International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

Copyright © 2018 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2018. Vol. 12(1): 97–114. DOI: 10.5281/zenodo.1467848
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

419 – It's just a Game: Pathways to Cyber-Fraud Criminality emanating from West Africa

Monica T Whitty[1]
The University of Melbourne, Australia / University of Warwick, United Kingdom

Abstract

Cyber-enabled mass-marketing frauds (e.g., romance scam, investment scam, 419) are believed to emanate from West Africa, especially from Nigeria. There has been some research and speculation about the reasons why cyberfraud might especially propagate from this region. This paper conducts a critical review of existing literature to consider how much we can attribute culture as a cause and enabler of this type of crime as well as West Africans, with a heavy focus on Nigerians' pathways to cyberfraud criminality. It is concluded that some cultural factors are important to consider (e.g., social and historical factors, social identity and attitudes towards this form of crime). However, a word of caution is made here to not overstate how the 'West African cultural explanation' as the reason for why this criminal activity has flourished in this region. Taking previous work into consideration, a theoretical framework is proposed to set out the pathways to cyberfraud criminality and the paper sets out a way forward in the development of successful disruption and prevention strategies.

Keywords: Cyber Scams, Cyber fraud, mass-marketing fraud, West Africa, Nigeria, 419 scam, pathways to criminality.

Introduction

There has been much concern about the amount of cyber dependent and cyber enabled crimes that emanate from West Africa, including financial fraud hacking, drugs and human trafficking, and terrorism (Quarshie & Martin-Odoom, 2012). The West African country, Nigeria, has been ranked as the leading State in the region for the conducting of malicious Internet activities (Aransiola & Asindemade, 2011; Longe & Chiemeke, 2008; Quarshie & Martin-Odoom, 2012).The cybercrimes that propagate from West Africa have become a global problem, affecting individuals, organisations and countries, especially in Western societies (Anderson et al., 2013). This paper, however, concerns itself with one of the cybercrimes that emanate from West Africa, that of cyberfraud, also referred to as cyberscams. Given that the literature has focused more on the cyberfrauds which emanate from Nigeria, the paper will focus more heavily on this West African country. The types of cyberfrauds conducted by these criminals are varied

[1] Professor of Human Factors in Cyber Security, University of Melbourne, Parkville 3010, Victoria, Australia; WMG, International Manufacturing Centre, University of Warwick, Coventry, CV4 7AL, United Kingdom. Email: MW@warwick.ac.uk

and continue to develop. The most well-known of these is the 419 scam (so named because of the Section Number of Nigerian criminal law that applies to it), that began as postal mail and moved to become an Internet scam, has its origins in Nigeria (often referred to as the Nigerian email scam). Money acquired from cyberfraud is said to fund terrorist groups and their activities (FATF, 2013) and the crime has tricked many victims, on a global scale, often causing severe financial and psychological harm (Whitty & Buchanan, 2012, 2016; Whitty, 2015). This paper conducts a critical review of the literature that considers the reasons why this crime has been so prominent in this region and sets out, based on this literature, pathways to cyberfraud criminality, particularly within a Nigerian context. The paper also points out the gaps in the literature. In this paper a theoretical framework is developed that provides explanation for the abundance of this crime emanating from this region. The framework is arguably important for prevention programmes and for guidance in the development of policy to disrupt this particular type of cybercrime.

1. Profile of a Cyber-Fraudster

Profiling criminals can be useful for detection and conviction of criminals as well as for the purposes of prevention (Nykodym, Taylor & Vilela, 2005). Understanding the profile of the cyberfraudster in cyberspace (including their digital footprints) and the physical realm (e.g., where gangs are likely to congregate) might also be helpful for these purposes. It might be equally important to understand the psychology of the cyberfraudster in order to improve detection and disruption strategies.

a. Socio-demographic description of a Nigerian cyberfraudster

There is very little research available on the profile of a typical Nigerian cyberfraudster. The existing research draws from very small samples and given there are also few arrests it is difficult to ascertain, with confidence, who are the cyber criminals. The scant available literature suggests the cyberfraudsters are young, often belonging to gangs. Rich (2018) makes the claim that Yahoo Boys (gangs of cybercriminals who reside in Nigeria) are usually adolescent males between the ages of 12 to 16 years. However, this is not based on any empirical research and, in fact, Rich gives no evidence for how he arrived at this demographic. Aransiola and Asindemade (2011) report that the sample of 40 cybercrime perpetrators (they obtained from snowballing) consisted of young people between the ages of 22-29 years. The method used to make this demographic claim, however, is weak, making it difficult to make these sweeping generalisations.

Interestingly, researchers have found that many cyberfraudsters in Nigeria are university students (Aghatise, 2006; Aransiola & Asindemade, 2011; Ojedokun & Eraye, 2012). Aghatise (2006) claims that 80% of these types of criminals are students – although, similar to Rich, he does not provide any evidence for how he arrived at this figure. Tade and Aliyu (2011) make the following statement:

> It would not be out of place to assert that most students in tertiary institutions are thinking of making quick money rather than progressing in their academic quest. To them, Internet fraud is a social security to escape exposure to anticipated difficulties. With money, yahoo-boys can *sort* corrupt lecturers, party with their friends and have unlimited girlfriends (p. 871).

Whilst their statement is a bold claim, it may be that a significant number of university students are interested in committing fraud, and if research supports this hypothesis then law enforcement might focus their attention towards universities in order to disrupt this crime.

b. Psychological make-up of the cyberfraudster

There is a dearth of research available on the psychological characteristics of cyberfraudsters. Given that these crimes often involve planning we might expect these individuals to score high on measures of pre-mediation. Moreover, given that the success of many of these crimes requires skills in networking, deceiving and persuasion, we might expect these criminals to score high on Machiavellianism. Furthermore, criminals who engage in versions of these frauds that involve deep psychological hurt and harm to victims (Whitty & Buchanan, 2016) might score high on Psychopathy. Given the estimated number of cyberfraudsters a generalised psychological profile might not be possible. Instead, we might find that those who gravitate to particular versions of these crimes, for example, those involving the development a relationship over time and a friendship or romance, such as, investment fraud or romance scam, might differ to those in other versions which involve a quick hit, such as consumer fraud or require more technical skills, such as a Phish. For example, someone who lacks empathy and is able to dissociate might be better able at committing romance scams.

c. Motivations for committing Cyber fraud

There are multiple reasons why a person might commit cyberfraud. Besides the obvious incentive of wealth acquired from their criminal exploits, cybercriminals enjoy an elevated social status and possess a prominent position amongst their peers. Male cyberfraudsters are popular and successful at attracting women (Tade, 2013). Criminals at universities are also well-known by their lecturers and exploit this knowledge to bribe corrupt lecturers in order to achieve better grades (Tade & Aliyu, 2011). The money acquired from these cybercrimes is spent on an extravagant standard of living, including: purchasing of expensive motor vehicles, parties and consuming alcohol, living in luxurious apartments, and owning expensive jewellery and technological gadgets (Aghatise, 2006; Aransiola and Asindemade, 2011). Little has been written about female criminals' motivations for becoming involved in this crime. Although women's roles in gangs are discussed later, it is worthwhile noting that their motivations for involvement in these crimes might be akin to men's, there is the likelihood that some women are coerced against their will to become involved in these crimes.

The motivations discussed above have been arrived at from research conducted on cyberfraudsters residing in Nigeria; however, these motivations might be easily generalised to all cyberfraudsters (more on this later in this paper with a wider discussion of the fraud triangle).

d. Environment

The environment that enables cybercrimes can be both physical and cyber. Wall (2007, 2008) has been critical of the lens the media, political commenters, and some scholars have taken when examining cybercrimes. He reminds us of the science fiction origins of the term 'cyberspace' and suggests that cybercrimes have been sensationalised and misunderstood – treating the phenomena akin to fantasy in preference to reality. As he states: "the science fiction moulded conceptualisation of cybercrime has shaped and distorted our expectations of them as being dramatic, futuristic and potentially dystopic" (p. 48).In line with Wall's point, the work on West African cyberfraudsters has, importantly, focused on the intersection of the cyber and physical environments, examining how both these realms promote cybercriminality.

e. Familial background

Criminologists are often interested in the familial background of the criminal to help understand how this background might have 'shaped' the person into becoming a criminal. With respect to Nigerian cyberfraudsters, Aransiola and Asundemade (2011) examined, in detail, a sample of university student Yahoo Boys. These students came from educated backgrounds with the majority of the perpetrators' parents possessing at least a university degree (80%). The majority of the criminals parents' incomes were low compared with their educational qualification; however, the researchers point out their incomes were consistent with the majority of Nigerians who still live below the poverty line. The majority of the cybercriminals (95%) believed that their parents were unaware of their criminal activities. Whilst these descriptive statistics might be useful to help understand how individuals' backgrounds might promote or deter a person from becoming a criminal, the research does not tell us how many well-educated citizens *do not* become criminals – making it very difficult to hypothesize that parental education is a predictor of criminal children, as the researchers imply.

Although again, unsupported with empirical evidence, Tade (2013) claims that:

> Owing to economic activities, parenting in Nigeria has become less effective. Children have been left to be guided by the Internet and their peers, while the parents' attention is glued to economic pursuit. The result is too much freedom to explore… (p.697)

Whilst this view is unsupported (for example, is it likely that all children who receive this type of parenting turn into cybercriminals? Or is poor parenting a mediating factor), understanding the differences between parenting non-cybercriminals and cybercriminals receive might be worthy of pursuit when taken together with other variables.

f. Gang culture

Research over the years has found that gang members are significantly more likely than non-gang members to commit crimes (Spergel, 1990). Belonging to a gang can be an early-starting developmental pathway to crime (Ingoldsby & Shaw, 2002). Notably, some research on white-collar fraudsters has found that male criminals are more likely to work in crime groups (Daly, 1989) – although these groups look quite different to the cyberfraudster gangs in Nigeria. Pyrooz, Decker and Moule (2015) note that understanding the gang behaviours of cyberfraudsters is especially important given that gang members fit the age group most likely to use the Internet (especially social media) and because gang membership facilitates involvement in crime.

The gangs of mass-marketing fraudsters, which exist in Nigeria, are well known; however, what is less known are the reasons why young people join these gangs and the sorts of people who join these gangs. Thornberry, Krohn, Lizotte and Chard-Wierschem

(1993) point out that gangs ought not be considered as "a homogeneous blob with no variation in their behaviors or characteristics...Some gangs are more violent than others, some more instrumental than others, some are more involved in drug use than others, and so on" (p.56). The following sections sets out what is currently believed to be known about these criminal gangs known as Yahoo Boys (in Nigeria).

Yahoo Boys

In Nigeria, Internet fraud is referred to as Yahoo Yahoo and the fraudsters are referred to as Yahoo Boys. According to law enforcement (NCA, personal correspondence) Yahoo Boys operate in gangs and often form loose networks across the world to commit these crimes. Yahoo Boys exploit the corrupt Nigerian culture to enable their crimes (e.g., banks, Western Union, MoneyGram, security officials etc.) (Aranisiola & Asindemade, 2011; Tade & Aliyu, 2011). It is noted here and discussed later in this paper the '*Yahoo Plus'* Boys who incorporate spirituality to enable their cybercrimes.

As is typical of gang structures (Decker & Curry, 2000), Yahoo Boy gangs appear to have a hierarchy of gang membership and membership is transient. Tade (2013) colourfully describes the transient nature of Yahoo Boys gangs as follows:

> The 'wet' season is when the fraudster consistently becomes successful in his rate of victimisation. He makes money via online fraud and spends it on friends and 'babes' (girls). He commands respect as a 'big boy'. This 'wet' season may not last. As the 'dry' (low success rate) season sets in, the new yahoo boy begins to make waves in the business. Attention is shifted from the former kingpin to the trainee who now becomes the cynosure of all eyes.

As Tade and others (e.g., Aransiola & Asindemade, 2011) explain, members of Yahoo Boy groups are competitive amongst each other and in-group hostility amongst cohort members is fairly common. Newer recruits, who are initiated by more experienced members, may move quickly up the hierarchy, depending on their success rates. Whilst more research is needed to confirm these early findings, they do shed light on the question of whether high profile court cases prosecuting kingpins in organisations might be a successful strategy to deter other gang members. If gang-members are vying for the top position they might not be so concerned that they have lost their top members.

If multiple arrests are needed, therefore, to deter cybercriminals, then it is necessary to easily identify and detect cybercriminals. Besides the use of cyber forensics to detect these criminals, research findings suggest that Yahoo Boys *stand out* amongst non-gang members (at least in university settings). In Ojedokun and Eraye's (2012) study on university students' perceptions of Yahoo Boys, that despite their covert activities, these students stood out amongst others given their extravagant lifestyles. Participants in their study described cybercriminals in the following extracts:

> *They (cyber criminals) buy expensive phones, jewelries and exotic cars, like Honda, Toyota, Benz, among others. These students usually spend money recklessly, because they are eager to show other people that they have arrived. Can you imagine a pre-degree student of LAUTECH living in a 3 bedroom flat all alone? (Male student/300L/Ladoke Akintola University of Technology).* [italics added] (p.1007)

> *University students, who are into cyber crime are free spenders, they usually spend money as if there is no tomorrow. They spend their money carelessly; they do not invest in something tangible, but rather prefer to spend it on parties, women, alcohol and buying unnecessary items. Their spending- habit is just too wasteful (Male student/200L/University of Ibadan).* [italics added] (p.1008)

2. Recruiting Criminals – Via Popular Media

The pathways to criminality discussed so far include: the exposure to criminality, family backgrounds and upbringing and motivations for committing these offences. However, as with other crimes, such as radicalisation of terrorists, the scant available literature suggests that cybercriminals attempt to recruit more criminals into their networks (one might hypothesize that an increased number of criminals to assist in perpetuating these crimes makes lighter work for the 'king pins'). Understanding how recruitment works might be useful in order to develop counter-measures.

Some researchers have suggested that propaganda material in the form of hip hop songs and film (esp. Nollywood) popularise cyberfraud, making it appealing especially to young people (e.g., Oduro-Frimpong, 2014). Music videos depict gangs drinking champagne, standing around expensive cars, surrounded by scantily clad women. They depict the victim as a greedy, stupid person who deserves to be conned out of their money. The criminal is depicted as a clever individual and the crime is referred to as a 'game' – suggesting the criminal act is *play* rather than a genuine crime and that the criminal is simply – good at playing this 'game'. This is illustrated in the extract of the song 'I go chop your dollar' cited below (Sweet Lyrics, 2017).

Chorus
National Airport na me get am
National Stadium na me build am
President na my sister brother
You be the mugu, I be the master

Oyinbo man I go chop your dollar
I go take your money and disappear
419 is just a game
You are the loser, I am the winner

The refinery na me get am
The contract, na you I go give am
But you go pay me small money make I bring am
You be the mugu, I be the master
Na me be the master oh

Popular music has been used in numerous ways to change behaviour (e.g., political beliefs, advertising, health behaviours). The framing of the message (e.g., 419 is a game) and the emotions evoked from listening to this media is believed to encourage endorsement of this criminal behaviour (see for example, Maibach, 1993; Street, 2003).It might be useful for academics to understand how individuals respond to this material and how the effects might be counter-acted.

Film might also be utilised in propaganda campaigns. Nollywood and Gollywood have produced numerous films about Yahoo and Sakawa Boys (the Ghanaian equivalent). Oduro-Frimpong (2014) reports on one film that achieved mass-appeal:

> …one could also see prominently displayed advertising posters for the most recent *Sakawa Boys* video at various locations in Accra, which arguably hyped the sakawa issue in the public domain. Producers also strive to convince audiences that the movies portray the "actual" rituals that sakawa fraudsters per-form. On private television channels the film's trailer showcased snippets of alleged sakawa rituals and spiritual fortification processes that are believed to occur in the supernatural realm to ensure the fraudsters' success. In one of the *Sakawa Boys* films for example, Socrate Safo, in an attempt to replicate an actual sakawa ritual, used real coffins for a scene in which a religious specialist (p. 133).

3. Spiritual Beliefs in West Africa and its Relevance to Crimes

Researchers have noted that rituals and spirituality are used by cyberfraudsters to help achieve success with their crimes. This form of religion is said to be persuasive across Nigerian culture and is not exclusively practiced by criminals.

Although Islam and Christianity are the dominant religions in West Africa (Kaba, 2005; Hassan, 2008), many ethnic groups and tribes belong to their own traditional religious groups. The Yoruba religion is an example of a Nigerian indigenous religion that is typically practised in South-Western Nigeria and adjoining parts of Benin and Togo. Magic and spiritual powers are an aspect of these indigenous religions, typically referred to as '*Juju*' (Mockler-Ferryman, 2012). The priests (also referred to as witch doctors or Juju men) of Juju religions are believed to have the power of life and death and can communicate with the dead.

Notably, people who practice the dominant religious – Christianity and Muslim– do so in their own unique ways. They also often engage, for example, in ritualistic practices and use protection amulets. Wildlife by-products are commonly used in cultural festivals held by most religious groups (e.g., masquerades, death ceremonies and installation of traditional rules) (Adeola, 1992).

Relevant to this paper is the question of whether these unique forms of spirituality enable cybercrimes or whether perhaps once a criminal is committed to conducting these crimes, these practices provide the 'superstitious belief' that the criminal will have success – motivating them to continue on with crimes rather than as a starting point into the pathway of criminality. The answer is possibly both, however, disrupting a culturally ingrained religion for the purposes of preventing cyberfraud might prove challenging.

In Nigerian society it is reported that the priests involved in these indigenous religions offer their services to the community. Those who subscribed to these religious beliefs take the priests' practices very seriously, often fearing the priests (sometimes referred to as Juju men). The fear of Juju should not be understated and is succinctly summarised by Nwolise (2012; cited in Tade, 2011; p. 690-691) below:

> The fear of juju and witchcraft in Nigeria and Africa is real and this has kept many young and old people away from their villages and this has serious negative implications for national development, especially rural areas... (p. 10).

Traffickers, for example, have drawn from their services to persuade parents to part with their children and to ensure allegiances are maintained. To ensure protection while travelling and success upon arrival in Europe, rituals are carried out before the victims leave West Africa, including making incisions onto bodies with sharp objects, sacrificing of animals and eating of animal hearts (Van Dijk, 2001). Women involved in human trafficking often feel bound to these rituals and are conditioned to follow orders of their own accord to warrant their families' as well as their own wellbeing (Baarda, 2016). Walsh (2009) describes how Juju is used in trafficking as follows:

> Traffickers subject their victims to an oath of allegiance, confidentiality, loyalty and faithfulness as a precondition to be employed in their "business undertakings" abroad. The priest takes body parts or samples (*e.g.* fingernails, hair, blood) as part of the oath. The victim believes that their being – that is, their very existence – is represented in those items collected and kept by the priest at a "shrine". A deviation from the terms of the oath is believed to result in death or insanity of the victim concerned, in a manner that will cast shame and hatred on his/her immediate family within that society forever.
>
> When the oath has taken place, the victim is then indebted to the trafficker and can, for example, be bonded to repay a loan on arrival at the destination country for the voodoo oath. The so-called loan sometimes includes travelling expenses, protection, accommodation, food, clothing, etc at the destination country. It symbolizes that the priest can punish you remotely if you breach the contract. The powers of the priest are perceived to be very real. Both victims and sometimes traffickers believe that the priest can cause harm remotely. (p.114)

The violent vigilante group known as the Bakassi boys has also been known to draw from Juju to defend themselves from gunshots and knife wounds or to extort confessions (McCall, 2004). This well-known militia group originated in Aba in the late 90s and took it upon themselves to rid the place of criminals (often using violence as well as killings). They emerged at a time when crime was rampant, as Meagher (2007) aptly describes:

> The Bakassi Boys emerged in a situation characterised by rampant crime and insecurity, a corrupt and inefficient police force, and intensifying power struggles between the Nigerian federal and state governments over the control of security forces. Even unsympathetic accounts of vigilantism in Nigeria recognise the appalling security situation faced by Nigerians during the 1990s. (p.93)

4. Rituals, spirituality and cybercrimes

Some Yahoo boys (referred to as Yahoo Plus Boys) are believed to incorporate Juju and witchcraft into their cybercrimes (Tade, 2011) to increase the success rate of attaining money from victims, who are referred to as '*maga*'. It is believed that employing Yahoo plus will hypnotise victims and consequently they will transfer their money with less difficulty than with the typical 'yahoo yahoo' method. Yahoo plus operators employ '*afose*' which is the power to make things happen, that the victim can never refute, '*oruka-ere*' which are magical ornaments that works in conjunction with incisions on the operator's bodies, and '*ijapa*' which refers to enchanted tortoises that the operators rest their feet on when surfing the Internet.

The charms, described above, can be obtained from herbalists, Juju witchdoctors, or a specific Yahoo plus priest. The latter is an individual who holds the belief that God divinely appointed them and fuses fetishism in the criminals' practice. It is believed by criminals that the use of these charms can help ensure greater and quicker success at obtaining money from victims (Tade, 2013). These criminals believe, for instance, that 'afose', cannot be refuted and once incanted the victims will have no choice but to comply. It is believed that the victims will only recover from this spell after complying with the commands of the yahoo plus operator. It is believed by these criminals that 'afose' is a useful incarnation in cybercrime given that it is believed to travel through air to any location, thereby bypassing the obstacle of the victims being abroad.

Yahoo plus can also include female criminals. Tade (2011) summarises how women are often exploited by their boyfriends to assist in these crimes:

> Usually, a girlfriend may agree to be part of the fraud with a sworn agreement that they share the proceeds. The agreement is traditionally executed at the shrine. This is because the lady plays a significant role in the final success of any cyber-fraud. In this partnership, the female loses weight when the Internet negotiation begins. She acts as a catalyst in the bewitchment process of the victims. As the deal near success, she loses more weight almost resembling somebody that has contracted AIDS. Ironically, the success is also dependent on her reduced size and the pain she endures. This is the normal cycle until the final payment is made and she regains her normal weight. (p. 701).

It has been argued that Yahoo plus operators believe in the spiritual forces they invoke (Tade, 2011). However, it might be important for researchers to investigate to what extent criminals believe in the power of Juju. The example of the how women are used in the crime given above, suggests that the criminals also employ the *fear of* Juju to employ accomplices to assist in their crimes. This might be akin to how criminals employ the fear of Juju to ensure success of other crimes, such as human trafficking (described earlier in this paper). It also suggests that female cyberfraudsters' pathways into criminality might be quite distinctive when compared with male criminals.

5. Rationalisations for Cybercriminal Behaviour

The paper, thus far, has focused on describing cybercriminals as well as providing reasons why West Africans might move into cybercriminality (e.g., joining a gang, desiring wealth and the social status that accompanies this wealth). Next, this paper examines rationalisations that are possibly unique to West Africans for their cybercrimes; however, it is noted that rationalising is a common defence mechanism employed by criminals to justify their behaviour. These rationalisations are employed in the early stages on cybercriminality as well as to maintain involvement in these types of cybercrimes. Rationalisation, therefore, is an important element in the pathways to criminality of cyberfraud, as explained below.

i. Maga – Greedy, stupid Westerns deserves it!

Maga or Muga is a common term used by Yahoo Boys to refer to someone who is stupid and greedy who has fallen victim to fraud (Tade & Aliya, 2011). Researchers argue that cybercriminals believe that their actions are revenge for being treated badly by foreigners (Argenti, 2007; Künzler, 2006; Longe, Ngwa, Wada, Mbarkia and Kvansny, 2009; Tade, 2013). This perceived injustice against West Africans includes the Transatlantic slave trade to the New World, which involved Portugal, Spain, France and England (Tade, 2013; Rawley & Behrendt, 2005). Criminals are rationalising, therefore, that their criminal acts are morally legitimate. Tade (2013) writes that:

> Those involved reported that the 'white' have exploited their fathers to build their countries while impoverishing them. They employ techniques of self-justification by condemning the condemners and describing those being defrauded as equally greedy. (p. 698).

Tade provides an extract from one of his interviews with a cybercriminal to support this view.

> This reason is greed. Once a guy could see that his friend is driving expensive cars, he or she could be easily influenced negatively. Again, corruption is the root of all evil acts. The issue of embezzlement is also germane. Monies given out to officials to create infrastructural facilities and even jobs to people are diverted into personal purse. This serves as negative influence on people particularly the youths. However, some believe that it is their forefathers' money that they are collecting back from the white. They believe that their forefathers have been exploited so they must inherit their forefather's wealth. (Yahoo plus/Male/24) (p.698)

The song lyrics quoted early in this paper include this form of rationalisation, overtly stating that it is the Westerns' greed that makes them susceptible to fraud. Frei (2014) contends that the phrase 'chop your dollar' should be understood as a normative expression related to the practices of accumulation and redistribution of wealth. According to Longe et al., (2009) this song suggests that scamming is 'just a game' – rather than a criminal or immoral act.

ii. Clever criminal vs Stupid victim

Extending on the above rationalisation is the discourse that 'only stupid people fall for scams' and that if the clever fraudster can trick the victim out of their money they deserve to reap this reward (Künzler, 2006).Cybercriminals, arguably, believe that the gullibility of the 'magas' (victims) excuses their own behaviour and the onus should be on the 'magas' to recognise that they are being scammed (Longe et al., 2009). They arguably take pride in their own cleverness and ability to trick victims into sending money (Longe et al., 2009).

We should be mindful, however, that the above rationalisation is of course not unique to West African fraudsters. This view is also commonly shared amongst white-collar criminals (Marks, 2012). Smith (2009) takes this a step further to argue that fraudsters and entrepreneurs both commonly hold the view that they are clever, cunning and daring individuals. Moreover, researchers have found that Westerners often blame the victim (including the victim themselves) for being scammed (Whitty & Buchanan, 2016), suggesting that the portioning of blame to others away from the criminal might not be unique to a West African culture.

iii. Some crimes are worse than others

Researchers have reported that West Africans perceive physical theft as more serious compared with cybercrimes. Ibrahim (2016) writes:

> This socio-cultural 'understanding' could be due to the relative absence of 'real victims' and 'blood and knives' when it comes to cybercrime…Unlike the case of cybercrime, negative societal reactions against terrestrial crime could act as a deterrence mechanism even in the presence of low moral standards. Therefore, it is the society's reactions that define what is a 'crime' in Nigeria. Social reactions inherent in Nigeria, in terms of cybercrime may have knock-on-effects on of cybercrime involvement among the youths. This suggests that morality may be more of an index factor for 'cybercrimes' than terrestrial crimes in the Nigerian context. (p. 6)

The above research is based on 17 parents' views of children's involvement in cybercrime. The small and selective sample makes the findings problematic to generalise and suggests that further empirical research is needed to support this claim. However, even if empirical research supports this claim, again we need to be mindful of research that extends beyond West African culture. For example, much of the literature on white-collar crimes tells a similar story. Levi (1987), for instance, writes in detail about the distinction made in the West regarding crimes that are more concerned about public-order issues, such as street crimes compared with white-collar crime, which is often not perceived as a 'real crime'. Whilst we might question whether West Africans maintain a different 'moral compass' compared to Westerners, research is needed to support such a claim – whilst being mindful of similar discourses in the West.

6. Rationalisations vs Excuses

From a psychodynamic perspective, rationalisations are defence mechanisms to excuse one's behaviour. They assist individuals in coping with behaviour that is socially unacceptable. Research is yet to elucidate whether the excuses discussed here (e.g., that Westerners deserve to have money conned from them) are genuine beliefs or rationalisations or somewhat mixed. Understanding the extent to which criminals genuinely believe these excuses might help in work to deter individuals from engaging in these crimes. Moreover, rationalisations that do not work might also be important to examine. For example, the rationalisations explained above do not explain why Nigerians scam their 'own' people, who share their own race and reside in their own countries.

Researchers have also considered social conditions within West Africa, which might be considered a causal factor when considering cybercrimes. The following section focuses on three of these factors examined in the literature: political and economic climate, poverty and e-waste.

a. Political and economic climate

Rich (2018) argues that the rise of cyberfraud is linked to Nigeria's political and economic climate, especially after its financial crisis in the 1980's. In brief, in the 1970's Nigeria experienced oil wealth bringing in enormous revenue (Künzler, 2006). The discovery of petroleum propelled the economy of Nigeria in the 1950's (Ibrahim, 2016). Instead of careful investment and smart expenditure of funds, this era highlighted failure of political leadership during which Nigeria underwent a quick succession of unstable rulers. Vigilantism, coups and militia contesting state authority was unbridled in the 1960's. Corruption, insurrections and political violence were rife under the rule of President Shagari and his successors. During this time, the emergence of a new group of elites consisting of educated bourgeoisie was evident, exemplifying the rise of the middle and upper classes.

Political assassinations have been a major outcome of political violence since the 1980s (Igbafe & Offiong, 2007). As Igbafe and Offiong (2007) wrote over 10 years ago:

> The level of political assassination in Nigeria is a clear manifestation of political vendetta; where peace has given way to violence and assassination has become the norm; where political actors resort to assassination of political opponents all in a bid to attain political power or positions. The spate of political assassinations in Nigeria has reached an alarming stage with a good number of her prominent politicians and citizens alike lost to this hydra-headed monsters. The government of Nigeria is finding it extremely difficult in handling the level of insecurity in the country, which has put the lives of its citizens in danger. Right from 1986 till date, the spate of political assassinations has risen in a geometric progression, thus eroding human values such that violence grew in time. (p.9)

The oil boom of the 1970s ended abruptly in the 1980s (see Turner, 1986). Perhaps, unsurprisingly, the corruption remained and arguably increased. Adogame (2007) reports embezzling funds was commonplace among politicians that further deteriorated the economy. This culture of corruption among authoritative figures of the region practiced by certain politicians gave way to political impunity.

Künzler (2006) maintains that the economic crisis and global capitalism subsequently catalysed Internet scams. Inflation and currency devaluation propelled advance fee frauds where the U.S. currency became an attractive target. Under the regime of General Babangida, 419 frauds flourished in the 1980's. According to Apter (1999), General Babangida supported cyberfraud and accrued profits from the operations. These politicians fostered fraudulent practices and viewed Westerners as a source of attaining financial gains (Adogame, 2007).

It is difficult to make a direct causal link between social circumstances and the rise of cybercrime in Nigeria; however, this might provide some explanation for the rise of crime. A corrupt culture might also have been an enabler of this crime. As reported earlier in this paper, cyberfraudsters have been known to bribe people (banks, security officers, etc.) in order to enact their crimes and given that corruption is rife in countries, like Nigeria, then this makes it a challenge to prevent cybercrimes which are, in part, dependent on those who are easily corrupted.

b. Poverty

Poverty is believed by some to be a cause of cybercrimes. Ibrahim (2016) contends that the deterioration of the region's economy and the increased number of unemployed graduates has been a catalyst for cybercrimes. Students are skilled to commit these crimes, and if they foresee little opportunity for employment after their studies, might be tempted into acquiring money by employing their skills in illegal activities to gain money.

As with other social conditions, it's difficult to attribute poverty as the cause of cybercrime; however, it may well be a contributing factor. Moreover, corruption and poverty make this crime difficult to tackle – as resources and new skills are needed to identify criminals to prosecute. As Hassan, Lass and Makinde (2012) point out:

> African countries are bedeviled by various socio-economic problems such as poverty, AIDS, fuel crisis, political and ethnic instability and other related crimes. This limits their strength to effectively combat cyber crime.

c. E-waste

An enabler of cybercrime not always considered is e-waste. As O'Brien (2011) points out in a newspaper article:

> CRIMINAL networks are feeding off Australians' lust for new technology by skimming data from computers dumped in Africa and Asia - and using it for blackmail, fraud and identity theft.
>
> They will pay as much as $200 on the black market for discarded computer hard drives, which they mine for bank details, credit card numbers and account passwords.

Abugri (2011) provides the example of a Ghanaian youth named Eric Agbosu who telephoned the U.S. Republican Congressman Robert Wexler and extorted him out of money, blackmailing him with Wexler's personal and credit information. Agbosu is believed to have retrieved this highly sensitive information by purchasing computer parts from Agbogbloshie's e-waste site.

The problem with e-waste does not need to be purely solved by West Africa. Western countries responsible for sending their e-waste to be recycled might think again where to send it and ensuring that data is properly deleted from computers. When developing an overall framework on strategies to employ to tackle these crimes, considerations of e-waste ought to be considered.

Theoretical Framework

The scholarly literature summarised in this paper points to multiple variables that ought to be considered when developing a framework to explain the pathways to criminality and enablers of cyberfraud conducted by criminals in Nigeria. This body of work suggests there might be some value in understanding cyberfraud criminality within a cultural context. The history of fraud in Nigeria suggests that this is a crime that emerged under specific social circumstances and that over time has potentially penetrated into the Nigeria psyche as a more acceptable crime compared with others. Popular media appears to strengthen this social identity. The song lyrics from an extract from a song quoted below, for example, written by Terry da Rapman (2002, cited in Künzler 2006) suggests that there is a distinct Nigerian identity.

Hi, I am e … ehn? I am a … what? … I am a Nigerian. Hi, I am a … who? I am a … what? I am a Nigerian. (2x)
Hi, do u trust Nigerians?
Kinda people who are rugged and resilient, shady like Sicilians?

Living' off experience and we crave to shine,
419 state of mind, don't wanna slave for mine.
I was born this way, I'm really trying to live straight,
but I'm not qualified for a job that pays 10k
by the month, so I guess I'm sunk, but I gota feed my trunk. Fighting my depression only when I'm drunk.
Since day one I've always been a minority,
living in poverty and this close to staging a robbery.
Got ticked off, one day I punched my boss in the face, Twisted his arm till he gave me the combinations to the safe. Cuz thanks to him I'm broke, livin' wit no hope.
Got bills to pay how am I supposed to cope?
*If I had a gun I'd robbin' all these rich ni**s,*
But here I am, unemployed looking like a stick figure…

The pathways to criminality suggest that there is an easy route into this crime for young people, in particular university students (although much more research is needed to confirm the profile of a cyberfraudster within Nigeria and West Africa as a whole). Gang culture appears to be important to understand with respect to recruitment and enabling this crime. Moreover, spiritually appears to play a role, even if this is simply to enhance the belief that the criminal will be successful at his/her crimes.

It is argued here, however, that a theoretical framework needs to go beyond cultural. Criminal youth gang culture, for example, is not unique to West Africa and whilst there may well be an abundance of cybercriminals within this region, not all fraudsters reside in West Africa. The trivialisation of fraud as a crime is also not unique to Nigeria.

Although the Fraud Triangle is not without criticism (Schuchter & Levi, 2016), it might be a useful lens to help understand why cyberfraud has emerged and continues to be a problem in West Africa. In this theory three factors are present in every instance of occupational fraud: motivation, rationalisation and opportunity. According to the theory, the individual first has a financial problem, which is non-shareable and they become motivated to commit fraud. Second, they perceive an opportunity to commit fraud and have the skills to do so. Third, individuals employ rationalisations to give themselves permission to commit fraud.

Applying the Fraud Triangle to a Nigerian context, the literature summarised in this paper highlights the motivations (e.g., escape from poverty and enjoying a life of high social status), opportunities (e.g., gang cultures which can support and educate young criminals, low cost crime), and rationalisations (e.g., Westerners are greedy and therefore are an acceptable target). The literature summarised suggests that there is easy access into pathways of this form of criminality – suggesting that disruption needs to close down these opportunities. The rationalisations presented in this paper suggest that this crime might be more acceptable in West Africa and that some work needs to go into challenging this discourse. Moreover, if these rationalisations are defence mechanisms, rather than genuine beliefs, then these excuses need to be challenged.

In addition to rationalisations, popular media suggests that Nigerians consider this activity as fun – existing in the realms of play rather than 'real' harm. Contrary to what the Fraud Triangle suggests, however, criminals are not necessarily in a situation where they are experiencing a financial problem which is non-shareable – but rather that this crime is more overt – which might be a contributor to the number of West Africans who move down this pathway of criminality.

Conclusion

In conclusion, although research is beginning to build a picture of the cyberfraudster profile and culture within Nigeria and West Africa as a whole, much more research is required. The emerging research suggests that the cultural context might be critical to understand if successful disruption and prevention programmes are to be developed to reduce the amount of crime that emanates from West Africa. Nonetheless, considerations beyond the culture context should not be disregarded or else we might be at risk of overplaying the West African cultural explanations for cyberfrauds.

Acknowledgements

This research was funded by the National Cyber Security Centre as part of a group of studies funded in the Research Institute in Science of Cyber Security.

References

Abugri, S. (2011). Ghana: Internet criminals cashing in on e-waste. *New African.* Retrieved from http://www.sydneyabugri.com/Home2/features/217ghana-Internet-criminals- cash-in-on-e-waste-dumping.html.

Adeniran, A. (2008). The Internet and Emergence of Yahooboys sub-Culture in Nigeria. *International Journal of Cyber Criminology, 2*(2), 368–381.

Adeola, M. O. (1992). Importance of wild animals and their parts in the culture, religious festivals, and traditional medicine, of Nigeria. *Environmental Conservation, 19*(2), 125-134.

Adogame, A. (2007). The 419 code as business unusual: youth and the unfolding of the advance fee fraud online discourse. *International Sociological Association E-bulletin.* Retrieved from http://www.isa-sociology.org/publ/e-bulletin/E-bulletin_7.pdf.

Agbiboa, D. E. (2015). Protectors or predators? The embedded problem of police corruption and deviance in Nigeria. *Administration & Society, 47*(3), 244-281.

Aghatise, E. J. (2006). Cybercrime definition. *Computer Research Centre.* Retrieved from http://www.crime-research.org/articles/joseph06/2.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Eds.) *The Economics of Information Security and Privacy* (pp. 265-300). Berlin, Germany: Springer-Verlag.

Aransiola, J., & Asindemade, S. (2011). Understanding Cyber Crime Perpetrators and the Strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking, 14*(12), 759-63.

Argenti, N. (2007). *The Intestines of the State. Youth, Violence, and belated Histories in the Cameroon Grassfields.* Chicago: University of Chicago.

Baarda, C. S. (2016). Human trafficking for sexual exploitation from Nigeria into Western Europe: The role of voodoo rituals in the functioning of a criminal network. *European Journal of Criminology, 13*(2), 257-273.

Daly, K. (1989). Gender and varieties of white-collar crime. *Criminology, 27*(4), 769-794.

Decker, S. H., & Curry, G. D. (2000). Addressing key features of gang membership: Measuring the involvement of young members. *Journal of Criminal Justice, 28,* 473-482.

FATF. (2013). *Financial Action Task Force report: Terrorist financing in West Africa*. Retrieved from http://www.fatf.gafi.org/media/fatf/documents/reports/tf-in-west-afriac.pdf.

Frei, B. (2014). 'I go chop your Dollar': Scamming Practices and Notions of Morality among Youth in Bamenda, Cameroon. In Hahn H. P., Kastner, K. (Eds.), *Urban Life-Worlds in Motion: African Perspectives* (pp. 41-72). North-Rhine Westphalia, Germany: Transcript Verlag.

Hassan, A. B., Lass. F.D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *Journal of Science and Technology, 2*(7), 626-631.

Hassan, H. D. (2008). *Islam in Africa* (CRS Report No. RS22873). Retrieved from http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RS22873_05092008.pdf.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 47*, 44-57.

Igbafe, A. A., & Offiong, O. J. (2007). Political assassinations in Nigeria: An exploratory study 1986-2005. *African Journal of Political Science and International Relations, 1*(1), 9-19.

Ingoldsby, E. M., & Shaw, D. S. (2002). Neighborhood contextual factors and early-starting antisocial pathways. *Clinical Child and Family Psychology Review, 5*(1), 21-55.

Kaba, A. J. (2005). Spread of Christianity and Islam in Africa: A Survey and Analysis of the Numbers and Percentages of Christians, Muslims, and Those Who Practice Indigenous Religions. *Western Journal of Black Studies, 29*(2), pp. 561.

Künzler, D. (2006). *Who wants to be a millionaire? Global capitalism and fraud in Nigeria*. Retrieved from https://lettres.unifr.ch/fileadmin/Documentation/Departements/Sciences_sociales/Soziologie__Sozialpolitik_und_Sozialarbeit/Documents/Kuenzler/pdf_s_zu_publikationen/Paper_Kuenzler.pdf.

Levi, M. (1987). *Regulating fraud: white-collar crime and the criminal process*. London: Tavistock Publications.

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

Longe, O., Ngwa, O., Wada, F., & Mbarika, V. (2009). Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Technology Impact, 9*(3), 155-172.

Maibach, E. (1993). Social marketing for the environment: Using information campaigns to promote environmental awareness and behaviour change. *Health promotion International, 8*(3), 209-224.

Marks, J. T. (2012). A matter of ethics: Understanding the mind of a white-collar criminal. *Financial Executive,* 31-34.

McCall, J. C. (2004). Juju and Justice at the Movies: Vigilantes in Nigerian Popular Video. *African Studies Review, 47*, 51-67.

Meagher, K. (2007). Hijacking civil society: The inside story of the Bakassi Boys vigilante group of south-eastern Nigeria. *The Journal of Modern African Studies, 45*(1), 89-115.

Mockler-Ferryman, A. F. (2012). *Imperial Africa: British West Africa*. Charleston, South Carolina: Nabu Press.

Nykodym, N., Taylor, R., & Viela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation, 2*(4), 261-267.

O'Brien, N. (2011). Dumped computers exploited in overseas fraud. The Sydney Morning Herald, October, 2011. Retrieved from http://www.smh.com.au/technology/security/dumped-computers-exploited-in-overseas-fraud-20111001-1l2rj.html.

Oduro-Frimpong, J. (2014). Sakawa Rituals and Cyberfraud in Ghanaian Popular Video Movies. *African Studies Review, 57*, 131-14

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.

Pyrooz, D. C., Decker, S. H., & Moule, R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly, 32*(3), 471-499.

Quarshie, H. O., & Martin-Odoom, A. (2012), Fighting cybercrime in Africa. *Computer Science and Engineering, 2(6), 98-100.*

Rawley, J. A., & Behrendt, S. D. (2005). *The Transatlantic Slave Trade: A History*. Lincoln, Nebraska: University of Nebraska Press.

Rich, T. S. (2018). You Can Trust Me: a multimethod analysis of the Nigerian email scam. *Security Journal*, *31*(1), 208-225.

Schuchter, A. & Levi, M. (2016). The fraud triangle revisited. *Security Journal, 29*(2), 107-121.

Shaw, R. (1997). The production of witchcraft/witchcraft as production: Memory, modernity and the slave trade in Sierra Leone. *American Ethnologist, 24*(4), 856-876.

Smith, R. (2009). Understanding entrepreneurial behaviour in organized criminals. *Journal of Enterprising Communities: People and Places in the Global Economy, 3*(3), 256-268.

Spergel, I. A. (1990). Youth gangs: Continuity and Change. In M. Tonry & N. Morris, *Crime and Justice: A Review of the Research,* Vol 12. (pp.171-275). Morris. Chicago: University of Chicago Press.

Street, J. (2003). 'Fight the power': The politics of music and the music of politics. Government and Opposition: *An International Journal of Comparative Politics, 38*(1), 113-130.

Sweet Lyrics (2017). Nkem Owoh – I go chop your dollar Lyrics. Retrieved from http://www.sweetslyrics.com/727896.Nkem%20Owoh%20-%20I%20go%20chop%20your%20dollar.html.

Tade, O. & Aliyu, I. (2011). Social Organisation of Cybercrime among University Undergraduates in Nigeria. *International Journal of Cyber Criminology 5,* 860-875.

Tade, O. (2013). A Spiritual Dimension to Cybercrime in Nigeria: the 'yahoo plus' phenomenon. *Human Affairs, 23*(4), 689-705.

Thornberry, T. P., Krohn, M D., Lizotte, A. J., & Chard-Wierschem, D. (1993). The role of juvenile gangs in facilitating delinquent behavior. *Journal of Research in Crime and Delinquency, 30*(1), 55-87.

Turner, T. (1986). Oil workers and the oil bust in Nigeria. *Africa Today, 33*(4), 33-50.

Van Dijk, R. (2001). Voodoo on the Doorstep Young Nigerian Prostitutes and Magic Policing in the Netherlands. *Africa, 71*(4), 558-586.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the Information Age.* Cambridge: Polity Press.

Wall, D. S. (2008). Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22* (1-2), 45-63.

Walsh, M. (2009). Human Trafficking. *Judicial Studies Institute Journal, No.1,* 104-129.

Whitty, M. T. (2015). Mass-marketing fraud: A growing concern. *IEEE Security & Privacy, 13*(4), 84-87.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious crime. *Cyberpsychology, Behavior, and Social Networking, 15*(3), 181-183.

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.

Youth Against Cyber Crime and Fraud in Nigeria (2008). Retrieved from www.yaccfin.org.