PRZESTRZEŃ Społeczna
Social SPACE

The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: a review

Yushawu Abubakari
University of Wrocław
D.S. Słowianka, Pl. Grunwaldzki 26, 50-363 Wrocław, Poland
yushawu.abubakari@uwr.edu.pl

Acknowledgement

I would like to extend my profound gratitude to Professor Mateusz Błaszczyk of the University of Wrocław for his guidance, recommendations, and review during the study.

Abstract

The fast and consistent growth of cybercrime and its socio-economic consequence have received scholarly attention both within organisations, governmental bodies and researchers in academic environment. Cybercrime is well known to have widely affected the economic conditions of organisations, political economies and individuals. The main objective of this study was to systematically review and outline the current state of research on the determiners of cybercrime adaptation, consequences of cybercrime and the hindrances of cybercrime policies in Anglophone West Africa. The database search was done between 20th December 2020 and 9th January 2021. The search was done through three electronic databases, including Scopus, Sage and Google Scholar. According to the eligibility criteria, articles were included if they were written in English and addressed the issue of cybercrime in Anglophone West Africa, and either the consequence or reasons for cybercrime adaptation or the hindrances of cybercrime policies. Included articles were critically read and data was extracted for reporting. The total number of articles included in the study amounted to 24. Out of the 24 articles, 13 addressed the issues of cybercrime consequences, 6 tackled the reasons and 6 addressed the hindrances of cybercrime policies and regulations. The study revealed that cybercrime has micro-, meso- and macroeconomic impacts in West Africa. At the micro level, citizens loses both financial resources and international travel opportunities. E-businesses at the meso level are victimised both financially and reputationally. At the macro level, countries where cybercrime is prevalence experience a reduction in foreign investment, damage of international reputation and financial problems. The review has

also shown that cybercrime perpetrators lose focus in education. The review also revealed that the reason for cybercrime adaptation is associated with economic strains and corruption at the governmental level. Lastly, hindrances of cybercrime policies circulate around corruption, government interference, ineffective implementation of cybercrime laws and inconsistencies in the content of cybercrime policies. Based on the limitations provided in the study, the present author recommends further studies to include articles in different languages. It is also recommended for future potential researchers to study how cybercrime reflects in the lives of perpetrators and their perspectives on the mitigative interventions. The author argues that to further increase the effectiveness of cybercrime mitigation process in Africa, future studies is needed to understand how cybercrime is organised in African societies.

Keywords: cybercrime, cybercrime adaptation, review, cybercrime policy, economic strain, West Africa

1. Introduction

Although individuals, organisations and the global economy have benefited exponentially with the massive development of technology and internet connectivity, the internet has also created a platform for fraudulent activities, including romance scam, identity theft, phishing, cyberbullying and other forms of cybercrimes. The aim of this study is to present the current scientific discussion of the determiners of cybercrime adaptation, impacts of cybercrime and hindrances of the cybercrime policies in Anglophone West Africa. Anglophone West Africa represent the countries in West Africa that adopts English as their lingua franca as a result of their colonial past. However, the data acquired for the analysis in this study covered only Ghana, Nigeria and Sub-Saharan Africa because of factors including the present author's language bias. The study sample included Ghana, Nigeria and Sub-Saharan Africa as a representative sample for Anglophone West Africa. This is because the prevalence of internet fraud in West Africa is centred around the Anglophone West Africa, thus Ghana, Nigeria, Liberia, Sierra Leone, Gambia and part of Cameroon, with Nigeria and Ghana being the hubs (Burrell 2012). Therefore, the study contends that the geographical limitation in this review has a negligible influence on the results of the findings. To achieve the objectives of the study, three questions were asked: (1) What

are the determiners of cybercrime adaptation in West Africa? (2) What consequences does cybercrime have on West African societies? (3) What factors hinders the effective implementation of the cybercrime policies and interventions in West Africa? Many studies have reported the social and economic impacts of cybercrime (Duah, Kwabena, 2015; Lewis 2018), the mitigation strategies (Akuta et al., 2011; Eboibi 2017) and the reasons for indulging in cybercrime (Igwe 2011; Anyanwu, Obiyo, 2012; Dukku 2019; Ogunleye et al., 2019).

The prevalence and the proliferation of cybercrime have received global attention (Lewis 2018). Although the growth of high-speed internet connectivity has played a significant role in cybercrime perpetration in West Africa, especially Ghana and Nigeria, high-speed internet connectivity is not the main catalyst of internet fraud, but rather the liberalism of the digital society is, where users are provided with anonymity, flexibility, and convenience (Rege 2009). The provision of anonymity and flexibility (Rege 2009) coupled with the limited cross-border law enforcement (McCombie et al., 2009) has made cyber environment a rational ground for criminal activities, considering the risk that are involve in the traditional and conventional forms of financial crimes. Criminologists have made substantial contributions and analysis of how rational decisions are considered during crime perpetration. For instance, criminologists, in, terms of rational choice theory, posit that perpetrators analyse the cost and benefit of their crime displacement (Cornish, Clarke, 1987; Paternoster et al., 2017) before undertaken any criminal activity. In other words, cybercrime is growing at a galloping rate because of the more advantages and less disadvantages it offers to perpetrators. It is importance to acknowledge that the inability of law enforcement agencies and personals to make cases against cyber fraudsters is a fuelling trajectory of cyber fraud perpetration (Boateng et al., 2010).

Although there are many other forms of cybercrimes which are not geared towards financial gains, e.g. cybersex, cyberbullying among students and profiling misleading news via WhatsApp, Facebook, Twitter, and other social media platforms, researchers and criminologist focus more on financial related cybercrimes. Financial cybercrimes do not only affect individuals, but also organisations, and transcend to national issues (Duah, Kwabena, 2015; Lewis 2018). In 2018, the global cyber-

crime report estimated that over two billion online users which represented two-thirds of online users have their personal information compromised or stolen for economic gains (Lewis 2018). Financial internet scams can broadly be classified into: (1) technology-oriented internet fraud and (2) interpersonal psychological scam. Whereas technology-oriented scammers use advance technological tools, including hacking technology to steal from their victims, interpersonal psychological scammers use interpersonal relationship to lure the victim into providing them the means to steal from such victims. On the one hand, fake online web clones, cyber hacking, phishing, and malware infiltration are examples of technology-oriented forms of financial cybercrime, while, on the other hand, romance fraud is an example of interpersonal psychological scam.

Deductively, interpersonal psychological scam affects internet users who seek interpersonal relationships online and technology-oriented fraud hacks into organizations' databases to steal. Interpersonal or romance scam is posited to emanate from West Africa, specifically Nigeria (Whitty 2018a). This type of financial scam requires perpetrators to create fake online profiles (Burrell 2012) and use these profiles to establish long-time online romantic relationship with their victims through a series of strategies to gain the trust of their victims, including personal recovery stories (Kopp et al., 2016), persuasive language (Burrell 2008b; Kopp et al., 2016; Shaari et al., 2019) or even sake occultic powers to facilitate the process (Armstrong 2011). M. Whitty's (2015) qualitative analysis of the posts of public online support groups and in-depth interviews with victims revealed that scammers use five steps to manipulate their victims:

> "In Stage 1, the criminal creates an attractive profile to draw in the victim; in Stage 2, the criminal grooms the victim, priming them to send money; in Stage 3, the criminal begins to request funds from the victim (there a four potential trajectories at this stage); in Stage 4, which only a few went through, the victim is sexually abused via cybersex; and finally Stage 5 is the revelation" (ibidem: 443).

The scammers use psychological appeals to obtain the trust of their victims and subsequently demand victims to send money. Victims, having trusted scammers

during this five-stage, do not psychologically suspect the process to be a scam. Meanwhile, it is crucial to note that financial purposely cyber fraud does not only affect individual, and e-business and banks, but has also affected countries and the global economy (Lewis 2018). According to J. Lewis (2018) report on the impact of cybercrime on the global economy, the latter suffered financial resources of 600 bln USD in 2017 alone. As all the mitigation strategies have not significantly tackled internet fraud penetration, the world economy continues to lose billions of dollars to internet fraud. In their survey study in the northern part of Ghana, F. Duah and A. Kwabena (2015) revealed that not only does internet fraud pose banking challenges to e-business, but also has an exponential negative effect on customers willingness to be part of e-banking. Even though the primary objective of financial internet fraud perpetrators is intended towards exploiting financial means from their victims (Buchanan, Whitty, 2014; Green, et al., 2020), several studies have shown that victims are also psychologically, emotionally, and physically affected (Rege 2009; Duah, Kwabena, 2015; Modic, Anderson, 2015; Whitty 2018b; Norris et al., 2019; Green et al., 2020). This poses challenge to both individuals and groups to develop measures that can support in curtailing internet fraud.

Although the international communities have made several attempts to reduce cybercrime globally, cybercrime seems to be positively associated with technology, globalisation, and digital capitalism. As technology and digital capitalism increase, cybercrime continues to increase. Apart from the legal policies created by the international communities to fight cybercrime, West African countries have also formulated some cybercrime policies to that effect. For instance, to tackle cybercrime, the Commission on Crime Prevention and Justice (CCPJ), that was created by the United Nations (UN), has been reinforced with cyber experts to help buttress cyber related crimes in the global economy (Akuta et al., 2011). Also, this policy governs the cyber related issue in West Africa. Additionally, as part of combating cybercrime, the Economic Community of West African States (ECOWAS) formulated cybercrime laws and directives to control cybercrime perpetration in West Africa (Jerome 2019). The ECOWAS was established in West Africa to promote regional and territorial cooperation coupled with integration for the purpose of economic development of

West African states. It was also established to create free trade movement among member countries to enhance international relationship among member states. Nigeria, one of the drivers of West African economy and the hub of cybercrime, formulated the first cybercrime prohibition and prevention Act in 2015 to fight against cyber related crimes (Eboibi 2017). Other laws that are used to fight cybercrime are the Advance Fee Fraud and other fraud related offence Act, 2006, the Criminal Code Act, 2004, Control of International Trade and Traffic Act, 2004, Cyber defamation Law, Evidence Act, and the Criminal procedure Act and Police Act (Olukolu 2019). However, the laws and policies that are used to fight cybercrime in West Africa have yielded little results. The reasons for the ineffectiveness of the cybercrime policies that are presented in the literature is reported in this review.

2. Methods

2.1. Reporting tool

This review is designed to report the current scientific discussion of the social and economic impacts of cybercrime in West Africa and the factors that hinder the effective enforcement and performance of the cybercrime regulations in West Africa. However, the study does not claim to cover all the scholarly and scientific studies on the phenomenon, given the language, geographical, and database coverage limitations. This review is carried out in alignment with the reporting checklist of PRISMA (Prefer Reporting Items for Systematic Reviews and Meta-analysis) that is formulated and recommended for social sciences (Pahlevan-Sharif et al., 2019). S. Pahleva-Sharif et al. (2019) version of PRISMA is designed from A. Liberati et al. (2009) which is suitable for the medical practitioners and researchers. The current study adapted S. Pahlevan-Sharif et al. (2019) version because of its suitability to the current review. Although in this systematic review some of the included articles are quantitative studies, the review does not include meta-analysis. It is important to note that the present author did not register protocol for this review.

2.2. Search criteria and exporting

The review depended on Scopus, Google Scholar and Sage publications to report the phenomenon. Scopus and Sage publications were used in conjunction to acquire authentic and reliable data for the review and to cover missing documents from any of these databases. Also, Google Scholar was employed to acquire more important papers that were useful although not included in either Scopus or Sage publication. The publications that were found during the research covered Ghana, Nigeria, and Sub-Saharan Africa. This is as the results of the language restriction in the search criteria. The search was carried out on 20th December 2020 and 9th January 2021. The database search was performed using titles, abstracts, and keywords. The results were exported to Microsoft Excel for screening and selection. The citation information, abstracts, authors keywords and index keywords were included in the extracted file. This was followed by the screening face.

2.3. Screening

The screening was carried out by the present author alone. Firstly, he used titles, author's names, and abstracts to eliminate duplicates before screening for inclusion and exclusion. During the screening, additional column was created and headed as screening. The author used 0, 1 and 2 to code for exclusion, inclusion, and potential to include articles, respectively. These codes were used for selections the articles for critical reading. At this phase, the author concentrated on codes 1 and 2 to select the final articles that met the eligibility criteria. Another column was created and headed "Selected" where final coding was done. The selection section had two codes, 0 and 1, representing exclude and include, respectively. The selection codes were then used for full text review.

2.4. Exclusion and inclusion criteria

In the Screening process, articles were included if they investigated any part of Anglophone West African, including Ghana, Nigeria, Sierra Leon, Liberia, and English part of Cameroon. If the published paper was conducted in more than one Anglophone West African country, it was included in the study since the focus of the

review was West Africa. Papers were included in the study if they had been published in English. Also, for the purpose of the quality and reliability of the paper, the study was limited to journal articles.

The exclusion criteria were also based on the objectives and focus of the papers that were found during the screening and selection process. Articles or papers were excluded if they examined other areas of cybercrime, e.g. the techniques of romance scam rather than cybercrime policies, impacts of cybercrime, or the reasons for cybercrime adaptation. If a study had examined any of the three objectives in a context different from the Anglophone West African region, such a paper was excluded from the study. For instance, though the study of I. Oleksiewicz (2019) addressed the objectives of the review, it was not, however, contextualised in West Africa, but rather generalised to the whole of Africa. Therefore, I. Oleksiewicz was excluded due to the geographical eligibility criteria.

2.5. Data extraction and synthesis

The data extracted for the analysis included the authors' names, year of publication, location of the research, focus or objective of the study, methods and the findings, and the observable conclusions. All the included articles – qualitative, quantitative and mix methods – were grouped according to the themes presented in the findings and observable conclusions. The articles were grouped in (1) the consequences of internet fraud, (2) the reasons of cybercrime indulgence and (3) the hindrances of the cybercrime regulations and policies. Depending on the themes presented in the findings, it was possible for an article to be grouped into more than one theme. For instance, in this study, F. Eboibi's study was categorised into the consequences of internet fraud in Anglophone West African and the hindrances of cybercrime regulations and policies (Eboibi 2017).

3. Findings

3.1. Publication coverage

The study conducted the search through Scopus, Sage Publications, and Google Scholar. The search was carried out on two dates, as presented in table 1. On

Scopus, Google Scholar, and Sage databases, 293, 36 and 63 articles were found, respectively. The number of articles that were found during the search covered publications between 1998 to 2021 (cf. Figure 1). Totally, 383 articles were found. Figure 2 illustrates the number of articles from 1998 to 2020. At the initial stage of the screening, 14 duplicates were excluded from the list. In the titles and abstracts screening, 346 articles were further excluded based on the eligibility criteria. Eight additional articles were excluded during the full text critical reading and examination. Therefore, 24 articles were included in the systematic review findings.

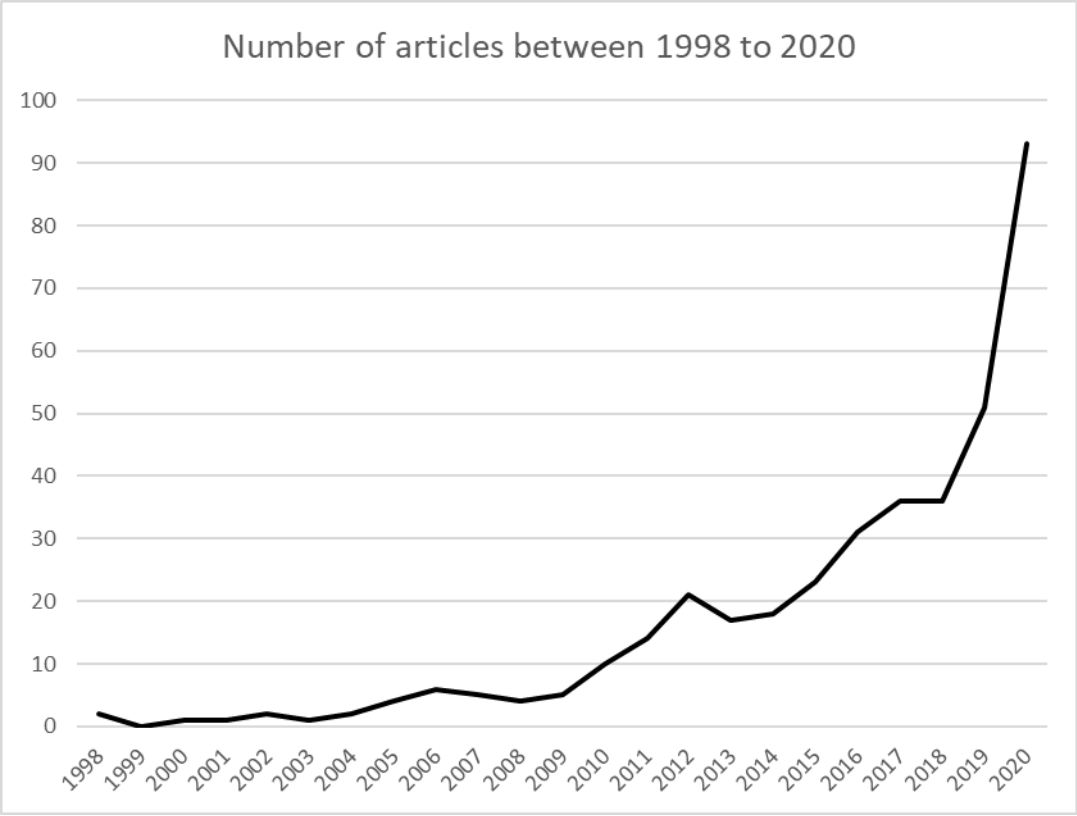

Figure 1. The trend of publication between 1998 and 2020

The graph illustrates the number of articles that were found during the search. The trend at the graph evidences the growing global concern of cybercrime. There is a growing trend of how studies are carried out on internet fraud in the world, especially in West Africa. For instance, from 1998 to 2008, less than 10 articles were found to be published each year. This signifies the inception of internet fraud at its youthful

stage. However, from 2010 onwards, the number of studies consistently increased and only experienced a slight declined in 2013.

3.2. Description and characteristics of the included studies

Articles included in the study were categorised into the consequences of internet fraud, reasons for internet fraud adaptation and hindrances of the cybercrime policies. With consequences of internet fraud 13 were allocated, six articles on reasons for cybercrime indulgence, and nine articles on hindrances of cybercrime regulations and policies.

The studies are centred around Nigeria, Ghana, and Sub-Saharan Africa (Table 1). Most of the articles are carried out in Nigeria, illustrating three quarter of the total amount of the articles.

Table 1. Included article based on location

Location	Number of articles	Percent
Ghana	4	16.67
Nigeria	18	75.00
Sub-Saharan Africa	2	8.33
Total	24	100.00

3.3. Determiners of cybercrime perpetration

The social conditions that push individuals and groups in Anglophone West Africa to perpetrate cybercrime encompass economic and financial strains, bad governance, and greed. Out of the six articles included in this review, six studies, including one quantitative ex-post Facto study (Anyanwu, Obiyo, 2012), one exploratory cross-sectional study (Ogunleye et al., 2019), three qualitative studies (Burrell 2011; Igwe 2011; Uzorka et al., 2018), and one mixed methods study (Dukku 2019) revealed that the socioeconomic deprivation or poverty and unemployment are major determiners of cybercrime adaptation in Anglophone West Africa. However, one article accounted that though poverty and unemployment compliment the individual's propensity

to engage in cybercrime, the main determiner is the frustration that comes with people's inability to find jobs or satisfy their economic conditions (Anyanwu, Obiyo, 2012). Internet fraud adaptation in the West African region can be substantiated in terms of the classical strain theories of crime (Merton 1938; Cohen 1955). These theories postulate that crime adaptation is emanated from a person's inability to satisfy their financial and economic needs or obtain a middle-class status. To escape the economic deprivation, the youth find resilience in cybercrime.

Another factor that informs perpetrators' decision to undertake internet fraud is the perceive neglect and corruption in the region. For example, two studies in Ghana and Nigeria by J. Burrell (2011) and C. Igwe (2011), respectively, revealed that government neglect of underprivileged communities and corruption subject people or young adults to perpetuate cybercrimes. Further, M. Uzorka's et al. (2018) recent findings revealed that young people's desire for wealth is the determiner of internet fraud perpetration.

3.4. Consequences of cybercrime

Among the 13 studies that revealed the impacts of cybercrime in the Anglophone West Africa, some of them present micro level consequence, others revealed meso level implications, and some – macro sociological impacts. Whereas six of the articles were qualitative studies (Viosca et al., 2004; Tettey 2008; Eboibi 2017; Enoghomwanse 2019; Olukolu, 2019; Chiluwa et al., 2020), four studies were quantitative (Longe, Chiemeke, 2008; Apau, Koranteng, 2019; Evans, 2019; Aribake, Aji, 2020), and three were mixed methods design (Ojedokun, Eraye, 2012; Ebenezer et al., 2016; Dukku 2019).

At the micro level, I. Chiluwa et al. (2020) revealed that cybercrime defraud individuals, causing victims financial losses. Also due to the security endangerment of cybercrime in the region (Eboibi 2017) most e-business are forced to liquidate, subjecting employees of such institutions to unemployment (Enoghomwanse 2019). The micro societal consequences of cybercrime are presented on how citizens of these countries are limited in benefiting international opportunities. M. Dukku (2019) re-

vealed that due to the prevalence of internet fraud in Nigeria, most Nigerians seeking opportunities abroad are denied the chance.

Cybercrime at the meso economic and social level has affected e-businesses in diverse ways. Two studies revealed that because of the security threats of cybercrime, customers have lost trust in undertaken e-banking, leading to a decline in e-business operations in the region (Apau, Koranteng, 2019; Dukku 2019; Aribake, Aji, 2020). A. Enoghomwanse (2019) study showed that some of this e-businesses are liquidated and hence leading to other economic challenges. Not only do this internet fraud and cybercrime perpetration is demonstrated to limiting customers participation in e-businesses and online transactions, cybercrimes in West Africa also discredit e-business by presenting customers with fake and attractive online business model which are intended to further defraud people, as revealed by I. Chiluwa et al. (2020).

Finally, at the macro economic and social implication of cybercrime in Anglophone West Africa, these fraudulent activities have shown to degrade and damage the reputation of the countries they prevail, especially Ghana and Nigeria (Viosca et al., 2004; Longe, Chiemeke, 2008; Tettey, 2008; Dukku 2019; Olukolu 2019). This reputation defect has also many implications on the economic development of the region, including the region's inability to attract foreign investment, policy formation, and international relations. Five studies revealed that the prevalence of internet fraud in Ghana and Nigeria has drastically affected foreign investment in the region (Tettey 2008; Ebenezer et al., 2016; Enoghomwanse 2019; Olukolu 2019). It is also accounted by R. Olukolu that governments in West African countries, especially Ghana and Nigeria, have spent monetary and material resources to enact cybercrime policies (Olukolu 2019), of which such policies and regulations have led to further economic and national challenges, including restrictions on economic growth and international relations (Eboibi 2017).

Conclusively, the article by U. Ojedokun and M. Eraye (2012) revealed that, on the perpetrators' perspective, cybercrime has empowered them with financial stability; however, they exhibit extravagance and irrational expenditures. The study also showed that cybercrime conversely affects the academic performance of students who are perpetrators. J. Burrell (2008a) carried an ethnographic study in Northern

Ghana and concluded by describing internet fraud as a problematic empowerment. In her study, a scammer revealed to have benefited financially from cyber fraud; however, this empowerment on the aspect of the scammer has a negative feedback to the reputation of the country in the international community. Problematic empowerment in that, cybercrime has empowered the scammer with a financial gain but adversely affects the national reputation at large.

3.5. Hinderance of cybercrime policies and regulations

Out of the 24 articles included in the review, six revealed the hindrances significant to describing the reasons associated with the ineffective performance of the cybercrime policies and regulations in Anglophone West Africa. Four of the articles employed qualitative research design (Burrell 2011; Igwe 2011; Uzorka et al., 2018; Ogunleye et al., 2019), one employed quantitative methodology (Hidayanto et al., 2015) and the one by M. Dukku (2019) used mixed methods approach.

Out of the six articles, five showed that there are deficits in the content and the implementation of the cyber regulations and policies. For instance, some states and countries have not successfully implemented the ECOWAS Acts and regulations that are formulated to control cybercrime in its member states (Jerome, Orji, 2019). F. Eboibi (2017) postulated that even countries and states that have implemented such policies did that after the prevalence and escalation of cybercrimes. A. Oriola (2005) and A. Enoghomwansi et al. (2019) in their qualitative analyses of the cybercrime regulatory documents revealed that the content of the cybercrime policies failed to effectively address cybercrimes. A. Oriola (2005) posited that even with the present cybercrime regulations which are not perceived to be consistent and effective to mitigate cybercrime, there is ineffective enforcement of the cybercrime laws.

Three articles provided more evidence to substantiate the findings of A. Oriola. For example, F. Sowunmi et al. (2010) revealed that government interference has contributed to the ineffective enactment of the cybercrime policies by the police and other law enforcement agencies. In their study, they posited that most cybercrime perpetrators shield under the powers and influence of some people in government. These government officials are said to protect perpetrators in case they are

found arrested for fraud. Also, E. Akuta et al. (2011) and J. Tettey (2008) demonstrated that lack of information and communication technology resources and skills for police officers and law enforcement agencies to trace and prosecute cybercrime perpetrators also hinders the implementation of the cybercrime regulations.

4. Discussion

4.1. Discussion of findings

The growing trend of digital capitalism has provided a platform for illegal internet users to indulge in various forms of cybercrimes which has resulted to global economic and social concerns. This review accounted for the socio-political and economic factors that account for the adaptation of cybercrime as a livelihood strategy in the region and the impacts that cybercrime have had on Anglophone West Africa. This systematic review is also among the first on the consequence of internet fraud in Anglophone West Africa. The review further provided the discussion how the cybercrime mitigative policies are hindered by certain political and economic phenomenon. The bibliography search resulted in the selection of 24 articles, where 13 examined the consequences of cybercrime, and six articles each of the themes, determiners of cybercrime and the hindrances of cybercrime policies.

The study reviewed the socio-political factors that account for the adaptation of internet fraud in Ghana, Nigeria, and Sub-Saharan Africa. The socio-economic deprivation of the youth results to the adaptation of internet fraud. Most of the findings circulated around poverty, unemployment, and governmental corruption as the causal factors of cybercrime adaptation (Igwe 2011; Anyanwu, Obiyo, 2012; Dukku 2019). However, it is important to mention that economic strains are not the primary reasons that account for the adaptation of internet fraud (Whitty 2018a), but other factors that are related to the strain that people can control. The study by M. Whitty (2018a) in Ghana provided accounts of two people which suggest that youth moral decline plays a role in adaptation of internet fraud in the region. In her study, a participant, on the one hand, attributed internet fraud adaptation to the government neglect and their inability to access jobs, and, on the other hand, another participant

noted that though it is difficult to access jobs, he postulated that internet fraud is not legitimate and should not be adapted as a cure to their economic struggle.

From another perspective, the impacts of cybercrime in Anglophone West Africa ranges from the micro to macro societal levels. It affects the individuals at the micro level, organisations at the meso level, and countries at the macro level. Internet fraud causes both individuals, organisations, and West African in general financial losses. Additionally, to financial institutions, including banks and e-businesses, cybercrime has negatively affected customers willingness to undertake bank activities, pushing some financial institutions to back out of business. Internet fraud in the region does not only cause financial losses to both individuals and organisations, but it has also tarnished the national reputation of countries it prevails. Cybercrime has also presented its negative consequence on formal education on the territory. As revealed by U. Ojedokun and M. Eraye (2012), the academic performance of scammers reduces because of their less attention to education after adapting internet fraud. In their study in Nigerian universities, O. Tade and I. Aliyu revealed that scammers at the university level bribe their corrupt lectures to obtain better grades (Tade, Aliyu, 2011). The issue of internet fraud is seen to be affecting the integration of Information and Communication Technology (ICT) in education in the region. A study conducted in the northern part of Ghana revealed how parents rejected social media integration into the Teacher-Parent Communication (TPC) as a results of internet fraud prevalence in the region (Abubakari 2020). The occurrence of internet fraud has demonstrated to have long-time consequences on education in West Africa.

Regarding the hindrances of the cybercrime regulations and policies, the articles included in this study showed that inconsistencies and ineffective consideration of the cybercrime regulations and directives are some of the major challenges of the formally and legally tackling of cybercrime in the region. Also, corruption on the aspect of some of the power holders in governance make cybercrime laws enforcement difficult. Deductively, while insistencies in the content of cybercrime policies, on the one hand, make is difficult for law enforcement agencies to categorise cyber behaviour as a crime, corruption and lack of technological resources and skills are the hinderances to enforce the regulations, on the other hand.

4.2. Limitations and future studies

This systematic review, just as other systematic reviews, is not free from limitations which need to be used to guide future research in the area. Firstly, the current study was limited to articles that were written in English, where important articles that could contribute to widening the understanding of the objectives of the study, but written in other languages, were eliminated. The study areas that were found during the database search included only Ghana, Nigeria, and Sub-Saharan Africa. Therefore, future studies of this sort should be widened to include articles in other languages to cover more articles that could be useful to capture other countries in West Africa.

Secondly, the review was carried out by a single author and this could limit the quality of the screening and selecting of the articles. The study posits that conflict resolution between researchers in systematic review process is important to the quality of the review process. However, since this study was done by a sole researcher, some articles that could be important for the study might have been excluded due to his bias. Future studies should include more students at all levels of the review process.

The papers that were reviewed for the impacts of cybercrime on Anglophone West Africa revealed three broader institutions, i.e. the micro institution (individuals), meso institutions (banks and e-businesses) and macro institutions (the national reputation and economic deficits). However, the evidence of the impact of cybercrime at the micro institutions are insufficiently tackled. Out of the 24 articles that were included in the study, two articles revealed impacts of cybercrime on individuals. While I. Chiluwa et al. (2020) revealed how cybercrime perpetrators use the Ponzi's schemes to discredits e-businesses, the government, and defraud people, U. Ojedokun et al. (2019) presented the impact of internet fraud on the academic achievement of scammers. They also noted that internet fraud empowered scammers economically; however, scammers are said to be extravagant. U. Ojedokun's et al. (2019) study is contrasting to J. Burrell (2011) which showed how a scammer used his monetary gains to establish a legitimate business for himself and stopped scamming. Therefore, the socio-economic status of scammers is well presented in literature.

4.3. Conclusion

This study reviewed the current state of research on the determiners of internet fraud adaptation, impacts of cybercrime and the hindrances of cybercrime policies in West Africa. The literature review revealed that the reasons for indulging in internet fraud perpetration in West Africa ranges from socio-economic deprivation of underdeveloped and marginalised societies and corruption at the governmental level. The current state of art also showed that cybercrime has damaged the reputation of West African states and causes financial lost to both individuals and e-businesses. Lastly, studies have outlined that, inconsistencies, corruption, and lack of technological resources are the impediments of cybercrime policies in Anglophone West Africa. Based on the determiners of internet fraud adaptation, there is a need for further studies to investigate the sociological implication of cybercrime adaptation and its socio-economic effect on marginalised and precarious youth in the underdeveloped societies in West Africa who indulge in this scamming business.

5. References

Abubakari Y., 2020*: Perspectives of Teachers and Parents on Parent-Teacher Communication and Social Media Communication*. "Journal of Technical and Educational Sciences jATES", 10, 4, 5-36; https://doi.org/10.24368/jates.v10i4.184.

Akuta E. A., Monari I., Jones C. R., 2011: *Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice.* "Gender and Development", 1, 129-137.

Anyanwu J. I., Obiyo N. O., 2012*: Cybercrime among university undergraduates: Implication for counselling.* "Journal of Home Economics Research", 17, 105-115.

Apau R., Koranteng F. N., 2019*: Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior*. "International Journal of Cyber Criminology", 13, 2, 228-254.

Aribake F. O., Aji Z. M., 2020: *The mediating role of perceived security on the relationship between internet banking users and their determinants*. "International Journal of Advanced Research in Engineering and Technology", 11, 2, 296-318.

Armstrong A., 2011: *"Sakawa" Rumours: Occult Internet Fraud and Ghanaian Identity.* Working Paper in Anthropology. University College, London.

Boateng R., Long O., Mbarika V., Avevor I., 2010: *Cyber Crime and Criminality in Ghana: Its Forms and Implications*. "Americas Conference on Information System", 507.

Buchanan T., Whitty M. T., 2014*: The online dating romance scam: causes and consequences of victimhood*. "Psychology, Crime and Law", 20, 3, 261-283; https://doi.org/10.1080/1068316X.2013.772180.

Burrell J., 2008a: *Problematic empowerment: West African Internet scams as strategic misrepresentation.* "Information Technology & International Development", 4, 4.

Burrell J., 2008b: *Problematic Empowerment: West African Internet Scams as Strategic Misrepresentation*. "Information Technologies and International Development", 4, 4, 15-30; https://doi.org/10.1162/itid.2008.00024.

Burrell J., 2011: *User agency in the middle range: Rumors and the reinvention of the internet in Accra, Ghana*. "Science Technology and Human Values", 36, 2, 139-159; https://doi.org/10.1177/0162243910366148.

Burrell J., 2012: *Invisible Users: Youth in the Internet Cafés of Urban Ghana*. MIT Press.

Chiluwa I. M., Kamalu I., Anurudu S., 2020: *Deceptive transparency and masked discourses in Ponzi schemes: a critical discourse analysis of MMM Nigeria*. "Critical Discourse Studies", 1-8; https://doi.org/10.1080/17405904.2020.1816481.

Cohen A., 1955: *Delinquent boys; The culture of the gang*.

Cornish D. B., Clarke R. V., 1987: Understanding Crime Displacement: an Application of Rational Choice Theory. "Criminology", 25, 4, 933-948; https://doi.org/10.1111/j.1745-9125.1987.tb00826.x.

Duah F. A., Kwabena A. M., 2015: *The Impact of Cyber Crime on the Development of Electronic Business in Ghana*. "European Journal of Business and Social Sciences", 4, 1, 22-34.

Dukku M. K., 2019: *The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Gombe, Gombe State, Nigeria*. "International Journal of Educational Research and Management Technology", 4, 1, 100-115.

Ebenezer A. J., Paula A. M., Allo T., 2016*: Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria*. "International

Journal of Cyber Criminology", 10, 1, 62-78; http://doi.org/10.5281/zenodo.58522.

Eboibi F. E., 2017: *A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015*. "Computer Law and Security Review", 33, 5, 700-717; https://doi.org/10.1016/j.clsr.2017.03.020.

Enoghomwanse A., 2019: *Cyber Crime and Its Economic Impact in Nigeria*. "South Eastern Journal of Research and Sustainable Development", 2, 1, 16-31.

Evans O., 2019: *Repositioning for Increased Digital Dividends: Internet Usage and Economic Well-being in Sub-Saharan Africa*. "Journal of Global Information Technology Management", 22, 1; 47-70; https://doi.org/10.1080/1097198X.2019.1567218.

Green B., Gies S., Bobnis A., Piquero N. L., Piquero A. R., Velasquez E., 2020: *The Role of Victim Services for Individuals Who Have Experienced Serious Identity-Based Crime*. "Victims and Offenders", 15, 6, 720-743; https://doi.org/10.1080/15564886.2020.1743804.

Hidayanto A. N., Junus K., Limupa A., Jumus K. M., Fitriah N., Budi A., 2015: *Investigating knowledge sharing behaviour on virtual community members: integration of technological, individual and contextual factors.* "International Journal of Business Information Systems", 19, 2, 180-204; https://doi.org/10.1504/IJBIS.2015.069430.

Igwe C. N., 2011: *Socio-economic developments and the rise of 419 Advance-Fee Fraud in Nigeria.* "European Journal of Social Sciences", 20, 1, 184-193.

Jerome-Orji U., 2019: *An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states*. "Computer Law and Security Review", 35, 6; https://doi.org/10.1016/j.clsr.2019.06.001.

Kopp C., Sillotoe J., Gondal I., Layton R., 2016: *Online romance scam: Expensive e-living for romantic happiness.* "29th Bled eConference Processings", 175–189.

Lewis J., 2018: *Economic impact of cybercrime: no slowing down*. Washington D.C.: Centre for Strategic and International Studies; https://www.csis.org/analysis/economic-impact-cybercrime.

Liberati A., Altman D. G., Tetlaff J., Mulrow C., Gøtzsche P. C., Ioannidis J. P. A., Clarke M., Devereaux P. J., Kleijnen J., Moher D., 2009: *The PRISMA Statement*

for Reporting Systematic Reviews and Meta-Analyses of Studies that Evaluate Health Care Interventions: Explanation and Elaboration. "Journal of Clinical Epidemiology", 62, 10.

Longe O. B., Chiemeke S. C., 2008*: Cyber crime and criminality in Nigeria - What roles are internet access points in playing?*. "European Journal of Social Sciences", 6, 4, 132-139.

McCombie S., Pieprzyk J., Watters P., 2009: *Cybercrime attribution: An eastern european case study*. "Proceedings of the 7th Australian Digital Forensics Conference", 41-51.

Merton R. K., 1938: *Social structure and anomie*. "American Sociological Review", 3, 5, 672-682.

Modic D., Anderson R., 2015: *It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud*. "IEEE Security & Privacy", 13, 5, 99-103.

Norris G., Brookes A., Dowell D., 2019: *The Psychology of Internet Fraud Victimisation: a Systematic Review*. "Journal of Police and Criminal Psychology", 34, 3, 231-245; https://doi.org/10.1007/s11896-019-09334-5.

Ogunleye Y. O., Ojedokun U. A., Aderinto A. A., 2019: *Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria*. "International Journal of Cyber Criminology", 13, 2, 309-325.

Ojedokun U. A., Eraye M. C., 2012*: Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria*. "International Journal of Cyber Criminology", 6, 2, 1001-1013; https://doi.org/10.1163/17087384-12340034.

Oleksiewicz I., 2019: *Policy to Prevent and Combat Cyber-crime in Africa*. "Humanities and Social Sciences", 7, 4, 138-146.

Olukolu R. O., 2019: *An assessment of the impact of municipal laws on the policing of cybercrimes in Nigeria*. "African Journal of Legal Studies", 11, 2, 234-253.

Oriola T. A., 2005*: Advance fee fraud on the Internet: Nigeria's regulatory response*. "Computer Law and Security Review", 21, 3, 237-248.

Pahlevan-Sharif S., Mura P., Wijesinghe S. N. R., 2019: *A systematic review of systematic reviews in tourism*. "Journal of Hospitality and Tourism Management", 39, 58-165; https://doi.org/10.1016/j.jhtm.2019.04.001.

Paternoster R., Jayne C. M., Wilson T., 2017*: Rational Choice Theory and Interest in the "Fortune of Others"*. "Journal of Research in Crime and Delinquency", 54, 6, 847-868; https://doi.org/10.1177/0022427817707240.

Rege A., 2009: *What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud*. "International Journal of Cyber Criminology", 3, 2.

Shaari A. H., Kamaluddin M. R., Paizi-Fauzi W. F., Mohd M., 2019: *Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims*. "GEMA Online Journal of Language Studies", 19, 1, 97-115; http://doi.org/10.17576/gema-2019-1901-06.

Sowunmi F. A., Adesola M. A., Salako M. A., 2010: *An appraisal of the performance of the economic and financial crimes commission in Nigeria.* "International Journal of Offender Therapy and Comparative Criminology", 54, 6, 1047-1069; https://doi.org/10.1177/0306624X09341043.

Tade O., Aliyu I., 2011: *Under a creative commons Attribution-Noncommercial-Share Alike 2.5 India License 860 Social Organization of Internet Fraud among University Undergraduates in Nigeria*. "International Journal of Cyber Criminology", 5, 2, 860-875; http://www.cybercrimejournal.com/tadealiyui2011julyijcc.pdf.

Tettey W. J., 2008: *Globalization and Internet Fraud in Ghana in Neoliberalism and Globalization in Africa.* New York: Palgrave Macmillan.

Uzorka M. C, Nweyilobu A. C., Harcour P., 2018*: Information Technology and the Escalation of Cyber Crime in the Niger Delta Region of Nigeria*. "International Journal of Scientific Research in Education", 11, 5, 894-901.

Viosca R. C., Bergiel B. J., Balsmeier P., 2004: *Effects of the electronic Nigerian money fraud on the brand equity of Nigeria and Africa*. "Management Research News", 27, 6, 11-20; https://doi.org/10.1108/01409170410784167.

Whitty M. T., 2015*: Anatomy of the online dating romance scam*. "Security Journal", 28, 4, 443-455; https://doi.org/10.1057/sj.2012.57.

Whitty M. T., 2018a*: '419 – It's just a Game: Pathways to cyber-fraud criminality emanating from West Africa.* "International Journal of Cyber Criminology", 12, 1, 97-114; https://doi.org/10.5281/zenodo.1467848.

Whitty M. T., 2018b: *Do You Love Me? Psychological Characteristics of Romance Scam Victims.* "Cyberpsychology, Behavior, and Social Networking", 21, 2, 105-109; https://doi.org/10.1089/cyber.2016.0729.

Wpłynęło/received 03.03.2021; poprawiono/revised 22.04.2021