institutions since 1983. These include fiscal discipline, reduction in public spending, including the removal of subsidies from education, agriculture, and health care delivery, interest rate hikes, privatization, increase in exports, trade and market liberalization, financial liberalization, deregulation of the labour market, introduction of a new comprehensive value-added tax (VAT), and promotion of individual property rights.

Scams: This is a term used to describe any fraudulent scheme that takes money or other goods from an innocent or unsuspecting people.

Online romance scams: This is a form of cybercrime based on the establishment of romantic relationships used as a deceitful tactic to defraud local and international victims in cyberspace.

Chapter Two

Literature Review

In this chapter, I review relevant literature to situate this paper within a wider body of scholarship thereby contextualizing the research. The first section of the chapter reviews literature on online scams in Africa and Ghana. Next, I explore the factors that contribute to the rise of cybercriminal activities in Ghana and analyze the adverse effects of the implementation of the Structural Adjustment Program in Ghana, including the exacerbation of criminal activities as coping strategies. This chapter further examines the concept of human security as a policing strategy, and human security versus the state-centric system of security, with the goal of exploring the former concept as a policing framework. Lastly, this chapter highlights the Human Security approach to the policing of cybercrime in Ghana.

Online Scams in Africa

Cybercrimes have recently grown exponentially in Africa (Finnan, 2015; Richards & Eboibi, 2021). This is because cybercriminal groups perceive that the African continent provides a favorable opportunity to perpetrate cybercrime (Kshetri, 2019). For example, Brody et al. (2019) argue that 419 scams started gradually in Nigeria and subsequently extended to other African countries like Benin, Senegal, Cameroon, Cote d' Ivoire, and Ghana as a result of the development of internet infrastructure. Evidence demonstrates that there are two categories of perpetrators who are involved in online scams in Africa (Eseadi et al., 2021; Alhassan & Ridwan, 2021). The first category of perpetrators of online scams are individuals who work independently to meet their essential needs (Eseadi et al., 2021). These individual scammers operate locally and target local victims and other government and private institutions such as banks (Alhassan et al., 2021). Most

of these individual scammers engage in cybercrimes where they target victims both locally and internationally (Anesa, 2020).

Aside from individual online scammers, we have other perpetrators of online scams who are organized in groups. These organized groups, which are often networks of online fraudsters found both locally and overseas, effectively coordinate their activities (Ennin & Mensah, 2019; Richards & Eboibi, 2021). These groups are mostly associated with the youth population in African countries. For instance, in Nigeria, a youth group called the “Yahoo Boys” engage in 419¹ scams also known as online scams. These boys work together to harm victims locally and overseas benefitting from cheap internet connection services in the country (Richards & Eboibi, 2021; Monsurat, 2020). The “Yahoo Boys” frequently engage in cybercrimes and sometimes hack into government institutional websites to steal relevant information to help with their operations (Richards & Eboibi, 2021). Perpetrators of online scams in organized groups have recorded many successes due to the nature of the groups they associate themselves with, which cuts across domestic and international networks (Richards & Eboibi, 2021). For example, it has been recorded that over 80 Africans were involved in the most recent internet scam that happened in the United States (Richards & Eboibi, 2021, p. 133). In this online scam, those who are engaged in this type of criminal behaviour have defrauded U.S victims through the stealing of personal identification information to file about 980 false federal tax returns demanding more than 6.6 million US dollars in fraudulent refunds which led to the loss of more than 2 million US dollars (Richards & Eboibi, 2021, p. 135). In Nigeria, the organized cybercriminal youth groups are known as “Yahoo Boys”; in Cameroun, they are popularly known as “Faymania Boys”; and in Ghana, they are known as

¹ 419 Scam is coined from section 419 of the Nigerian criminal code dealing with fraud. See Chapter 38 of the Nigerian criminal code for more details <http://lawsofnigeria.placng.org/laws/C38.pdf>

“Sakawa Boys” (Monsurat, 2020; Whitty, 2018; Tade & Aliyu, 2011). These organized cybercriminals youth groups in Africa are primarily dominated by poor youth who use dishonest tactics to defraud both African and international victims with the aim to survive the economic pressures (Richards & Eboibi, 2021). One of the most popular forms of cybercrime that target both Africans and international victims is internet fraud, specifically online romance scams (Richards & Eboibi, 2021; Whitty, 2018).

The proliferation of internet fraud and the emergence of these organized cybercriminal groups have propelled African countries to develop policing strategies to curb the menace. Most African countries have established legal frameworks to assist in arresting, investigating, and prosecuting cybercriminal groups. Also, there have been campaigns against cybercrimes, the development of policies, and an increase of surveillance to curb the rise of cybercrime in Africa (Richards & Eboibi, 2021). However, despite regional and national efforts to control cybercrime, Africa has experienced a significant increase in cybercrime (Finnan, 2015). In West Africa, Nigeria and Ghana are the leading states that have been witnessing the rise in internet-based crime activities (Aransiola & Asindemade, 2011; Quarshie & Martin-Odoom, 2012). The perpetrating criminal groups are mostly made up of unemployed university graduates, often young males who join these groups hoping to achieve quick wealth in the context of devastating African economies (Udelue & Mathias, 2019; Whitty & Ng, 2017). These criminal groups often operate in groups or gangs with loose networks across the world (Whitty & Ng, 2017). Sometimes it is difficult to commit this crime alone. Therefore, they form local and international collaborations to make their operations easier and less challenging (Aransiola & Asindemade, 2011). These criminal groups form international networks to more easily clear cheques and goods across borders, while local networks allow the sharing of the knowledge and skills needed to be successful in their operation.

This paper specifically focuses on both the nature of the individual and organized group scammers who use unscrupulous tactics to defraud victims online both locally and overseas.

Organized Cybercriminal groups in Ghana

In Ghana, perpetrators of online scams are known locally as “Sakawa Boys” because those involved are dominated by poor young men who are hungry with no real option for making ends meet or to find a real career path (Duah & Kwabena, 2015). A compelling body of literature shows that cybercrime, especially those related to online romance scams, have increased exponentially in Ghana since 1999 (Warner, 2011; Barnor et al., 2020). As a result, the government has deployed various policing strategies to control this form of crime. However, Eboibi (2020) argues that despite these policing strategies, cybercrime continues to worsen in Ghana. One school of thought suggests that the proliferation of cybercrime is associated with the growth in public access to internet connectivity (Baylon & Antwi-Boasiako, 2016; Ennin & Mensah, 2019; Warner, 2011). Baylon and Antwi-Boasiako (2016) specifically argue that the expansion of Ghana's internet infrastructure and the widespread development of cheaper and faster internet connectivity have provided greater resources for criminal groups to effectively target potential victims in Ghana and overseas. They further argue that the development of internet infrastructure has also contributed massively to the proliferation of cybercrime and has increased the number of “Sakawa Boys” in the country.

Another school of thought posits that the proliferation of cybercrime is associated with the failure of the traditional use of law and enforcement agencies as a policing approach to address the problem (Baylon & Antwi-Boasiako, 2016; Eboibi, 2021; Richards & Eboibi, 2021). In other words, they argued that the use of law enforcement agencies as a traditional approach of policing cybercrime is ineffective for controlling cybercrime in Ghana. Given the failure and

ineffectiveness of the traditional approach of controlling cybercrime in Ghana, this paper focuses on using the Human Security framework to reflect the non-traditional policing strategy used to control cybercrime. The Human Security framework draws upon the works of critical criminologists such as Mark Neocleous (1998, 2000), Stuart Hall et al. (1978), Kempa (2010), and other critical security exponents to address the issue of cybercrime. Critical criminologists use a concept of policing that goes beyond the use of formal law enforcement agencies to address cybercrime (Daleiden, 2004; Kempa, 2010; Neocleous, 2000). These critical criminology scholars also indicated that the economic needs of individual citizens play a major role in contributing to cybercrime (Neocleous, 1998; Kempa, 2008). They further stated that adopting the Human Security framework tackles the security needs of poor youth—and therefore, must be at the hub of policing cybercrime activities in a country, especially in the Global South.

Other scholars argue that the proliferation of cybercrime is highly connected to the expansion of poverty and unemployment created by the adoption of the country's neoliberal economies in 1983 (Baylon & Antwi-Boasiako, 2016; Barnor et al., 2020; Mohammed et al., 2019). The massive retrenchment caused by the implementation of SAP in 1983 (Obeng-Odoom, 2012; Oduyayo, 2015), made the poor young adult to use a non-conforming means to survive the economic pressures. They further argue that the country's adoption of neoliberal economies and its devastating effects of the SAP contributed to cybercrime's emergence in Ghana.

Lastly, several studies have argued that Ghana's implementation of SAP embedded in the IMF and the World Bank conditions on loans has had significant adverse effects on the population and the economy (Ezeonu, 2000; Obeng-Odoom, 2012). As a result, youth have been propelled to acquire a creative negative survival skill, using cybercrime as an alternative means of survival. Also, the devastating effects of the SAP, such as inadequate job opportunities, high cost of

education, and lack of access to health care, confronts many poor Ghanaian youth and pushes young men and women into armed robbery, prostitution, illegal migration, and swindling activities.

Structural Adjustment Programme/ Neoliberal Policies in Ghana

In 1983, Ghana adopted neoliberal policies (the SAP) under the influence of the IMF, the World Bank, and other partners with development organizations to help reverse the economic crisis Ghana experienced in the 1970s and early 1980s, popularly known as the "lost decade" in the country (Azindow, 2005; Ezeonu, 2000). The SAP has two phases, the first phase was introduced as the Economic Recovery Program (ERP) in 1983, and the second phase was initiated in 1986 (Azindow, 2005; Danaher, 1994). The initial SAP Ghana implemented lasted from 1983 to 1992, in which most of the neoliberal policies were incorporated in the Washington Consensus (Otoo, 2015). Akonor (2006) and Ismi (2004) assert that Ghana also implemented the Enhanced Structural Adjustment Facility to redress the negative effects of the initial SAP.

Danaher (1994), Azindow (2005), and Ismi (2004) argue that the implementation of Ghana's adjustment programs to address the economic crisis led to a huge cut in government expenditure in health, education, agriculture, transportation, and energy sectors. Also, the adjustment led to the sale of some state-owned enterprises to the private sector, causing massive retrenchments of workers and many people losing their source of family income. Research shows that the implementation of the Economic Recovery Program as an adjustment strategy has achieved some of its objectives of enhancing economic growth by way of government commitment to fiscal and monetary discipline (Azindow, 2005; Danaher, 1994; IMF, 1998). However, Ghana's adjustment has brought more difficulties and hardship to the Ghanaian population, especially for

poor young men and women, with inadequate job opportunities being the major troubling effect (Nnorom et al., 2015).

Negative Impacts of SAP in Ghana

Studies demonstrate that Ghana's adoption of neoliberal policies embedded in the IMF and the World Bank loan conditionalities has had significant negative impacts on the population and the economy in general (Ayelazuno, 2014; Ezeonu, 2000; Obeng-Odoom, 2012). One of the major negative impacts was the high rate of youth unemployment. Essamuah & Tonnah (2004) argue that the implementation of policies under SAP, such as government downsizing, cuts in public infrastructure expenditure, and the privatization of state-owned enterprises, led to a greater loss of jobs in the civil and public services. Also, the privatization of state-owned enterprises associated with the neoliberal policies caused massive retrenchment among young people in Ghana who have completed college and university education (Amankrah, 2012). These young people have acquired the necessary skills and knowledge ready to work but unfortunately, they are unable to find any meaningful work due to inadequate job opportunities available (Ayelazuno, 2014 Braimah & King, 2006). As a result, many young men turn to cybercrime and young women resort to sex work and sugar daddy schemes (Oduro, 2012; Nnorom et al., 2015). Amankrah (2012) specifically argues that in Ghana, about 60% of youth are unemployed, making the country's youth one of the highest unemployed populations in the world. Further, research conducted by the Institute of Statistics, Social and Economic Research (ISSER) of the University of Ghana revealed that only 10% of graduates find jobs after their first year of completing college or university degree due to the challenges of inadequate job opportunities and low capacity of industries to absorb a greater number of graduates (ISSER, 2017, p. 1). Mr. David Nkrumah-Boateng, the Head of Impact, Camfed Ghana, specifically stated that graduate unemployment is not only becoming a national

issue, but a security threat to the population (ISSER, 2017). Ezeonu (2000) also reports that employment in the manufacturing sector fell from 78,700 in 1987 to 28,000 in 1983 due to market and trade liberalization associated with Ghana's neoliberal policies (p. 93). These troubling statistics indicate that unemployment has become a serious phenomenon that affects the country's economic growth because of the country's adoption of the SAP.

Again, the SAP has expanded the ecology of poverty among Ghanaian youth (Ezeonu, 2000). Oberhauser and Yeboah (2011) and Oduro (2012) argue that the neoliberal policies continue to devastate impoverished Ghanaian youth, driving them into greater poverty and ushering them to acquire creative negative survival skills. They further posit that the devastating effects such as poverty associated with adopting neoliberal policies in Ghana have pushed some young men and women into sex work, armed robbery, and internet fraud activities. Although the IMF and World Bank's main objective is to alleviate poverty in developing countries (Moosa & Moosa, 2019), Konadu-Agyemang (2018), Owusu (2005), and Anyinam (1994) argue that poverty in Ghana was higher after the economic adjustment than before its implementation. Owusu (2005) argues explicitly that the implementation of SAP has negatively affected urban inhabitants and exacerbated poverty in the urban areas, especially in the areas of housing, education, health, environment, water, and sanitation.

The government withdrawal of housing subsidies under the implementation of SAP has contributed to the housing crisis experienced by poor Ghanaian youth (Konadu-Agyemang, 2001, 2018). Prior to the implementation of SAP, the government of Ghana was involved in the provision of state interventions in housing by providing roofing and building materials, loans, and group lending to facilitate the development of organized neighborhoods (Owusu, 2005). These state interventions helped provide low-cost housing for poor and landless people in the country (Ofosu-

Kusi & Danso-Wiredu, 2014). However, under the dictate of SAP, the government withdrew itself from delivering housing to its poor population, but allowed market forces to operate (Owusu, 2005). Konadu-Agyemang (2001, 2018) also argues that the introduction of Value Added Tax (VAT) to housing production, due to less government intervention in housing delivery under SAP, has contributed to the high cost of housing development in the country. Based on this evidence, I argue that the inability of the government to provide affordable housing units for its poor youth under the dictate of SAP pushed some young men into “Sakawa” and young women into sex work activities etc., as they attempted to afford the high cost of housing in the country.

The health sector in Ghana was also affected negatively as a result of the implementation of SAP (Owusu, 2005; Konadu-Agyemang, 2018). Under the implementation of SAP, the government's ability to maintain, expand, and improve the health care delivery system declined enormously due to the government's SAP-induced cutbacks in health expenditure and the introduction of user fees in public health institutions (Anyinam, 1994; Owusu, 2005). Anyinam (1994) specifically argues that Ghana's health fees have increased by 800 to 1000 percent; due to the high cost of healthcare services, poor Ghanaian youth find it difficult to seek medical care in the country. The SAP-induced cutbacks in the health expenditure have had a debilitating effect on the population, especially on poor Ghanaian youth who are unable to pay for medical bills and purchase essential drug prescriptions (Owusu, 2005). The introduction of user fees under the implementation of SAP has compelled many poor Ghanaian youth to resort to self-treatment and alternative medicine provided by untrained and unregulated herbalists due to the high cost of medical care (Owusu, 2015). Anyinam (1994) posit that the implementation of SAP did not only prevent the poor Ghanaian population from accessing healthcare, but also led to inequalities in the healthcare system. The inequalities in the healthcare system were also manifest urban-rural

disparities (Anyinam, 1994). Konadu-Agyemang's (2001) study shows that in 1999 under the implementation of SAP, a significant proportion of Ghana's lower socioeconomic population resided in rural areas. As a result, approximately 8 million people were unable to access necessary health care because most healthcare facilities were located in urban areas. The inequalities in health care delivery and the lack of effectiveness of the healthcare system signify the failure and the ineffectiveness of SAP in the country.

An increase in food prices and limited access to clean drinking water as a basic necessity of life to poor Ghanaian youth are some of the deleterious effects of the implementation of SAP in the country (Anyinam, 1994). Under the implementation, the only attempt was to improve the food sector in order to expand export production but not domestic consumption (Apusigah, 2002). The focus to expand export production led the government to divert resources towards export production through cutbacks and agricultural subsidies (Owusu, 2005). Apusigah (2002) explicitly argues that the agricultural sector's cutbacks under SAP reduced the country's agricultural budget from 10 percent in 1983 to 4.2 percent in 1986 and 3.2 percent in 1988. The promotion of massive export production under the implementation of SAP led to a continuing shortage and increase in food prices in domestic markets (Owusu, 2005). Poor Ghanaian youth, especially unemployed young men and women, bear the brunt under these conditions, thus causing them to resort to unconventional means of survival.

Access to clean drinking water for poor Ghanaian youth was also denied due to SAP implementation. Anyinam (1994) demonstrates that there were inequalities in the distribution of safe drinkable water resources in the country under SAP. As a result, poor Ghanaian youth were victimised. He further stated that the privatization of public services associated with SAP meant, for example, that only those with higher incomes could access quality drinking water. Therefore,

those who could not afford it had to rely on other water supply sources, such as untreated water from ponds and rivers, which have health-related consequences. Again, the introduction of user-pay adjustment policies suggested by IMF and World Bank limited the accessibility to clean drinking water by the deprived community in the country (Anyinam, 1994).

A review of the literature in this area indicates that the implementation of Structural Adjustment Programs in Ghana has created an economic crisis, resulting in poverty, hunger, and unemployment among youth. The SAP implementation has had a significant impact on young men, many of whom have been pushed into "Sakawa" activities to survive these economic crises. Throughout this paper, I therefore argue that the government policing of "Sakawa" in Ghana should be situated within the broader context of the economic crises created by the country's adoption of neoliberal economics (SAP).

Human Security as a Policing Strategy

Critical criminologists and security exponents have argued for a broad conception of policing which goes beyond the public police as an agency of the state to control criminal behaviour (Kempa, 2010; Neocleous, 2000; Hall et al., 1978). This expansive framework was borrowed from the earliest European idea to include the entire domain of what the government does to maintain the well-being of the people (Kempa, 2008, 2010). In other words, the concept of policing includes the mechanisms and social policies the government uses to maintain law and order in society (Hall et al., 1978). Gill (2002) also demonstrated that the expansive concept of policing is more useful as it focuses on the economic and social regulation of people in a country. Given the expansive framework of policing, the concept of human security is used as a policing strategy to promote the well-being of the civil population. Kempa (2008, 2010), in particular, argues that human security as a policing strategy must take the economic well-being of a country's

poor population into consideration. He further stated that the human security policing framework provides a holistic approach to policing which emphasizes not only the protection of state security, but also protects people from the threat of poverty, unemployment, political repression etc. Human Security as a policing strategy is centred on the general welfare of the people to maintain order rather than the ad hoc repressive and reactive measures taken by the formal policing institutions (Neocleous, 2000, 2006). The introduction of Human Security as a policing strategy creates awareness of the changes in the nature of policing over time in relation to the welfare of the poor population and the changes in the political economy of a state (Crowther, 2000). This paper highlights the human security framework as a new policing strategy to address the security needs of the civilian population, especially poor youth in Ghana.

Human Security versus State-Centric Security

Studies show that the concept of security has been interpreted narrowly after the devastating effects of the Cold War on several nation-states globally (Axworthy, 2001; Liotta & Owen, 2006; Paris, 2001; Singh, 2014). After the end of the Cold War, the concept of security traditionally focused on the state to protect its citizens (Axworthy, 2001; David, 1997). The realist paradigm of security centered on the states as a referent object and how to protect territories from external threats, attacks, and aggression (Lin, 2011). The state-centric security system emphasizes how the state can enhance its military interventions and protect its national interest from foreign policies and the threat of nuclear weapons (Kerr et al., 2003). However, several critical security studies demonstrate that the state-centric security system is limited and inadequate to address the threat associated with individual welfare and freedom— i.e., Human Security (Fukuda-Parr & Messineo, 2012; Paris, 2001). Liotta and Owen (2006) argue specifically that the primary objective of the state-centric system of security – i.e., the traditional form of security – has failed to protect the

individual from the threat of poverty, diseases, unemployment, hunger, natural disaster, violence, landmines, and human rights abuse. Below is a table that clearly demonstrates the distinction between state-centric security (traditional security) and human security and its referent object.

Traditional vs. Human Security

Type of Security	Referent Object	Responsibility to Protect	Possible Threats
Traditional Security	The State	The Integrity of the State	Interstate War Nuclear Proliferation Revolution.
Human Security	The Individual	The Integrity of the Individual	Disease, Poverty, Natural Disaster, Violence, Landmines, Human Rights Abuses

Sourced: Liotta and Owen (2006)

Several critical security experts argue that Human Security provides a broad and holistic approach that goes beyond the capacity of the state-centric form of security (Hanlon & Christie, 2016; Singh, 2014; Paris, 2001). In other words, human security goes beyond the notion of the traditional form of security (state-centric) that encompasses only the military dimension or interventions.

Human Security is centered on public security which focuses on poverty and inequality, which create different kinds of threats to society. The Human Security also symbolizes the protection of people from the threat of diseases, hunger, unemployment, crime, social conflict, political repression, environmental disasters, and poverty (United Nations Development Program, 1994). Hanlon and Christie (2016) argue that the Human Security specifically deals with protecting individuals from the economic and social crises that have created impoverishment and hardship to millions of people in the Global South.

The Human Security approach also focuses on putting measures in place to safeguard people from the threat of unemployment, crime, and poverty (United Nations Development Program, 1994). This means that state government should develop initiatives and programs that liberate and protect people from the anxiety of losing their jobs, accessing healthcare, securing daily income, and acquiring the basic essential needs for their lives (United Nations Development Program, 1994; Winter, 2014). Winter (2014) specifically argues that freedom from fear associated with Human Security signifies a means to an end—i.e., the objectives or goals of the initiatives and strategies implemented by states should be to eradicate poverty, unemployment, hunger and the spread of deadly diseases such as HIV/AIDS.

The concept of Human Security has four significant characteristics that are elaborated in the 1994 Human Development report. First, Human Security is universal—i.e., human security is relevant to people everywhere, especially those in developing countries that suffer many threats such as poverty and unemployment. Second, Human Security is interdependent, meaning the security of people is endangered anywhere in the world. In other words, threats such as poverty and unemployment are not confined within the national border but transcend to other countries across the globe, especially developing countries. Third, Human Security is best ensured through early prevention, rather than later intervention. Lastly, Human Security is people-centered—i.e., it is concerned with how people live and how much access they have to market and social opportunities in a state.

Moreover, the concept of Human Security is categorized into seven characteristics which include economic security—i.e., freedom from poverty and unemployment; food security (freedom from hunger); health security (freedom from disease, e.g., access to health care and protection from disease); environmental security (the availability of clean water and air, and

protection from disasters or danger, e.g., environmental pollution and depletion); personal security (freedom from fear of violence, crime, and drugs); community security (freedom to participate in family life and in one ethnic group); and political security (freedom to exercise one's basic human rights) (United Nations Development Program, 1994; Hanlon & Christie, 2016). Hanlon and Christie (2016) posit that the human security concept ensures individual survival and dignity as human beings. Therefore, it is significant to think about security that goes beyond merely protecting human life in a situation of conflict.

Generally, literature in this area has demonstrated that even though the state-centric form of security is important, it does not adequately protect people from the threat of poverty, unemployment, hunger, diseases, etc., during conflict situations. However, the concept of Human Security broadly highlights and expands on state-centric security – i.e., traditional, or national security – and considers the protection of people from the threat of poverty, unemployment, hunger, and diseases. As a result, the literature hypothesizes Human Security as an alternative to address the expansion of cybercrime, especially online romance scams in Ghana. The Human Security framework protects the welfare of the perpetrators of cybercrime – i.e., Sakawa Boys – and addresses poverty, unemployment, hunger, and diseases associated with these criminal groups.

Human Security and Policing of Cybercrime in Ghana

Several critical criminologists have used the concept of Human Security in the context of exploring other forms of crime and its prevention, such as drug trafficking, terrorism, and transnational organized crime (Adesina, 2017; Benedek, 2010; Kim & Cho, 2013). For example, in the context of terrorism and organized crime, Benedek (2010) and Bobic (2014) argue that Human Security provides a practical approach to address the security needs of the individual, such as the alleviation of unemployment and poverty, even though terrorism and organized crime threaten the security of

the state. Also, Kim and Cho (2013) argue that Human Security provides a better approach to policing drug trafficking operations in North Korea due to its prioritization of basic human needs and welfare as a necessary condition of society.

Further, in the context of cybercrime, Shannon and Thomas (2005) argue that cybercrime poses a real challenge to national infrastructure and development. As a result, the best way to police this threat is to adopt the Human Security approach (Shannon & Thomas, 2005). Adesina (2017), Okubo, and Shelly (2011) argue that in Nigeria, Human Security – i.e., the welfare of the people – must be at the center of any effort to tackle cybercrime considering the level of poverty and unemployment. In Ghana, the concept of Human Security has been used to address issues in climate change and gender inequality (Dankelman, 2008; Marfo, 2013). It has also been used as a conflict resolution approach in promoting peace among ethnic groups (Dankelman, 2008; Marfo, 2013).

However, very few studies in the literature have used the Human Security concept as an alternative approach to address cybercrime in Ghana, especially online romance scams. This paper aims to fill this gap and contribute to the literature by adopting the Human Security approach to address the high rates of cybercrime in Ghana.

Chapter Three

Cybercrime in Ghana

The objective of this chapter is to provide a historical overview of the development of “Sakawa Boys” in Ghana. The Sakawa Boys often utilize various strategies to target their victims. This chapter provides a detailed understanding of the nature of the cybercriminal activities of the Sakawa Boys in order to formulate an appropriate policing response initiative.

Historical Development of Cybercrime in Ghana

The development in global telecommunication infrastructure, including computers, mobile phones, and the internet, has brought about a major transformation in world communication, businesses, and the economy, especially in the Global South. (Baylon & Antwi-Boasiako, 2016; Warner, 2011). In Ghana, the young and the old now have access to the world from their homes, offices, and cyber cafes. Recently, internet or web-enabled phones and other devices like iPods, laptops, and Blackberry, have made internet access easier and faster (Warner, 2011). However, one of the dark sides of this broad access is the issue of cybercrime (Duah & Kwabena, 2015; Warner, 2011). In Ghana, the utilization of the internet has seen a significant increase since the liberalization of the telecommunication industry in the 1990s (ITU, 2008). The country had 43 Internet users per 1,000 people in 2008 as compared to 1 Internet user in 1999 (ITU, 2008). The number of PC owners doubled to 52 owners per 1,000 people between 1999 and 2005 (ITU, 2007). Until 1990, Ghana had few records in the cybercrime books (Warner, 2011). This shows that Ghana is not exempt (Baylon & Antwi-Boasiako, 2016). Warner (2011) specifically indicated that the rise and practice of cybercrime in Ghana has gained unsavoury records alongside with other countries such as Cameroon and Nigeria, as among the top ten cybercrime producing states. He further indicated that, historically, the term and practices of cybercrime in Ghana began in the

early 1990s and became intensive in the late 2000s when second-hand computers and laptops thrived in the electronic market in the country.

Cybercrime which is otherwise known in Ghana as “Sakawa” – i.e., online scam – is a Hausa term that consists of the root “saka”- [to put it in] and “wa” (a simultaneously past and plural affix). Combined, these affixes literally mean “to [have] put something in” (Duah & Kwabena, 2015; Warner, 2011). The name “Sakawa” emerged to describe poor Ghanaian youth alleged to be involved in internet-based crime activities (Duah & Kwabena, 2015). Baylon and Antwi-Boasiako (2016) argued that the development of related criminal groups in Ghana could be traced to the advent of internet connectivity in Ghana. This cheaper and faster means of mass communication made it possible for Ghanaian cybercriminal groups to engage in all forms of illegal activities which targeted both local and international victims (Baylon & Antwi-Boasiako, 2016). Warner (2011) identified three different forms of cybercrime which were prevalent in Ghana: online romance fraud, fake gold dealers, and estate fraud. Burrell (2008) also indicated that cybercrime in Ghana was an extension of a more good-natured practice: writing to foreign pen pals (boyfriends, girlfriends, or other relationships). Some of the young people who were involved in this earlier practice considered these relationships primarily as strategic attachments for recognizing material gain (Burrell, 2008).

Before the internet became easily accessible in Ghana, the most common form of electronic-based crime was credit card fraud (Warner, 2011). This type of internet-based fraud happens when Ghanaian youth steal and share pertinent information about Western visitors' credit cards with scammers living overseas to assist them in purchasing goods on the internet and having them shipped to Ghana (Warner, 2011). This form of internet-based crime was reduced in approximately 2004 (Warner, 2011). However, new forms of internet-based fraud began to

develop due to easy internet accessibility (Baylon & Antwi-Boasiako, 2016). A common tactic of internet fraud that is perpetuated in Ghana, is Advanced-fee fraud (AFF). The Advanced-fee fraud occurs when a scammer falsely promises a local or foreign victim a considerable sum of money in exchange for an upfront payment (Baylon & Antwi-Boasiako, 2016; Warner, 2011; Webster & Drew, 2017). The Advanced-fee fraud tactics used by Sakawa Boys has progressed into different forms and types – i.e., the modern online scams (Baylon & Antwi-Boasiako, 2016).

Nature of Online Scams in Ghana

Online scam perpetrators use various strategies to be successful in their operation (Ennin & Mensah, 2018). In this form of online criminal activity, there are two categories of perpetrators. These are individual online scammers – i. e., those who operate or work independently – and those who are involved in an organized group and whose activities are coordinated. These scammers steal people’s bank accounts details and credit card information to gain access to their funds (Ninson, 2017). They could use such information to buy goods online (Warner, 2011). They also use malicious software to access web pages containing confidential information (Oduro-Frimpong, 2011). In a study investigated by Ennin and Mensah (2018), it was found that individual scammers often engage in online scams such as online shopping, identity theft, and online romance scam. However, the most common online scam that has increased in Ghana is online romance scam (Baylon & Antwi-Boasiako, 2016; Cassiman, 2019; Warner, 2011). Many individual scammers reside within major cities such as Accra, Takoradi, and Kumasi where they can have easy access to internet connectivity (Ninson, 2017). These individual scammers are mostly Ghanaian youth, especially graduates who are unemployed or underemployed and in need of alternative ways of making quick wealth in order to survive the economic hardship in the country (Warner, 2011; Baylon & Antwi-Boasiako, 2016). These scammers target individual victims, institutions, banks,

and other government and private corporate bodies both locally and internationally (Warner, 2011; Baylon & Antwi-Boasiako, 2016; Mohammed et al, 2019).

Along with individual scammers, there are also online scammers who are involved in more coordinated activities both locally and internationally (Ennin & Mensah, 2018). An empirical study conducted by Ennin and Mensah (2018) demonstrated that these online scammers are individuals who find it difficult to commit this form of criminal activity alone. In their study, they indicated that the majority of these online scammers have both local and international associates with whom they conduct their activities. They receive more knowledge and skills from such local and international networks especially when they are having difficulty in their operation (Ennin & Mensah, 2018). For example, they highlighted that one of the participants in cybercriminal activities reported that even though he had colleagues overseas, he had a lot of colleagues in Ghana with whom he shared ideas when dealing with local and foreign victims. The Inspector-General of Police, James Opong-Boanuh, indicated that organized criminal groups engage in this form of crime by forming networks of well-resourced criminal gangs who are found both locally and internationally (MyNewsGH, 2021). This is demonstrated by a recent case of a Ghanaian-based internet scammer who identified himself as John Jacob and reported friend and fellow scammer based in the US (named Ruph Adoe Awuni.), to the US Federal Bureau Investigation (FBI) (Ikeji, 2021). The internet scammer based in Ghana reported his fellow scammer because the latter refused to split the 10 million US dollars they successfully made together from an unemployment online scam (Ikeji, 2021).

Also, similar evidence highlights a group of six “Sakawa Boys” based both the US and Ghana who are involved in several online scams, such as business emails and online romance scams, against individuals and businesses located in Ghana and across the United States (United

States Attorney's Office, 2021). According to the New York office of the FBI, these Sakawa Boys worked collectively to control more than 45 bank accounts through which they accessed approximately 55 million US dollars (United States Attorney's Office, 2021). Further, these criminal groups engaged in romance scams by using electronic messages sent via emails, text messages, and online dating websites with fake identities to defraud local and international victims who believed they were in a romantic relationship with real people (United States Attorney's Office, 2021). This evidence demonstrates that these criminal activities are perpetrated by poor youth who form various networks both locally and internationally, thus causing a massive threat to individuals, organizations, and government institutions (Alhassan & Ridwan, 2021; Boateng et al., 2011; Duah & Kwabena, 2015). This also shows that there are individual online scammers who work independently and are not part of the organized groups whose activities are coordinated. However, sometimes they associate themselves with friends overseas with whom they share similar goals.

Forms of Online Scams in Ghana

Gold Fraud and Sakawa Boys

Warner (2011) and Osei-Mensah (2019) assert that gold fraud is another one of the internet-based crimes that is perpetuated by Sakawa Boys. In gold fraud, there are several tactics used by Sakawa Boys to swindle victims. Ghana is recognized as a country that has an abundance of gold ore. As a result, the Sakawa Boys utilize this opportunity to advertise fake gold products on the internet. In Osei-Mensah's (2018) study, a Sakawa Boy explained that he uses gold dealership to defraud people on the internet because his victims believe that Ghana has access to sufficient gold ore, so victims find it plausible that the perpetrator is an investor or trader in gold in Ghana. In this fake gold dealership, the Sakawa Boys offer a competitive gold price on the internet which falls

below world market prices. These prices attract foreign investors online and thus provides an opportunity for Sakawa Boys to dupe investors. For investors to believe in the dealership, the Sakawa Boys generate fake licenses and documents from government institutions such as the mineral commission and General Survey Department. After the investors have paid the initial deposit for delivery, the scammers invent an excuse to explain a major problem that has affected the delivery process, which may require extra fees (Warner, 2011). This tactic would proceed until the investors (victims) get frustrated and realize that this is a fake online gold business (Osei-Mensah, 2018). After people realize they participated in a scam, the Sakawa Boys immediately cut ties with the victim.

Online Estate Scam and Sakawa Boys

The online estate fraud takes a cue from gold fraud (Warner, 2011). In this form of criminal activity, cybercriminals (Sakawa Boys) create a fake online real estate business to dupe their potential victims (Obiri-Yeboah, 2015; Warner, 2011). The Sakawa Boys would contact victims, mostly Ghanaians residing overseas, to help build their houses for them in Ghana (Nana, 2015; Warner, 2011). They portray themselves as real estate agents that provide assistance to Ghanaians abroad who may want to build a house in Ghana and return upon their retirement (Warner, 2011). The Sakawa Boys use this opportunity to defraud victims of money that has been sent from overseas for the construction of the houses (Nana, 2015; Warner, 2011). Moreover, the Sakawa Boys know that creating this fake online estate business provides an investment opportunity for people living abroad (Warner, 2011). Therefore, it encourages potential victims to invest in properties such as lands and hotels (Warner, 20011). In most cases, the Sakawa Boys provide the victims with fake documents that were purportedly issued by the government of Ghana, such as land documents from the land commission, and business certificates from the Registrar General

Department (Nana, 2015). At times, a duplicate website is designed to look like a legitimate one, or will direct people to a legitimate website when visited (Duah & Kwabena, 2015). This form of crime has affected individuals, as well as the government's reputation on an international level (Duah & Kwabena, 2015).

Credit Card Fraud and Sakawa Boys

Modern technology has made it possible for businesses to transact and transfer money electronically (Ninson, 2017). This has gained massive recognition and patronage by general populations. However, Sakawa Boys are devising new and innovative ways to steal people's money, which poses a bigger challenge to the digital economy. Schmallegger and Pittaro (2009) explained that Credit Card Fraud is a kind of scam where criminals use credit card of someone else to make transactions without the knowledge of the original owner that his/her card is being used. This is an illegal use of different people's credit cards or bank details for profit through fraud and impersonation. A study conducted by Eurobarometer in 2013 engaged with 27000 participants in all member states. In this study, they indicated that all the respondents agree that there is a very high danger of becoming credit card/banking online fraud victims. The Sakawa Boys put fear into individuals and organisations when it comes to online transactions.

Malware and Sakawa Boys

Malware, according to Merriam-Webster online dictionary, is "software designed to interfere with a computer's normal functioning" (Mirriam-Webster, n.d). Sakawa Boys inject viruses, worms, Trojan horse, adware and spyware over the cyberspace to attack individuals, corporate and even government websites to collect vital information. Malware is a computer code designed with spiteful intentions. Occasionally, malware is categorically used by Sakawa Boys to

attack government or company websites to collect protected information, and to interrupt their process and procedures to their advantage. However, malware can also be launched to target people in order to gain access to their personal details such as personal identification numbers, bank details, credit card numbers, and passwords to defraud them (tapestry networks, 2015). For instance, in 2015 the Ministry of Communication website in Ghana was attacked by these cybercriminal groups to retrieve relevant information from the government (Darko, 2015).

Online Romance Scam and Sakawa Boys

Online dating romance scams have grown exponentially in Ghana over the past several years (Baylon & Antwi-Boasiako, 2016; Cassiman, 2019; Warner, 2011). This form of online scam is being perpetuated individually and in a group format (Warner, 2011). Duah and Kwabena (2015) estimated that 90% of the cases of online romance scams involve often poor young men, posing as women to dupe their clients. The Sakawa Boys who are involved in this form of crime are mostly found in slum areas in Ghana such as Nima, Maamobi, Accra New Town, and Mallam Atta (Cassiman, 2019). The Sakawa Boys are also found in other countries, where those based in Ghana coordinate their activities with those overseas. Atta-Asamoah (2009) and Warner (2011) argue specifically that this form of internet-based crime has made Ghana acquire a negative label and international stigma as a hub of internet-based crime.

Online Romance Scam is an advance-fee fraud based on a romantic relationship referred to as "Sweetheart Swindles" (Huang et al., 2015; Kopp et al., 2015), wherein the victim's end goal is to be in a trusted and committed relationship (Whitty, 2015). In this type of internet-based crime, the cybercriminal contacts the victim via online dating sites or social network websites by creating a fake profile with a deceptive photograph to attract and target more potential victims (Kopp et al., 2015). Once the scammer contacts the victim, he tries to establish rapport and connection to build

trust, confidence, and a romantic relationship with the victim (Barnor et al., 2020). After the connection has been established, the scammer develops an alternative mode of communication with the victim by using email and instant messenger outside of the dating website (Kopp et al., 2015). Kopp et al. (2015) posit that using an external channel of communication shows that the scammer may want to continue and maintain the rapport that he had built with the victim, even if the fake profile he created on the dating site got suspended. The scammer continues to develop a channel to contact the victim directly in the form of direct calls or emails, and this is done to cement the fake romantic relationship (Kopp et al., 2015). As the romantic relationship develops, the scammer proceeds to ask the victim for smaller gifts such as phones, laptops, and cameras. If these requests are successful, then the scammer continues to request large sums of money (Buchanan & Whitty, 2014; Kopp et al., 2015). Kopp et al. (2015) and Whitty and Buchanan (2016) emphasize that this mode of operation happens successfully when the scammer introduces a reasonable story of emergency that the victim would believe, causing them to send money swiftly. The scammer creates an emergency story that seems reasonable to the victim, for example, that he has been involved in an accident and money is needed to pay medical bills. The swindler could also ask for money to purchase a ticket to visit the victim (Kopp et al., 2015; Whitty & Buchanan, 2016). Sometimes the scammer promises the victim that he will pay the money back when he comes over to join him/her overseas, but this never materializes. In a study conducted by Ennin and Mensah (2018), one of the Sakawa Boys stated that they get in contact with other scammers who are in other countries with the aim to gaining access to internationally based dating sites. This is because these sites require the use of credit card information, which is almost hard to obtain in Ghana. Some of these sites include ChristianMingle.com, seniorpeoplemeet.com, blackpeoplesmeet.com, match.com, flirt.com, etc. In Ennin and Mensah's (2018) study, the

Sakawa Boy also mentioned that due to the difficulty of getting access to credit card information in Ghana, sometimes they contact other Sakawa Boys outside the country to help them with the registration and creation of a profile on these dating sites.

Studies show that the online romance scam does not only involve an individual, but also a group of cybercriminals with loosely organized networks who are active and found in several countries (Alhassan & Ridwan, 2021; Atta-Asamoah, 2009; Baylon & Antwi- Boasiako, 2016). These cybercriminal groups in Ghana also use various strategies to hack into government institutions and businesses (Diaspora Community, 2018). For example, in 2018 these cybercriminal groups hacked into Universal Merchant Bank (a financial institution in Ghana) and stole about GHC 326M (The Finders Newspaper, 2018). A report provided by the Cyber Crime Unit under the Criminal Investigation Department of the Ghana Police Service indicates that most of these cybercriminal groups are found in Ghana, and they collaborate with other Ghanaian cyber criminals overseas (Nyaaba, 2019). The report further indicates that these cybercriminal groups partner and target local banks, public institutions, commercial network providers, and other private organizations (Nyaaba, 2019). As a result, this has put the Ghana government's cyber security at risk.

Chapter Four

Cybercrime: Organization, Growth, and the Challenges on Ghanaian Society

Introduction

Cybercrime, especially internet-based crimes, pose a serious challenge to Ghanaian society. These internet-based crimes, particularly online romance scams, have become a prevalent type of cybercrime that serves as a threat to the government of Ghana and the civil population (Alhassan & Ridwan, 2021; Cassiman, 2019). This chapter first reviews how the activities of the perpetrators (Sakawa Boys) of online romance scams are organized. Second, the chapter focuses specifically on discussing online romance scams as a prominent form of cybercrime that has grown exponentially in Ghana. Finally, it examines the challenges “Sakawa Boys” and online romance scams create in society.

How “Sakawa Boys” Organize their Activities

Sakawa Boys use various methods in getting their victims both locally and internationally (Ninson, 2017). Many of these internet fraudsters patronize cyber cafes, browsing the internet all night, sending scam mails to unsuspecting victims who are seeking romantic relationships on the internet (Cassiman, 2019). In online romance scams, the Sakawa Boys mostly coordinate their activities to target both local and foreign individuals, especially females who are looking for spouses via the internet (Ennin & Mensah, 2018; Whitty & Buchanan, 2016). Even though some of these scammers operate individually, they normally are involved in a group working together to achieve their goal (Ennin, 2015). Some of the Sakawa Boys work with people in Ghana and overseas to share ideas and information that are relevant to their operation (Ennin & Mensah,

2018). The Sakawa Boys form local and international networks with the purpose of acquiring more knowledge and skills when they are having difficulty in succeeding in their operation (Alhassan & Ridwan, 2021). This form of criminal network is not regarded as a formal organized criminal group because they do not have rules that governs them, even though they coordinate their activities (Penn, 2015)

In an empirical study conducted by Ennin and Mensah (2018) on Sakawa Boys, some of the participants shared that they organize their activities by forming local and international networks. The first participant indicated that he does not have friends outside the country, however, he has a lot of friends in Ghana with whom he shares ideas. He further stated that when he encounters potential victims who are difficult to scam, he gets in touch with some local contacts to discuss it, and then proceeds from there. The second participant also stated that the practice of online romance scam has helped some of his friends to travel to Europe and America. Those overseas are able to disclose people's bank statements and credit card top-up (popularly known as "cc top-up"). With this information, the Sakawa Boys are able to steal money from people's accounts without their knowledge. He also stated that they depend on their friends outside Ghana for people's credit card details, as it is easy to acquire such information overseas. On the contrary, the last participant stated that the people who normally give out the credit card information are from Vietnam. He mentioned that the abettors in Vietnam charge them before they divulge the information. He then claimed that a colleague internet fraudster in Vietnam does not accept Ghana's currency because the software to facilitate the acquisition of the credit card information can only be bought in US dollars. After the fraudsters in Vietnam send the software to the Sakawa Boys, the Sakawa Boys then send payment. Evidence shows that the Sakawa Boys organize their activities by connecting with other friends or colleagues with whom they share the same interest.

Even though they operate locally, Sakawa Boys receive support from outside the country to enable them to operate effectively. This is partly confirmed in a news media reported online on a Sakawa Boy who worked with a friend based in the U.S. to defraud victims. These Sakawa Boys organized their activities by sharing information with each other. The one who resided in the U.S. stole people's private information and shared it with the fraudster in Ghana to file for unemployment benefits. After a successful fraudulent operation, the U.S. fraudster refused to give even a penny of the gains to his colleague in Ghana. This triggered the Sakawa Boy in Ghana to alert the FBI about the illegal operation, which led to the incarceration of both parties (Ikeji, 2021). With easy access to internet connectivity in Ghana (Baylon & Antwi-Boasiako, 2016), these cybercriminal groups are able to communicate and contact each other to share information and ideas that help them to effectively target individuals and institutions both in Ghana and abroad.

Online Romance Scam in Ghana

As discussed in the previous chapter on the various forms of cybercrime in Ghana, online romance scam is the most prevalent form of cybercrime and has grown exponentially in the country (Alhassan & Ridwan, 2021; Barnor et al., 2020; Cassiman, 2019). This form of crime is also known as "Sweetheart Swindles" (Whitty & Buchanan, 2019). One of the unique features of an online romance scam is that the potential victim is driven by the quest for a romantic relationship (Offei et al., 2020). The romantic relationship distinguishes online romance scams, or romance fraud, from any other form of internet-based crime, and therefore demands special attention (Cross, 2018). In this form of internet scam, perpetrators (i.e., Sakawa Boys) operate as individuals and often as groups (Duah & Kwabena, 2015). These cybercriminals work in loosely connected groups of friends and depend on each other for knowledge and ideas on the inner workings of these

schemes and offer additional support when frauds become more complicated (Beek, 2018). Online romance scams emerged in the early 2000s with the advent of online dating sites. Since then, the format has become more diversified, targeting both women and men on various dating sites (Barnor et al., 2020). Since the 2010s, online romance scams are among the most prevalent and prolific of online criminal activity (Barnor et al., 2020; Beek, 2018). Communication with victims is done through emails, calling with fake European numbers and instant messaging on various dating platforms (Beek, 2018). The cybercriminals fabricate stories to convince their potential victim to trust them (Kopp et al., 2015). Oftentimes, when the scammers encounter difficulties in duping their victims, they pass the victims on to their colleague scammers to proceed with the storyline (Kopp et al., 2015). In the process of scamming, one scammer establishes contact with the victim via email while another handles phone calls (Whitty & Buchanan, 2016; Beek, 2018). Online dating platforms have become an important medium for both men and women to search for a partner. This type of internet scam remains largely invisible because victims feel ashamed and do not report it (Barnor et al., 2020). Sakawa Boys use the promise of love or romance to entice and manipulate online victims (Beek, 2018). Perpetrators browse the internet in search of victims, often finding them in chat rooms, on dating sites and even within social media networks (Cassiman, 2019; Beek, 2018). These cybercriminals seduce victims with small gifts, poetry, claims of common interest or the promise of constant companionship. Once the scammer gains the trust of the victim, he then begins requesting money, asking the victim to receive packages, or seeking other favors (Beek, 2018). This crime not only affects victims financially but also emotionally and mentally (Ninson, 2017; Whitty & Buchanan, 2016)

In an ethnographic study conducted by Beek (2018), one Sakawa Boy named Seidu narrated that he has signed up for more than fifty online dating sites, including American, German, Chinese, and Lithuanian sites, as well as Indian matrimonial sites. He claimed to have written more than 1,000 emails and had several hundred targets. Seidu searched for people that fit a certain profile, mostly older women. He further stated that the main commonality among these women seemed to be that they desperately longed for an affectionate relationship, either because they had never had one or had experienced failed relationships. He also indicated that sometimes he contacts friends to assist him with drafting a storyline that would gain the trust from his potential victims. Seidu continues to use this format to defraud victims who reside both in Ghana and overseas.

According to Ennin's (2015) study, one participant named Ama elucidated how she got herself involved with an online romance scam and was swindled by these Sakawa Boys. She explained that it all happened when she received a message on her dating profile account from a man called Julius living abroad. She read the message and the person wrote, "O you are beautiful, responsible and you don't look like the classic girls in the U.K." (p. 125). On that day, Ama chatted with him for a while and then she logged out. The next day, Julius requested Ama's phone number. Initially, she did not want to give her number to him but upon further appeal, she gave in. According to Ama, they became friends for almost three months and then Julius expressed his desire to marry her. Ama accepted the proposal although they had not met physically. Julius introduced her on phone to one of his uncles who resided in Accra. The uncle used to call Ama and even promised to visit her at home. After Julius won Ama's trust, he took the opportunity to initiate a business proposal. One day, Ama received a call from Julius that he wanted to ship some items, including three accident vehicles and other home appliances, to Ghana. However, the price of the freight was quite expensive, so he implored Ama to help him finance the shipment process.

Fortunately for him, Ama had just received two years' salary and so she agreed to help. He promised to pay her back and share the profit that would be accrued from selling the shipment. Also, he registered one of the vehicles in her name as part of his commitment towards their relationship. Ama was convinced that Julius was a nice man, so she transferred \$1800 into his foreign account. The next day, she was trying to find out whether he had received the money, but his phone was switched off. She further sent him an email and Facebook messages and yet he did not respond. She called his uncle's phone number and it was also off. She narrated this story to her friend, Agnes, who told her she had been scammed. Subsequent investigation proved that all the emails, text messages, and the phone numbers sent by Julius were initiated from Ghana, while the culprit claimed to be in the United Kingdom. Sadly, all the police efforts to arrest Julius and his accomplice proved futile.

Online romance scam is an emotionally devastating type of fraud because dating websites allow fraudsters to cast their nets wider and disappear more easily than other forms of internet scams (Beek, 2018; Whitty & Buchanan, 2016). The romance component of the online scam acts as an inducement to lure the victim. In the narrative above, Ama succumbed to the perpetrator's financial request after Julius proposed to her. This form of internet-based crime poses a lot of challenges to individuals and the government, as it is difficult to trace these cybercriminal groups and their activities.

Challenges Imposed by Cybercriminal Activities on Ghanaian Society

The increasing practice of internet-based crimes in Ghana, especially online romance scam, has posed many challenges to individuals, government, and organizations (Baylon & Antwi-Boasiako, 2016; Duah & Kwabena, 2015). The high incidence of internet scams has caused Ghana to lose a whopping \$229.9 million between 2016 and August 2018 (Allotey, 2018, p. 1). According

to the Head of the Cybercrime Unit of the Criminal Investigation Department (CID) of the Ghana Police Service, Dr. Herbert Gustave Yankson, in 2020, the Sakawa Boys succeeded in stealing \$19.8 million (Daily Guide, 2021, p. 1). The victims who lost this money include individuals, government institutions, and corporate bodies.

Challenges to Individual Victims

The harm suffered by individual victims of internet scams goes beyond just the financial loss (Ninson, 2017; Whitty & Buchanan, 2016). Ninson (2017) and Whitty and Buchanan (2016) assert that some of these individual victims experience physical harm, as well as emotional and psychological trauma. In Whitty and Buchanan's (2016) study, most participants who were victims of online romance scams disclosed that they suffered a range of emotions, including shame, embarrassment, shock, anger, worry and stress. Some victims also experience other psychological impacts such as fear and feelings of being mentally derailed. Ninson (2017) mentions that some individual victims even go to the extent of imposing self-injury and committing suicide. These are some of the studies that demonstrate the implications of internet-based crimes, particularly online romance scams, on individual victims. On the other hand, there is also the need to analyse the challenges this form of internet scam imposes on the government and corporate institutions.

Challenges to the Government and Corporate Institutions

The government of Ghana has experienced setbacks as a result of the high rate of internet-based crime activities in the country (Duah & Kwabena, 2015). Ghana is ranked as second in Africa and seventh in the world with regard to the number of cases of internet-based crimes (Baylon & Antwi-Boasiako, 2016; Duah & Kwabena, 2015). One of the negative impacts of this form of crime is the loss of credibility for institutions such as Banks and state-owned businesses

and poor reputation for the country (Ninson, 2017). Ghana and other African countries have been blacklisted from credit card transactions with the Western world because the latter are not able to distinguish between fraudulent and genuine credit card transactions with these African countries (Ninson, 2017). This negative impact informs the difficulty Ghana faces in competing in Western markets with its locally manufactured products. Also, many Western businesses are careful when investing and engaging with Ghanaian companies in business deals because of the high incidence of “Sakawa” activities in the country (Duah & Kwabena, 2015). The lack of investment by foreign investors in Ghanaian companies shows that the government is losing a lot of potential revenue especially from the private sector (Ninson, 2017). In other words, the high incidence of internet-based crimes has drained the country and private businesses of huge amounts of potential money that could have been attained from foreign investment and international trade. This is owing to foreign investors’ fear and limited confidence in investing and trading with the country.

Apart from the financial loss and lack of investment in the economy as stated above, the major challenge of this form of crime is that it affects the development of the country (Duah & Kwabena, 2015; Ninson, 2017). The human resource potential of the country is being reduced because most people who are involved in these internet frauds are youth (Alhassan & Ridwan, 2021). These youths do not acquire the relevant education and skills needed for an honest job, as they partake in online scams to meet their daily needs and to support their families (Ninson, 2017). As a result, the government of Ghana has channelled the scarce resources of the country to combat these forms of crime. For instance, in 2021, the Ministry of Communication and Digitalisation committed about GH¢ 131, 626, 912.71, which is equivalent to \$17 million US, to combat cybercrime activities and digitalize the economy in the country (Ministry of Communications and Digitalisation, 2022, p. 3). Meanwhile, these resources could have been used for other

infrastructure development. Due to the challenges caused by cybercriminal groups and their activities on Ghanaian society, the government has developed numerous traditional policing strategies to combat crime. These traditional policing strategies are discussed in the next section of this paper to elucidate the ineffectiveness of these approaches.

Chapter Five

A Critique of the Traditional Policing of Cybercrimes in Ghana

Introduction

In the context of this paper, policing is defined as the totality of government policies, structures, and institutions used to organize and promote conformity to the social order and dominant norms (Kempa, 2010; Neocleous, 2000). This heterodox conception of policing is different from its common usage in traditional criminology (Loader, 2006; Reiner, 1988). This section argues for the non-traditional approach to policing – i.e., the Human Security framework – as an alternative to traditional policing methods adopted by the government to curb this form of crime. Human Security reflects the non-traditional form of policing best articulated in the works of Kempa (2008, 2010) and Neocleous (1998, 2000, 2008). First, this section discusses the traditional policing strategies against cybercrimes in Ghana and demonstrates that these strategies are considered repressive and reactive, therefore limiting the effectiveness of policing cybercrime. Finally, this section analyzes how the Human Security framework could be adopted as an alternative non-traditional form of policing to curb cybercrime.

Traditional Policing Strategies Against Cybercrime in Ghana

The government of Ghana has deployed various traditional policing strategies to control cybercrime, especially online romance scams (Ennin & Mensah, 2019; Baylon & Antwi-Boasiako, 2016). The government relies on the police force and other state institutions such as the Economic and Organized Crime Office (EOCO), Bureau of National Investigation (BNI), National Security Council Secretariat (NSCS) and the Ministry of Communication and Digitalisation to combat the incidence of cybercrime in the country. These institutions and the Criminal Investigation Department (CID) of the Ghana Police Service have been authorized to investigate and prosecute

cybercrime perpetrators (Apau & Koranteng, 2020). Other Acts such as the Electronic Transaction Act (ETA), Data Protection Act (DPA), National Information Technology Act (NITA), the Criminal Code Act 29/60 section 131 and the Cybersecurity Act 1038 have been enacted to regulate the incidence of cybercrime (Ennin & Mensah, 2019; Eboibi, 2020; Ministry of Communication and Digitalisation, 2020). In addition to these strategies, the government has also established the Ghana National Cyber Security Policy and Strategy (NCSPS) and Cyber Security Awareness Month with the purpose of intensifying capacity building and enhancing awareness of cybercrime in the country (Ministry of Communication, 2015). However, several studies have argued that these traditional policing methods have not been able to control this form of crime (Baylon & Antwi-Boasiako, 2016; Eboibi, 2020; Mohammed et al., 2019). The following sections discuss the traditional policing strategies mentioned above in further detail to explore how they are being deployed to police cybercrimes in Ghana.

Electronic Transaction Act (Act 772)

The threat of cybercrime, especially online romance scams, in Ghana has compelled the government to enact laws to regulate activities in cyberspace. One of the legislative Acts that has been enacted is the Electronic Transaction Act (Electronic Transaction Act, 2008). The government of Ghana enacted the Electronic Transaction Act in December 2008 to secure cyberspace as a means to alleviate cybercrime incidence on the internet (Electronic Transaction Act, 2008). The purpose of this Act is to regulate electronic communications and its related transactions in the interest of the public. The Act secures and regulate all electronic activities of the public and private bodies, institutions, and citizens of the country (Electronic Transaction Act, 2008). The Act also empowers the security agencies, especially the Police Service, to seize computers, electronic records, documents, and programs if it is believed that an offense has been

or about to be committed (Electronic Transaction Act, 2008). The Act was enacted to illegalize computer hacking and pave the way for the appropriate agencies, such as the Bureau of National Investigations (BNI) and the Cyber Security Authority (CSA) to deal decisively with suspected cybercriminals in the country. Despite the enactment of this Act to secure and regulate activities in cyberspace, cybercriminals continue to hack into government and corporate websites. For instance, in 2015, Ghana's official government websites were hacked by cybercriminals along with other corporate institutions websites (Owusu, 2015). These cybercriminals hacked into these websites and stole information that is useful for the government in transacting business electronically (Owusu, 2015). This evidence shows that the implementation of the Electronic Transaction Act serves as a reactive strategy that limits the effectiveness of policing these cybercriminal activities.

Data Protection Act (Act 843)

The Data Protection Act was enacted and passed by the Ghanaian parliament in May 2012 to improve legal certainty and transparency in cyberspace (Data Protection Act, 2012). The Act was also enacted to protect individual privacy and personal data by regulating the processing of personal information (Data Protection Act, 2012). The Data Protection Commission (DPC) is an independent statutory body that is established under the Data Protection Act with the mandate to protect the privacy of individual and personal data by regulating the processing of personal information (Data Protection Act, 2012). The commission provides “the process to obtain, hold, use or disclose personal information” (p. 5). The DCP aims to:

Implement and monitor compliance with the provisions of this Act; make the administrative arrangements it considers appropriate for the discharge of its duties; investigate any complaint under this Act and determine it in the manner the commission

considers fair; and keep and maintain the Data Protection register. (Data Protection Act, 2012, p. 6)

Some of the personal data that the commission aims to protect include names, photos, bank account details, IP addresses of personal computers, and biometric data (Data Protection Act, 2012).

This commission was established to protect personal data from the threat of being retrieved by cybercriminals but one of the limitations of this Act is that it does not include the protection of personal data that are held in foreign social media sites such as Instagram, Twitter, and Facebook. Ennin (2015) stated that some of the Sakawa Boys use these foreign sites to retrieve personal information such as names, photos, etc., from their potential victims. According to Dr. Herbert Gustave Yankson, the Head of the Cybercrime Unit of the Criminal Investigation Department (CID) of the Ghana Police Service, these vulnerable victims also disclosed and share their personal information to the public via these foreign social media platforms (Ansah, 2019). This makes it easy for cybercriminals to retrieve personal information from their victims. Further, he stated that the sharing of personal data on social media and online dating platforms makes it difficult for the police to trace the perpetrators. The failure to protect and regulate personal data on foreign social media and online dating platforms by this Act both gives cybercriminals the opportunity to defraud their victims, and limits the ability of Ghanaian policing authorities to control these crimes.

National Information Technology Act (Act 771)

In December 2008, the government of Ghana enacted the National Information Technology Agency Act (National Information Technology Agency Act, 2008). The Act established the National Information Technology Agency (NITA), which has a mandate to regulate Information Communication Technology (National Information Technology Agency Act, 2008). The National

Information Technology Agency has the certification authority to implement and enforce the provision of the Electronic Transaction Act. NITA also has the mandate to manage and protect critical and sensitive data in accordance with clause 30 (1) of the Electronic Transaction Act 2008 (National Information Technology Agency Act, 2008). This Act was enacted with the responsibilities to certify the Agency established under the ETA 2008, issue licenses and ensure fair competition among license holders in the cyberspace, as well as to monitor, enforce, and ensure effective compliance with the conditions contained in licenses and tariffs. Moreover, the responsibility of NITA is to provide the means and technology to protect electronic transactions and reduce electronic tampering and cybercrime incidences (National Information Technology Agency Act, 2008). Despite establishing this Act, Sakawa Boys continue to create false websites every day to defraud innocent people in Ghana and overseas without NITA apprehension and detection (Ennin & Mensah, 2019). Also, Ghana continues to experience fake business transactions and advertisements by cybercriminals on the internet. NITA has been unable to put mechanisms in place to control these criminal activities on the internet, hence, causing many Ghanaian youth to engage in all forms of internet scams including online romance scams.

Criminal Offense Act (Act 29)

Section 131 of the criminal offence Act 29 is also used by law enforcement agencies such as the Ghana Police Service and the judiciary to arrest, investigate, and prosecute internet-based scammers. Section 131 of the criminal offence Act states that:

A person who defrauds any other person by a false pretence commits a second degree felony; a person who by means of a false pretence or by personation obtains or attempts to obtain the consent of another person to part with or transfer the ownership of a thing by a false representation of acting in accordance with the instructions, orders or a request of the

President or member of the Cabinet, commits a second degree felony under subsection (1) and is liable to a term of imprisonment of not less than ten years and not more than twenty-five years despite section 296 of the Criminal and Other Offences (Procedure) Act, 1960 Act 30. (Criminal Offence Act, 29, section 131)

Ennin and Mensah (2019) mentioned that these offences are bailable offences that do not deter scammers from perpetuating such crimes (Ennin & Mensah, 2019). Boateng et al. (2011) argue, in particular, that due to the nature of internet-based crimes, the criminal offense Act section 131 would be thoroughly inappropriate to support charges against cybercriminal groups. Hence, defence lawyers are likely to take advantage of that to acquit their clients. In other words, the criminal offence Act relied on by law enforcement to investigate and prosecute Sakawa is unsuccessful in tackling the nature of online scams activities in the country. The nature of online romance scam activities has been enhanced by Sakawa Boys to include other sophisticated schemes to defraud their victims. The implementation of this act, therefore, limit the ability to control this advanced form of crime.

Ghana National Cyber Security Policy and Strategy (NCSP&S)

The increasingly high rates of cybercrime and the inadequate implementation of laws to control cybercriminal groups compelled the government to initiate Ghana's National Cyber Security Policy and Strategy (NCSP&S) as an institutional policy to combat cybercrime in the country (Ministry of Communication, 2015). In 2015, the Ministry of Communications adopted NCSP&S as a strategy to control cyber fraud and to find ways to implement and enforce the laws on cybercrime (Ministry of Communications, 2015). The objective of this policy is to control cybercriminals who defraud internet users in Ghana. The implementation of this policy was to secure the cyberspace and protect individuals, government, and private corporate bodies from

cyber attacks such as those perpetrated by Sakawa Boys. The cyber security policy therefore addressed cyber risks facing government from attacks on the Critical National Information Infrastructure (CNII). Critical National Information Infrastructure is “defined as those assets (real and virtual), systems and functions that are so essential to the country that their destruction would have a devastating effect on the national economy, reputation, and security” (Ministry of Communication, 2015, p. 19). The policy also “seeks to address the lack of awareness of risks internet users and businesses face doing business in cyberspace” (Ministry of Communication, 2015, p. 22). “The policy also addresses the need to develop technology framework for combating cybercriminals in the country and enhance capacity building for cyber security and experts to make Ghana self-sufficient in the fight against cybercrime” (Ministry of Communication, 2015, p. 22). Despite the implementation of the policy to combat Sakawa activities and its perpetrators, the country continues to record a high incidence of cybercrime (Eboibi, 2020). Eboibi (2020) argues that the implementation of the policy has unfortunately not been able to combat Sakawa activities. He further stated that the failure to tackle this form of crime is attributed to the gaps that align with the implementation of the policy and laws in the country.

The rise of cybercrime has made the government of Ghana put cybercrime laws and institutional policy in place to control cybercriminals including those involved in Sakawa activities. Statistics over the years have shown a consistent increase in the amount of money lost by both individuals and the government to cybercrime in the country. For instance, in 2016, the amount of money lost rose over \$35 million US, while in 2017 this almost doubled, to reach more than \$ 69 million US and \$97 million US in 2018 (Cyber Security and Investigation Bureau, 2019). This evidence shows that the laws and policies implemented by the government such as Electronic Transaction Act (ETA), Data Protection Act (DTA), National Information Technology Act

(NITA), Criminal Offence Act (section 131) and the National Cyber Security Policy and Strategy (NCSP&S) have been unable to effectively tackle the incidence of cybercrime and its perpetrators in the country. Sakawa Boys continue to defraud individual victims and the government in cyberspace because of the failure of traditional policing strategies to adequately control these criminal activities.

Cybersecurity Act (Act 1038)

In December 2020, the government of Ghana passed the Cybersecurity Act to improve Ghana's cybersecurity development (Cybersecurity Act, 2020). In 2020, the Cybersecurity Act was enacted with the purpose of establishing a cybersecurity authority, protecting the critical information infrastructure of the country, regulating cybersecurity activities, and to provide for the protection of children on the internet and developing Ghana's cybersecurity ecosystem (Ministry of Communication and Digitalisation, 2020). The Cybersecurity Authority body has been established under the Cybersecurity Act with a wide mandate aimed at ensuring that Ghana is better protected from cyber-attacks and breaches. The Authority ensures the monitoring of cybersecurity threats within and outside Ghana, taking measures in response to cybersecurity attacks and breaches, especially those with the potential of threatening Ghana's national security, international relations, and economy (Cybersecurity Act, 2020). The Minister of Communication and Digitalisation, Ursula Owusu-Ekuful, has indicated that the Cybersecurity Act is very critical to the economic development of the country and essential for the protection of individual rights within the national digital ecosystem (Ministry of Communication and Digitalisation, 2021). However, despite several laws established to control the threat of cybercrime, cybercrime, especially online romance scams, continues to expand in the country (Duah & Kwabena, 2015; Eboibi, 2020). According to Dr. Herbert Gustav Yankson, the Head of Cybercrime Unit of the

Criminal Investigation Department of Ghana Police Service, in 2020 a total of \$19.8 million US was lost to victims as a result of the activities of cybercriminals in the country (Tenyah-Ayettey, 2021). Further, he stated that there has been an increase (39%) in cybercrime compared to the previous year. He attributed the increase to the Covid-19 pandemic, where more people were doing business transaction online than in person. This evidence reveals that cybercriminals continue to defraud victims on the internet despite the enactment of laws to control Sakawa activities in the country.

The discussion in this paper so far thus demonstrates that government policing strategies adopted to control cybercrime in the country have unfortunately been unsuccessful in tackling the root cause of this form of crime. Hence, it has limited the ability to control the complicated nature of this criminal group. Moreover, these traditional policing strategies are considered reactive and repressive attempts to combat cybercrime in the country. As Hall et al. (1978) argue, specific crime control mechanisms deployed by the state only serve the interest of the powerful, and the defence of propertied individuals, and therefore, must be seen as a repressive way of the state to ignore the crisis faced by the poor and the powerless group. They further argue that the state deploys all the traditional policing strategies to support neoliberal ideology. Therefore, the rapid increase of crime, such as cybercrime, in the midst of the various policing strategies by the state has made critical criminologists argue for a non-traditional policing strategy that is deeply connected to the devastating effects of a country's political economy (Kempa, 2010; Neocleous, 2008). Kempa (2010) argues explicitly that shifting the concept of policing to reflect the realities of the political economy of neoliberal states would be helpful to address contemporary threat to human well-being. The Human Security framework advocates this non-traditional alternative means of policing this form of crime (Kempa, 2010; Neocleous, 2008)

Non-Traditional Form of Policing Strategy

The study of policing has undergone a massive conceptual change over the years (Hall et al., 1978; Neocleous, 2000). Classical criminologists' approach to policing emerged from the "police science" tradition, which focuses on public police institutions as an agency of the state to maintain law and order among individual citizens (Kempa, 2008, 2010). This in turn led both developed and developing countries to invest millions of dollars in state police agencies to improve the performance and effectiveness of state security (Kempa, 2007). The investment in the institutional police force by the developed and developing world is based on the idea that this reflects the population's security and economic needs (Kempa, 2010). However, Kempa (2010) and Neocleous (2000) along with other critical criminologists such as Crowther (2000) and Daleiden (2004) challenged the classical ideology of police science and argue instead that policing geared towards promoting order and human well-being should be the focus of a state. A wider range of policing may better serve the interests of marginalized groups in the world of daily policing and governance because it addresses the economic needs of the marginalized groups in society (Kempa, 2010). The expansive framework of policing was borrowed from the earliest European idea of policing, which uses different mechanisms and social policies to maintain order (Hall et al., 1978; Neocleous, 1998, 2000). Neocleous (1998, 2008) also argues for a broader framework of policing that focuses on the market-driven system of needs –i.e., the economic needs of the people for the conformity of social order and dominant norms. In other words, a broader framework of policing can provide a more holistic approach that seeks to address how better meeting the social, political, and economic needs of individuals may lead them to be more likely to comply with dominant norms and act in accordance with rules, standards and laws. Kempa

(2010) argues specifically therefore that conceptions of policing should go beyond the state institutional force as part of a repressive state apparatus.

Policing is established to ensure the security of the civil population. The concept of security has undergone an extensive rethinking that includes the possibility of going beyond a focus on the protection of state, to include the protection of individual citizens (Neocleous, 2000). Kempa (2010) argues that it is important to go beyond the classical concept of security focused on the national security characterized by institutional police force and military activities. This more narrow security concept has often been used by political scientists and international relations scholars (Kempa, 2000; Neocleous, 2008), but critical security studies have deepened and broadened the concept of security to include individuals' economic, health, and food protection rather than the narrow focus on military and territorial issues typical of security studies (Neocleous, 2000). This led to the adoption of the Human Security framework by critical security studies to challenge the realist paradigm of national security (Neocleous, 2000; United Nations Development Report, 1994).

Human Security as Non-Traditional Policing Strategy

Human Security reflects the non-traditional form of policing that has been articulated in the works of Kempa (2010, 2008) and Neocleous (1998, 2000). Human Security is considered a people-centred alternative way of thinking about public security (Kempa, 2010). It conceptualizes public security more broadly to include ecology of poverty and inequality, which creates different forms of threat to society (Kempa, 2010; Neocleous, 2000). Kempa (2010) argues that Human Security must be at the centre of policing all forms of crime because it takes the welfare of people into consideration. Neocleous (2008) also stated that Human Security provides different ways of thinking about and examining human safety and well-being. Hence, the social and economic well-

being of the people must be the focus of policing. Human Security as a non-traditional policing strategy takes into consideration the economic threats that affect the well-being of the civil population, especially the poor (Neocleous, 1998, 2000). Neocleous (1988, 2000) particularly stated that Human Security—i.e., the welfare of the civil population – must be the government’s focus of policing. Neocleous (2000) specifically termed Human Security as “Social Security” because it provides support for a wide range of needs and protects individuals from the threat of poverty, unemployment, diseases, and crime.

Policing of Cybercrime in Ghana using Human Security Architecture

While traditional policing strategies offer limited solutions to combat cybercrime in Ghana, a deeper look provokes questioning of these traditional methods. These traditional policing strategies have failed to tackle Sakawa activities and cybercriminal groups because of the continual increase of cybercrime incidences in the country. Due to the failure of traditional policing strategies to tackle the root cause of cybercrimes, the Human Security framework, which reflects the non-traditional policing strategy, might be more effectively deployed to effectively control this form of crime. Also, traditional policing strategies have been unable to provide solutions to the cause of this form of crime, which is mainly economic and attributed to the country’s adoption of neoliberal policies (i.e., SAP). Therefore, the government might consider more of a Human Security policing strategy that would proactively ensure that poor youth do not need to engage in this form of crime due to the threat of poverty, unemployment, and subsequent loss of income (Kempa, 2010; Neocleous, 2000).

The adoption of neoliberal policies, which encouraged massive retrenchment, deregulation of capital, deregulation of labour, and the introduction of user-fees, took away social services and economic benefits, such as free health care, free education, and daily income from poor youth,

thus leaving them in a state of massive poverty (Ayelazuno, 2014; Ezeonu, 2000). The massive retrenchment and the privatization of state-owned enterprises associated with SAP have also caused high unemployment among poor youth, intensifying their economic insecurity. This economic threat is attributed to adopting the country's neoliberal policies (i.e., SAP), which must be understood as the root cause of cybercrime among poor youth (Obeng-Odoom, 2012), and be addressed thoroughly.

I argue that the government can achieve a meaningful form of policing by focusing on addressing the increase of poverty due to the country's adoption of neoliberal economics. The devastating effects of neoliberal policies in the Global South, particularly Ghana, and the limitations of traditional methods of policing, has made other critical criminologists argue for an extensive framework of policing that is geared towards the political economy of the country to tackle any form of crime (Kempa, 2010; Neocleous, 1998, 2000). To better address the issue of online romance scams, consideration must go deeper to address the security needs, mostly economic, that manifest as poverty and diseases, which affect the Sakawa Boys rather than the state repressive apparatus –i.e., Law enforcement to fight this menace. In the context of this paper, I argue that the Human Security framework can be advocated as a non-traditional form of policing strategy that would better address the security needs of the Sakawa Boys.

The United Nations Development Program (UNDP) espoused the Human Security framework in its Human Development Report of 1994 (United Nations Development Program, 1994). In this report, Human Security was conceptualized as a people-centred alternative way of thinking about public security (UNDP, 1994). It defines public security threats more broadly to highlight destitution and inequality, which create different kinds of threats to society (UNDP, 1994). In this context, the major security threats in society are commonly economic and manifest

as poverty, diseases, and different forms of crime (Reveron & Mahoney-Norris, 2011; Okubo & Shelly, 2011). Otoo (2016) and Alao et al. (2019) argue that the Human Security architecture –i.e., the welfare of the people – must be the hub of any effort to tackle cybercrime in the Global South. The concept of Human Security for developing countries stresses the protection of poor population from the threat of poverty, unemployment, chronic diseases, hunger, crime, political repression, social conflicts, and environmental hazards (UNDP, 1994). Hence, when youth are provided with their means of survival, there is less of a risk that they will engage in cybercrime to meet the same needs.

Using the Human Security approach to fight cybercrime, would mean the government of Ghana working to create an enabling economic environment that would provide sufficient opportunities to sustain the livelihood of those most likely to be otherwise recruited to criminal groups. This environment would create an avenue for poor youth to provide for their most basic needs, thus preventing the quest for survival via criminality. Most poor youth, especially young men who engage in Sakawa activities, often struggle to provide for themselves and their families. Some even drop out of school due to their inability to pay tuition fees. Some poor youth are unable to access health care and pay their medical bills for themselves and their families due to less government intervention to ensure adequate access to healthcare for the poor. The government's ability to create a more enabling economic environment would allow poor youth, especially young men who otherwise may turn to Sakawa, to survive the economic crisis in other less criminal ways.

Unemployment Benefits

One of the economic enabling environments that would help these poor youth, especially young men, meet their most basic needs is for the government to create an unemployment benefit for the poor population. The government should take cues from developed countries such as

Canada, USA, and the UK. For example, in Canada, the government has established an unemployment insurance benefit that helps poor individuals who are unable to find a job or who have lost their jobs through no fault of their own due to shortage of work or seasonal or mass layoffs (Government of Canada, 2021). With the high unemployment situation in Ghana getting worse each day, the introduction of unemployment benefits would provide support for poor youth, hence, reducing their desperation to engage in cybercrime activities as means of survival in the country. As indicated earlier, most of the poor young men who are involved in online romance scam activities are young graduates with creative and technical skills that need to be geared into a more productive venture. However, due to the lack of job opportunities created through the implementation of SAP, these poor young men have no option but to engage in Sakawa activities to take care of themselves and their families. Some of these poor graduates, especially young males, have families that depend on them; however, because of the lack of state intervention in the economy, they share what little they have with their families. As a result, they are forced to become involved in this lucrative venture to meet their basic needs and to support their families' survival.

The introduction of unemployment benefits by the Ghana government would help reduce (control) the poverty crisis experienced by poor youth. Other critical criminologists have indicated that the ability of the government to control the economic threat associated with neoliberal policies is the best approach to promote the conformity to social norms and order in society (Kempa, 2010; Neocleous, 2008). In other words, policing the economic crisis associated with SAP must be at the center to tackle any cybercrime in the country. As Neocleous (2000, 2006) specifically states, the fabrication of economic order must be at the heart of every government to combat any form of crime, especially for the Global South. While the unemployment situation is intolerably high, the establishment of unemployment benefits by the Ghana government would go a long way to secure

the basic needs and daily income for poor youth in the country, thus reducing online romance scams drastically.

Job Creation Opportunities

The plight of poor youth, especially young men, is made worse due to the state's inability to provide socio-economic safety nets for unemployed youth due to the pressure on the government to be fiscally disciplined and to roll back public expenditure (Asante, 2016). Youth unemployment is a very serious phenomenon due to the possible ripple effects it can have on the individual and the state. Nnorom et al. (2015) have indicated that about 250,000 new entrants, who are mainly youth, enter the job market. Most of these new entrants to the workforce are ready, able, and willing to work but cannot find employment opportunities. Currently, Ghana is faced with 12% youth unemployment and more than 50% underemployment, both higher than overall unemployment rates in Sub-Saharan African countries (World Bank, 2020). Despite major investments by both government and private sectors, this challenge of unemployment will intensify if job opportunities remain limited for poor youth. Most of the Sakawa Boys are often poor and have graduated from school with limited job opportunities (Duah & Kwabena, 2015). The inadequate job opportunities encountered by poor youth, especially young men, have forced those with tertiary education to establish the Unemployed Graduates Association of Ghana (UGAG) to pressure the state to intervene in job creation (Amankrah, 2012; Asante, 2016).

In addition, the implementation of the SAP has removed subsidies from education and brought an end to the previously free education instituted by the socialist government of Kwame Nkrumah, a situation that has led many poor young men to drop out of school. The fallout from such a draconian decision forced many young men into Sakawa activities because they could not afford to sustain expenditures on education. The government should take a cue from Western

countries such as the UK, USA, and Canada, as to how they have created employment opportunities for high school and post-secondary students to work during and after school in order to meet their basic needs. For instance, in Canada, the government has introduced paid employment programs (Summer jobs) in organizations such as Walmart, Tim Hortons, McDonald's etc., for students in high school, university and colleges. This employment program provides them with some basic income for their survival (Government of Canada, 2021). Similarly, Ghana's government should introduce a paid hiring program with public and private organizations that can employ most of the poor youth in high school, university, and colleges. These job opportunities would help reduce poverty experienced by most poor graduates in the country. Creating adequate job opportunities for impoverished young people to work during and after school prevents them from developing negative creative skills for survival. Thus, their skills would be directed towards a productive venture. Also, the availability of job opportunities helps poor young men to receive daily income to access health care and food as necessary conditions for security.

Regulation of Labour

The implementation of SAP as a reflection of a neoliberal framework in Ghana encourages the deregulation of labour (Akonor, 2006; IMF, 1998). The World Bank and IMF primarily maintained the objective that the adoption of the deregulation of labour policy would promote economic growth and alleviate poverty (Akonor, 2006; Oduyayo, 2015). However, critics of SAP argue that the implementation of SAP, such as the deregulation of labour, has exacerbated poverty and caused massive retrenchment of civil workers because of the government's aim of reducing expenditure in the public sector (Ezeonu, 2000; Oduyayo, 2015). Oduyayo (2015) notably indicated that the draconian policies in Ghana contributed to 200,000 individuals losing their jobs in the

public sector. This reduced the size of the labour force in formal sector employment to less than 10% because workers who are supposed to work and earn a living in the formal sector has been retrenched (Oduyayo, 2015). As a result, the affected workers desperately began to seek alternative forms of employment to take care of their families and fulfil their financial obligations. Less government intervention to regulate the labour market through SAP made the private sector succeed in relying on cheap labour as an engine to increase their performance and growth. Less regulation of labour encouraged the private sector to pay workers below the minimum wage (Oduyayo, 2015). This affected workers in most significant ways, causing them to struggle to meet even their most basic necessities. This, in turn, pushed poor workers to resort to other forms of crime such as sex work, armed robbery, fraud etc. to survive this economic crisis (Ezeonu & Koku, 2008; Nnorom et al., 2015).

Moreover, studies show that the introduction of SAP in Ghana gave foreign multi-national companies (MNCs) more power to impose minimum wage below the standard labour wage (Akorsu & Cooke, 2011; Baah & Akorsu, 2007). Baah and Akorsu (2007) posit that most developing countries, particularly Ghana, often sacrificed the welfare of their citizens, especially the poor working class, for the economic benefits of MNCs in the form of taxes from Foreign Direct Investment (FDI). This, in turn, affected the labour market in the most significant ways. To address the issue of workers being paid below the minimum wage, the government should regulate and impose a standardized minimum wage to respond to the growing number of needs and challenges faced by poor workers in the country. The goal of imposing a standardized minimum wage is to promote opportunities for the poor working class to obtain decent and productive working conditions and labour relations. The government's regulation of labour would ensure full

access to income earning opportunities in conditions of freedom, equity, security, and human dignity.

Further, it would lead to economic development in which employment, income, and social protection of the poor working-class could be achieved. The government could learn from the Western world, such as Canada, USA, and the UK, who have imposed a standardized minimum wage in the labour market to regulate employee-employer relations. Regulating labour is necessary to provide minimum protection to poor workers who are likely to be exploited by their employers due to the large size of the informal sector and the intense competition for wage employment in the formal sector (Akorsu & Cooke, 2011).

This chapter thus argues that the traditional policing strategies deployed by the government to control the cybercrime menace is overly repressive and reactive and it does not tackle the root cause of the problem. In order for the government to control these crimes, the country's adoption of neoliberal economic policies – i.e., SAP, that gave rise to this form of crime – must be revisited. Also, the government should adopt the Human Security framework as a non-traditional policing strategy to effectively address the economic needs of these criminal groups, as argued by critical criminology scholarship.

Chapter Six

Summary and Conclusion

Cybercrime, especially online romance scams, poses a serious security threat to the Ghana government and individual citizens (Baylon & Antwi-Boasiako, 2016). This has made the government deploy various traditional policing strategies to tackle this form of crime in cyberspace (Ebobi, 2020; Ennin & Mensah, 2019). However, despite these traditional policing strategies, the country continues to record a high and rising rate of cybercrime (Baylon & Antwi-Boasiako, 2016; Eboibi, 2020). The Minister of National Security in Ghana, Kan Dapaah, confirmed that cybercrime has become a major challenge for the country to combat because of the challenges associated with law enforcement agencies (Obeng, 2017). This paper is informed by the limitations of traditional policing strategies deployed by the government to control this form of crime. Critical criminologists have argued that policing that only focuses on the institutionalized police force as part of the repressive state apparatus is an ineffective and inadequate mechanism of addressing any form of crime in a country (Kempa, 2010). Therefore, it is important for the government to rethink their traditional policing strategies of controlling these cybercriminal groups. Moreover, critical scholars have argued for a non-traditional form of policing that should be directed towards the political economy of a country (Kempa, 2010; Neocleous, 1998, 2000). In other words, policing should seek to address the social, political, and economic needs of individuals of a country to conform to the social order and dominant norms. This non-traditional approach provides an effective and holistic way to address the root cause of any form of crime.

Several studies show that the implementation of the Structural Adjustment Program in Ghana has contributed to the rise of this form of crime (Aning, 2007; Appiahene-Gyamfi, 2003; Asante, 2016). Critics of SAP have argued that the Ghanaian neoliberal policies, such as privatization of state-owned enterprises, devaluation of the currency, deregulation of capital and

labour, and the introduction of user-fees, have exacerbated poverty, especially among young men (Ezeonu & Koku, 2008; Oduyayo, 2015; Oduro, 2012). Also, the implementation of SAP led to the massive retrenchment of workers in the public sector, which made workers redundant in society. The removal of subsidies from social services such as healthcare and education made it difficult for poor youth to access these essential services (Oduyayo, 2015; Ezeonu, 2000). These draconian consequences of SAP posed a security threat to poor youth, mostly economic, which manifested as poverty, diseases, and unemployment. Based on these devastating effects of SAP, this paper argues that the policing of cybercrimes must address the fundamental problems of SAP. In other words, the government's traditional policing strategies must be restructured to address the economic needs—i.e., the ecology of poverty, diseases, and unemployment — resulting from the country's adoption of neoliberal economics (SAP). Again, this paper demonstrates that the conception of security must go beyond the usual emphasis on national security threats and the deployment of state repressive apparatus. Rather, security must be conceived more broadly to accommodate other forms of threats to life, especially those of economic nature. This is what the concept of Human Security was developed to address (UNDP, 1994). Combating economic insecurity, therefore lies at the heart of the heterodox policing strategy highlighted by Kempa (2008) and Neocleous (2000). Based on this, this paper argues that no matter how much repressive force the government deploys to tackle the threats posed by Ghanaian cybercriminals at home and abroad, the problem will remain intractable without confronting the economic foundation of this form of crime.

As already demonstrated in this paper, adopting the country's neoliberal agenda has exacerbated an ecology of poverty and unemployment among these impoverished young men. The government's adoption of its traditional policing strategies put state security at its heart rather than

the welfare of individual citizens. However, as stated in this paper, the Human Security framework provides a novel approach to address the social welfare of these criminal groups. The Human Security framework helps prevent poor young men from resorting to cybercrimes to cushion the effects of poverty. Again, the introduction of the Human Security approach addresses the limitations of the traditional way of controlling these criminal groups in the country. The framework also reveals the mechanisms and strategies that provide opportunities for the Sakawa Boys to meet their essential needs. As indicated in this paper, while unemployment and debilitating poverty are intolerably high among this population (Baylon & Antwi-Boasiako, 2016; Eboibi, 2020), there is the need for the government to introduce unemployment benefits for these impoverished young men. The unemployment benefits would provide a daily income for these impoverished young men and help them to avoid the temptation to engage in cybercrime activities for survival. In addition, the government's ability to introduce adequate job opportunities for these poor populations would limit the unemployment issue and reduce debilitating poverty in the country. Regulation of the labour market by the government would offer security to this population, who are already working with the fear of losing their jobs and being exploited by private sector organizations.

As the rate of cybercrime is high in the country (Baylon & Antwi-Boasiako, 2016; Eboibi, 2020), the Human Security approach to policing must be at the centre to tackle the root cause of this form of crime. In other words, for the government to effectively tackle the cybercrime menace, the policing strategy should address the economic consequences that resulted from the country's implementation of SAP. Adopting Human Security as a non-traditional way of policing as best articulated in the works of critical criminologists such as Kempa (2008, 2010) and Neocleous

(1998, 2000), provide an effective strategy for the government to achieve a meaningful form of policing these criminal groups in the country.

References

- Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian Social Sciences*, 13(4) 19- 29. doi:10.3968/9394
- Akonor, K. (2006). *Africa and IMF conditionality: The unevenness of compliance, 1983-2000*. Routledge.
- Akorsu, A. D., & Cooke, F. L. (2011). Labour standards application among Chinese and Indian firms in Ghana: typical or atypical? *The International Journal of Human Resource Management*, 22(13), 2730-2748. doi: 10.1080/09585192.2011.599941
- Alao, D. O., Osah, G., & Adam, E. M. (2019). Unabated cyber terrorism and human security in Nigeria. *Asian Social Science*, 15(11), 1911-2017. doi:10.5539/ass.v15n11p105
- Allotey, G. A. (October 4, 2018). *Ghana loses \$230m to cyber criminals – CID*. CITI newsroom. <https://citinewsroom.com/2018/10/ghana-loses-230m-to-cyber-criminals-cid/>
- Alhassan, A. R. K., & Ridwan, A. (2021). Identity expression—the case of ‘Sakawa’ Boys in Ghana. *Human Arenas*, 1-22. doi:10.1007/s42087-021-00227
- Amankrah, J. Y. (2012). *Youth unemployment in Ghana: Prospects and challenges* (Centre for Policy Analysis Working Paper). Ghana Statistical Service. <http://www.cepa.org.gh/researchpapers/Youth73.pdf>
- Anesa, P. (2020). Lovextortion: Persuasion strategies in romance cybercrime. *Discourse, Context & Media*, 35(1), 1-8. doi: 10.1016/j.dcm.2020.100398
- Aning, K. (2007). Are there emerging West African criminal networks? The case of Ghana. *Global Crime*, 8(3), 193-212. doi: 10.1080/17440570701507729
- Anyinam, C. (1994). Spatial implications of structural adjustment programmes in

- Ghana. *Tijdschrift Voor Economische en Sociale Geografie*, 85(5), 446-460.
<https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-9663.1994.tb00703.x>
- Ansah, M. (May 03, 2019). *Ghana Lost \$105M in 2018 through Cybercrime*. CITI newsroom.
<https://citinewsroom.com/2019/05/ghana-lost-105m-in-2018-through-cybercrime-director/>
- Apau, R., & Koranteng, F. N. (2020). An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy*, 2(1), 299-309
<https://doi.org/10.1016/j.fsisyn.2020.10.002>
- Apusigah, A. A. (2002). *Reconsidering women, development and education in Ghana: Toward critical transformations* [Unpublished doctoral dissertation]. School of Graduate Studies and Research, Queen's University.
- Appiahene-Gyamfi, J. (2003). Urban crime trends and patterns in Ghana: The case of Accra. *Journal of Criminal Justice*, 31(1), 13-23.
<https://reader.elsevier.com/reader/sd/pii/S0047235202001964?token=9D8600AC597D79582217CFDBC3C74192F5FACD51FEEAD01A5554766BE6740A7DF1A01E1860593F267B3684C43D0D1810&originRegion=us-east-1&originCreation=20220330035158>
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759-763. doi: 10.1089/cyber.2010.0307
- Asante, F. (2016). *Ghana in retrospect*. The government of Ghana.
<http://www.ghana.gov.gh/index.php/media-center/features/1234-ghana-in-retrospect>
- Atta-Asamoah, A. (2009). Understanding the West African cyber crime process. *African Security Studies*, 18(4), 105-114. doi: 10.1080/10246029.2009.9627562

- Axworthy, L. (2001). Human security and global governance: Putting people first. *Global Governance*, 7(1),19-23. <https://www.jstor.org/stable/pdf/27800284.pdf>
- Ayelazuno, J. A. (2014). Neoliberalism and growth without development in Ghana: A case for state-led industrialization. *Journal of Asian and African Studies*, 49(1), 80-99.
doi: 10.1177/0021909613478787
- Azindow, Y. (2005, November 2). *Why Ghana opted for SAP*. GhanaWeb.
<http://www.ghanaweb.com/GhanaHomePage/features/Why-Ghana-Opted-For-SAP-93436>
- Baah, A. Y., & Akorsu, A. D. (2007). *Economic growth, labour standards and social equity: The case of Ghana during half a century of Independence*. (Global Labour University Working Paper). Global Labour University. http://www.global-labour-university.org/fileadmin/Papers_Wits_conference_2007/A5/akorsu_paper.pdf
- Baah-Boateng, W. (2004). *Employment policies for sustainable development: The experience of Ghana*. [Paper presented at a National Workshop organized by Government of Ghana/UNDP/ILO]. National Workshop on An Employment Framework for Ghana's Poverty Reduction Strategy, Accra, Ghana.
<https://catalog.ihsn.org/index.php/citations/39411>
- Barnor, J.N.B., Boateng, R., Kolog, E.A., & Afful-Dadzie, A. (2020). *Rationalizing online romance fraud: In the eyes of the offender*. [Paper presentation]. The Americas' Conference on Information Systems.
https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/21
- Baylon, C. & Antwi-Boasiako, A. (2016). *Increasing internet connectivity while combatting*

- cybercrime: Ghana as a case study*. (Centre for International Governance Innovation Paper No. 44). Chatham House.
- https://www.cigionline.org/static/documents/documents/GCIG%20no.44_0.pdf
- Beek, J. (2018). How not to fall in love. In F. Mulhfred (Ed.), *Mistrust: Ethnographic approximations* (pp. 49-69). Dover Publications.
- Benedek, W. (2010). The human security approach to terrorism and organized crime in post-conflict situations. In W. Benedek, C. Daase, V. Dimitrijevic & P. van Duyne (Eds.), *Transnational terrorism, organized crime and peace-building* (pp. 3-16). Palgrave Macmillan.
- Boateng, R., Olumide, L., Isabalija, R.S., Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, 11(2), 85-100.
- <https://www.researchgate.net/profile/Richard-Boateng>
6/publication/265446452_Sakawa_Cybercrime_and_Criminality_in_Ghana/links/54be0c460cf27c8f2814dbb8/Sakawa-Cybercrime-and-Criminality-in-Ghana.pdf
- Bobic, M. (2014). Transnational organised crime and terrorism: Nexus needing a human security framework. *Global Crime*, 15(3-4), 241-258.
- doi: 10.1080/17440572.2014.927327
- Braimah, I., & King, R. S. (2006). Reducing the vulnerability of the youth in terms of employment in Ghana through the ICT sector. *International Journal of Education Using Information and Communication Technology*, 2(3), 23-32. file:///C:/Users/ea17gd/Downloads/article_42242.pdf

- Brody, R.G., Kern, S. and Ogunade, K. (2019). An insider's look at the rise of Nigerian 419 scams. *Journal of Financial Crime*, 29(1), 202-214.
<https://doi.org/10.1108/JFC-12-2019-0162>
- Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261-283.
doi: 10.1080/1068316X.2013.772180
- Burrell, J. (2008). Problematic empowerment: West African internet scams as strategic misrepresentation. *Information Technologies & International Development*, 4(4), 15-30.
<https://itidjournal.org/index.php/itid/article/download/308/308-746-2-PB.pdf>
- Cassiman, A. (2019). Spiders on the world wide web: Cyber trickery and gender fraud among youth in an Accra zongo. *Social Anthropology*, 27(3), 486-500. doi:10.1111/1469-8676.12678
- Cybersecurity Act (2020). *Act 1038*. <https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf>
- Cyber Security and Investigation Bureau. (2019, Nov 4). *Ghana's cyber-security mechanism receives further boost*. <https://e-crimebureau.com/2019/11/04/ghanas-cyber-security-mechanism-receives-further-boost/>
- Criminal Offences Act. (1960). *Act 29*.
<https://www.wipo.int/edocs/lexdocs/laws/en/gh/gh010en.pdf>
- Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice*, 55, 1-12. <https://doi.org/10.1016/j.ijlcj.2018.08.001>

- Crowther, C. (2000). Thinking about the 'underclass': Towards a political economy of policing. *Theoretical Criminology*, 4(2), 149-167. <https://doi.org/10.1177/1362480600004002002>
- Daily Guide Network (February 20, 2021). *Cyber fraudsters stole \$19.8m in 2020*. <https://dailyguidenetwork.com/cyber-fraudsters-stole-19-8m-in-2020/>
- Daleiden, J. R. (2004). A clumsy dance: the political economy of American police and policing. *An International Journal of Police Strategies & Management*, 29(4), 602-624. doi: 10.1108/13639510610711565
- Danaher, K. (1994). *50 years is enough: The case against the World Bank and the international monetary fund*. South End Press.
- Dankelman, I. E. M. (2008). *Gender, climate change and human security lessons from Bangladesh, Ghana and Senegal*. The Women's Environment and Development Organization. <https://repository.ubn.ru.nl/bitstream/handle/2066/72456/72456.pdf>
- Darko, S. (2015, January 21). *Ghana government websites targeted by hackers*. BBC News. <https://www.bbc.com/news/world-africa-30914000>
- Data Protection Act. (2012). *Act 843*. National information technology. <https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf>
- David, B. (1997). The concept of security. *Review of International Studies*, 23(1), 5-26. <file:///C:/Users/ea17gd/Downloads/the-concept-of-security.pdf>
- Duah, F. A., & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences*, 4(1), 22-34. <http://www.ejbss.com/recent.aspx/>

- Eboibi, F. E. (2020). Concerns of cyber criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking cybercrime policy implementation and institutional accountability. *Commonwealth Law Bulletin*, 46(1), 78-109. doi: 10.1080/03050718.2020.1748075
- Electronic Transaction Act. (2008). Act 772. Ministry of commerce.
<https://moc.gov.gh/sites/default/files/downloads/Electronic%20Transactions%20Act%20772.pdf>
- Ennin, D (2015, July). *Cybercrime in Ghana: A Study of offenders, victims and the law*. [Unpublished Master's thesis]. University of Ghana
- Ennin, D. & Mensah, R. O. (2018). Assessing the various opportunities explored by cybercriminals in Accra. *Developing Country Studies*, 8(12), 1-7
<https://d1wqtxts1xzle7.cloudfront.net/61060361/45632-49125-1->
- Ennin, D., & Mensah, R. O. (2019). Cybercrime in Ghana and the reaction of the law. *Journal of Law, Policy and Globalization*, 84, 36-45. doi: 10.7176/JLPG
- Eseadi, C., Ogbonna, C. S., Otu, M. S., & Ede, M. O. (2021). Hello pretty, hello handsome!: Exploring the menace of online dating and romance scam in Africa. In H. C. Choon & S. Adjorlolo (Eds.), *Crime, mental health and the criminal justice system in Africa* (pp. 63-87). Palgrave Macmillan.
- Essamuah, Margaret & Tonah, S. (2004). Coping with urban poverty in Ghana: An analysis of household and individual livelihood strategies in Nima/Accra. *Legon Journal of Sociology*, 1(2), 79-96. https://journals.co.za/doi/pdf/10.10520/AJA08556261_55
- Esson, J. (2015). Escape to victory: Development, youth entrepreneurship and the migration of Ghanaian footballers. *Geoforum*, 64, 47-55.
<https://doi.org/10.1016/j.geoforum.2015.06.005>

- Ezeonu, I. C. (2000). Ghana and Uganda: A reappraisal of the “success story” of market-led development strategy. *Africa Quarterly*, 40(4), 77-118. <https://www.africabib.org/rec.php?RID=230239064>
- Ezeonu, I., & Koku, E. (2008). Crimes of globalization: The feminization of HIV pandemic in Sub-Saharan Africa. *The Global South*, 2(2), 112-129. <https://www.jstor.org/stable/pdf/40339262.pdf>
- Finnan, D. (2015, February 16). *Lack of laws governing cybercrime making Africa a safe haven for cybercriminals*. RFI. <https://www.rfi.fr/en/africa/20150215-lack-laws-governing-cybercrime-making-africa-safe-haven-cybercriminals-interview>
- Foucault, M. (1965). *Madness and civilization* (R. Howard, trans.). Pantheon.
- Foucault, M. (1979). On governmentality. In G. Burchell, C. Gordon & P. Miller (Eds.), *The Foucault effect: Studies in governmentality* (pp. 87-104). University of Chicago Press.
- Fukuda-Parr, S., & Messineo, C. (2012). *Human security: A critical review of the literature*. (Centre for Research on Peace and Development Working Paper No. 11). CRPD. <https://soc.kuleuven.be/crpd/files/working-papers/wp11.pdf>
- Government of Canada (2021). *Employment insurance benefits and leave*. <https://www.canada.ca/en/services/benefits/ei.html>
- Gill, P. (2002). Policing and regulation: What is the difference? *Social & Legal Studies*, 11(4), 523-526. <https://doi.org/10.1177/096466390201100403>
- Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Robert, B. (1978). *Policing the crisis : Mugging, the state, and law and order*. Holmes & Meier
- Hanlon, R. J., & Christie, K. (2016). *Freedom from fear, freedom from want: An introduction to*

- human security*. University of Toronto Press.
- Huang, J., Stringhini, G., & Yong, P. (2014). Quit playing games with my heart: Understanding online dating scams. In S. Dietrich (Ed.), *Detection of intrusions and malware, and vulnerability assessment* (pp. 216-236). Springer.
- Ikeji, L. (2021, February 21). *Ghanaian man calls FBI to report his US based fraudster friend after the friend refused to split money they made from fraudulent activities*. Linda Ikeji's blog. <https://www.lindaikojisblog.com/2021/3/ghanaian-man-calls-fbi-to-report-his-us-based-fraudster-friend-after-the-friend-refused-to-split-money-they-made-from-fraudulent-activities-audio.html>
- International Monetary Fund. (1998). *Ghana—Enhanced structural adjustment facility economic and financial policy framework paper, 1998–2000*.
<http://www.imf.org/external/np/pfp/ghana/ghana0.htm>
- International Telecommunications Union. (2007). *ICT statistics database*. Geneva.
https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-OVW-2007-E09-PDF-E.pdf
- International Telecommunications Union. (2008). *Africa, ICT indicators 2007*. ITU WorldTelecommunication/ICT Indicators Database. Geneva. <https://www.itu.int/pub/D-IND-YB-2007>
- Institute of Statistics, Social and Economic Research (2017). *Only 10% of graduates find jobs after the first year*. <https://www.isser.ug.edu.gh/research-impact/only-10-graduates-find-jobs-after-first-year-%E2%80%93-isser>
- Ismi, A. (2004). *Impoverishing a continent: The World Bank and the IMF in Africa*. Halifax initiative. <http://www.halifaxinitiative.org/updir/ImpoverishingAContinent.pdf>
- Kempa, M. (2008). Conceptualisation et réforme des processus policiers à l'ère de la

- mondialisation : l'économie politique de la sécurité humaine. *Criminologie*, 41(1), 153–175. doi: 10.7202/018423ar
- Kempa, M. (2007). Tracing the diffusion of policing governance models from the British Isles and back again: Some directions for democratic reform in troubled times. *Police Practice and Research*, 8(2), 107-123. , doi: 10.1080/15614260701377604
- Kempa, M. (2010). The Political economy of human security: A conceptual approach to policing studies and reform. In V. Strimelle & F. Vanhamme (Eds.), *Rights and voices: Criminology at the University of Ottawa* (pp. 101-117). University of Ottawa Press.
- Kerr, P., Tow, W. T., & Hanson, M. (2003). The utility of the human security agenda for policy-makers. *Asian Journal of Political Science*, 11(2), 89-114.
doi: 10.1080/02185370308434229
- Kim, W., & Cho, S. K. (2013). Human security in the Korean Peninsula: A case of the north Korean drug trafficking. *Global Economic Review*, 32(3), 23-39.
- Konadu-Agyemang, K. (2001). Structural adjustment programs and housing affordability in Accra, Ghana. *Canadian Geographer*, 45(4), 528-544. doi: 10.1080/12265080308422923
- Konadu-Agyemang, K. (Ed.). (2018). *IMF and World Bank sponsored structural adjustment programs in Africa: Ghana's experience, 1983-1999*. Routledge.
- Kopp, C., Layton, R., Sillitoe, J., & Gondal, I. (2015). The Role of the love stories in romance scams: A Qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, 9(2), 205-217. . doi: 10.5281/zenodo.56227
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81. doi: 10.1080/1097198X.2019.1603527

- Liotta, P. H., & Owen, T. (2006). Why human security. *The Whitehead Journal of Diplomacy and International Relations*, 7(1), 37-54. <http://www.taylorowen.com/Articles/Owen%20and%20Liotta%20-%20Why%20Human%20Security.pdf>
- Lin, L. (2011). *State-centric security and its limitations: The case of transnational organized crime*. (Research Paper No. 156). Research Institute for European and American Studies. <http://rieas.gr/images/rieas156.pdf>
- Loader, I. (2006). Policing, recognition, and belonging. *The Annals of the American Academy of Political and Social Science*, 605(1), 201-221. <https://doi.org/10.1177/0002716206286723>
- Marfo, S. (2013). Human security: A key to a meaningful conflict resolution and development in a ‘New Ghana.’ *Procedia-Social and Behavioral Sciences*, 91, 545-555. doi: 10.1016/j.sbspro.2013.08.453
- Merriam-Webster. (n.d.). Malware. In *Merriam-Webster.com dictionary*. Retrieved March 21, 2022, from <https://www.merriam-webster.com/dictionary/malware>
- Ministry of Communications (2015, July). Ghana national cyber security policy & strategy. Republic of Ghana. https://www.academia.edu/37141183/NATIONAL_CYBER_SECURITY_POLICY_AND_STRATEGY_REPUBLIC_OF_GHANA?pdf
- Ministry of Communication and Digitalisation (2020). *Cybersecurity Act passed to promote & regulate cybersecurity activities*. <https://www.moc.gov.gh/cybersecurity-act-passed-promote-regulate-cybersecurity-activities>
- Ministry of Communication and Digitalisation (2022). *Programme based budget estimates for 2022*. <https://mofep.gov.gh/sites/default/files/pbb-estimates/2022/2022-PBB-MOCD.pdf>

Modern Ghana (2019, May 5). *\$105m lost in 2018 through cybercrime.*

<https://www.modernghana.com/news/930163/105m-lost-in-2018-through-cybercrime-dr-yankso.html>

Modern Ghana (2021, October 18). *Government's payroll is full, use your skills to become entrepreneurs – Finance minister to university graduates.*

<https://www.modernghana.com/news/1111972/governments-payroll-is-full-use-your-skills-to.html>

Mohammed, A. A., Yussuf, A. B., & Saidi, A. M. (2019). Computer human interaction: A blessing or curse for Ghanaian youth? *International Journal of Academic Research in Business and Social Sciences*, 9(3), 884-901. doi: 10.6007/IJARBS/v9-i3/5753

Monsurat, I. (2020). African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the yahoo boys in Ilorin, Nigeria. *International Journal of Cyber Criminology*, 14(1), 300-315.

file:///C:/Users/ea17gd/Downloads/African_Insurance_(Spiritualis.pdf

Moosa, I. A., & Moosa, N. (2019). *Eliminating the IMF: An analysis of the debate to keep, reform or abolish the fund.* Palgrave Macmillan.

MyNewsGH (2021, March 22). *Crime perpetrated by well-resourced gangs – IGP lays out Police combat readiness.* My News Ghana. <https://www.mynewsgh.com/crime-perpetrated-by-well-resourced-gangs-igp-lays-out-police-combat-readiness/>

National Information Technology Agency Act. (2008). *Act 771.* Ministry of communications and digitalisation.

<https://moc.gov.gh/sites/default/files/downloads/National%20Information%20Technology%20Agency%20Act%20771.pdf>

Neocleous, M. (1998). Policing the system of needs: Hegel, political economy, and the police of the market. *History of European Ideas*, 24(1), 43-58. doi: 10.1016/S0191-6599(98)00009-6

Neocleous, M. (2000) *The fabrication of social order: A critical theory of police power*. Pluto Press.

Neocleous, M. (2006). From social to national security: On the fabrication of economic order. *Security Dialogue*, 37(3), 363-384. doi: 10.1177/0967010606069061

Neocleous, M. (2008). *Critique of security*. McGill–Queen’s University Press.

Ninson, C. (2017). *Internet fraud and its socio-economic implications for peace and development of Agona Swedru Ghana*. [Unpublished master’s thesis]. The Institute for Development Studies, University of Cape Coast.
<https://ir.ucc.edu.gh/xmlui/bitstream/handle/123456789/3416/NINSON%202017.pdf?sequence=1&isAllowed=y>

Nnorom, C. C., Oduro, G. Y., & Yahaya, A. B. (2015). The “dog-chain” syndrome: A voluntary and compelling phenomenon among unemployed youth in Ghana. *Journal of Arts and Social Sciences*, 2(1), 1-19.

Nyaaba, F.E. (2019). *Cyber pirates target banks, telecoms in Ghana*. Modern Ghana.
<https://www.modernghana.com/news/941545/cyber-pirates-target-banks-telecoms-in-ghana.html>

Obeng, H. (2017). *Cybercrime, major security threat in Ghana - Kan Dapaah*. Modern Ghana.

<https://www.modernghana.com/news/766530/cybercrime-major-security-threat-in-ghana-kan.html>

Obeng-Odoom, F. (2012). Neoliberalism and the urban economy in Ghana: Urban

unemployment, inequality, and poverty. *Growth and Change*, 43(1), 85-109.

<https://doi.org/10.1111/j.1468-2257.2011.00578.x>

Oberhauser, A. M., & Yeboah, M. A. (2011). Heavy burdens: Gendered livelihood strategies of porters in Accra, Ghana. *Singapore Journal of Tropical Geography*, 32(1), 22-27.

doi:10.1111/j.1467-9493.2011.00417.x

Obiri Yeboah, N. L. (2015). *An Investigation of Youth in Cybercrime in the Ayawaso East*

Constituency of Greater Accra. Retrieved from

<http://ugspace.ug.edu.gh/bitstream/handle/123456789/21698/An%20Investigation%20of%20Youth%20in%20Cybercrime%20in%20the%20Ayawaso%20East%20Constituency%20of%20Greater%20Accra%202015.pdf?sequence=1&isAllowed=y> (Sourced: November

20 2021)

Oduro, G. Y. (2012). "Children of the street": Sexual citizenship and the unprotected lives of Ghanaian street youth. *Comparative Education*, 48(1), 41-56.

doi:10.1080/03050068.2011.637762

Oduro-Frimpong, J. (2011). *Sakawa: On occultic rituals and cyberfraud in Ghanaian popular cinema*. (Media Anthropology Network Working Paper). European Association of Social

Anthropologists. <https://www.easaonline.org/downloads/networks/media/35p.pdf>

Odutayo, A. (2015). *Conditional development: Ghana crippled by structural adjustment*

- programmes*. E-international relations. <http://www.e-ir.info/2015/03/01/conditional-development-ghana-crippled-by-structural-adjustment-programmes/>
- Offei, M., Andoh-Baidoo, F. K., Ayaburi, E. W., & Asamoah, D. (2020). How do individuals justify and rationalize their criminal behaviors in online romance fraud? *Information Systems Frontiers*, 1-17. <https://doi.org/10.1007/s10796-020-10051-2>
- Ofosu-Kusi, Y., & Danso-Wiredu, E. Y. (2014). Neoliberalism and housing provision in Accra, Ghana: The illogic of an over-liberalised housing market. In L. Asuelime, J. Yaro & S. Francis (Eds.), *Selected themes in African development studies* (pp. 95-109). Springer.
- Okubo, S., & Shelly, L. (2011). *Human security, transnational crime and human trafficking: Asian and western perspectives*. Routledge.
- Otoo, K. N. (2015). *Growing informality in Ghana's labour market: How structural adjustment reversed the formalisation process in Ghana*. [Unpublished master's thesis]. Legion Centre for International Affairs and Diplomacy, University of Ghana.
<http://ugspace.ug.edu.gh/handle/123456789/27439>
- Otoo, C. K. (2016). *Breaking the cybersecurity dilemma; Balancing national security and human security in cyberspace*. <http://ugspace.ug.edu.gh/handle/123456789/27439>
- Overa, R. (2007). When men do women's work: Structural adjustment, unemployment and changing gender relations in the informal economy of Accra, Ghana. *Journal of Modern African Studies*, 45(4), 539-563. doi:10.1017/S0022278X0700287X
- Owusu, G. (2005). Small towns in Ghana: Justifications for their promotion under Ghana's decentralisation programme. *African Studies Quarterly*, 8(2), 48-69. <http://www.africa.ufl.edu/asq/v8/v8i2a3.ht>

Owusu, Y.W. (January 01, 2015). *Hackers strike government websites*. Modern Ghana.

<https://www.modernghana.com/news/593852/hackers-strike-govt-websites.html>

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security*, 26(2), 87-102. : <https://www.jstor.org/stable/3092123>

Penn, M. (April 07, 2015). *Organized cyber crime: Comparison of criminal groups in cyberspace*. The cyber defense review. <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136136/organized-cyber-crime-comparison-of-criminal-groups-in-cyberspace/>

Quarshie, H. O., & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering*, 2(6), 98-100. doi: 10.5923/j.computer.20120206.03

Reiner, R. (1988). British criminology and the state. *The British Journal of Criminology*, 28(2), 138-158. : <https://www.jstor.org/stable/23637377>

Reveron, D. S. & Mahoney-Norris, A. K. (2011). *Human security in a borderless world*. Westview Press.

Richards, N. U., & Eboibi, F. E. (2021). African governments and the influence of corruption on the proliferation of cybercrime in Africa: Wherein lies the rule of law? *International Review of Law, Computers & Technology*, 35(2), 131-161. doi:10.1080/13600869.2021.1885105

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet*. Pearson Prentice Hall.

Shannon, J., & Thomas, N. (2005). Human security and cyber-security: Operationalising a policy framework. In R. Broadhurst & P. Grabosky (Eds.), *Cyber-crime: The challenge in Asia* (pp. 328-346) University of Hong Kong Press.

- Singh, J. (2014). Human security: A theoretical analysis. *International Journal of Political Science and Development*, 2(8), 175-179. doi: 10.14662/IJPSD2014.041
- Stuart, H., Chas, C., Tony, J., John, C., & Brian, R. (1978). *Policing the crisis: mugging, the State, and law and order*. Macmillan.
- Tade, O., & Aliyu, I. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, 5(2), 860-875
https://oculbu.primo.exlibrisgroup.com/permalink/01OCUL_BU/p5aakr/cdi_proquest_journals_1032532393
- Tapestry networks (2015). *Cyber Security in Financial Institution*.

<http://www.tapestrynetworks.com/issue./financial>
- Tenyah- Ayettey, L. (February 20, 2021). Cyber fraudsters stole \$19.8m in 2020. Daily guide network. <https://dailyguidenetwork.com/cyber-fraudsters-stole-19-8m-in-2020/>
- The United State Attorney's Office (2021). *Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise*. <https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting>
- Udelue, M. C., & Mathias, B. (2019). Prevalence of cybercrimes among youth in Onitsha South local government area of Anambra state, Nigeria. *International Journal of Health and Social Inquiry*, 5(1), 82-106. file:///C:/Users/ea17gd/Downloads/1024%20(1).pdf
- United Nations Development Programme. (1994). *Human development report*.
http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

- Warner, J. (2011). Understanding cybercrime in Ghana: A view from below. *International Journal of Cyber Criminology*, 5(1), 736-749.
<https://www.ripandscam.com/pdf/Cyber-crime-in-Ghana.pdf>
- Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF): Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science & Management*, 19(1), 39-53. doi: 10.1177/1461355716681810
- Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455. file:///C:/Users/ea17gd/Downloads/Anatomy%20of%20the%20romance%20scam_Whitty_Security%20Journal.pdf
- Whitty, M. T. (2018). 419-It's just a game: Pathways to cyber-fraud criminality emanating from West Africa. *International Journal of Cyber Criminology*, 12(1), 97-114.
doi: 10.5281/zenodo.1467848
- Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, 16(2), 176 -194. doi: 10.1177/1748895815603773
- Whitty, M. T., & Ng, M. (2017). *Literature review for underwear: Understanding West African culture to prevent cybercrimes*. University of Warwick. https://minerva-access.unimelb.edu.au/bitstream/handle/11343/198264/underware_literature_review_whitty.pdf?sequence=1&isAllowed=y
- Winter, J. (2014). Freedom from fear: A new paradigm for human security? *Undercurrent*, 10(3), 37-45.
https://d1wqtxts1xzle7.cloudfront.net/37435891/Undercurrent_article-with-cover-page-v2.pdf?Expires=1648614511&Signature=P-

World Bank (2020, September 29). *Addressing youth unemployment in Ghana needs urgent action, calls new world bank report.* <https://www.worldbank.org/en/news/press-release/2020/09/29/addressing-youth-unemployment-in-ghana-needs-urgent-action#:~:text=Ghana%20is%20faced%20with%2012,if%20job%20opportunities%20remain%20limited.>