The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents

Article *in* Telematics and Informatics · May 2019

DOI: 10.1016/j.tele.2019.04.009

CITATIONS
5

READS
188

2 authors:

Suleman Lazarus
University of Portsmouth
15 PUBLICATIONS **98** CITATIONS

SEE PROFILE

Geoffrey Okolorie
University of Derby
1 PUBLICATION **5** CITATIONS

SEE PROFILE

The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents.

THIS COPY IS THE FINAL DRAFT VERSION. However, the Version of Record can be found: https://doi.org/10.1016/j.tele.2019.04.009

Cite article as:

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

Abstract: -

While this article sets out to advance our knowledge about the characteristics of Nigerian cybercriminals (Yahoo-Boys), it is also the first study to explore the narratives of the Economic and Financial Crimes Commission (EFCC) officers concerning them. It appraises symbolic interactionist insights to consider the ways in which contextual factors and worldview may help to illuminate officers' narratives of cybercriminals and the interpretations and implications of such accounts. Semi-structured interviews of forty frontline EFCC officers formed the empirical basis of this study and were subjected to a directed approach of qualitative content analysis. While prior studies, for example, indicated that only a group of cybercriminals deploy spiritual and magical powers to defraud victims (i.e. modus operandi), our data analysis extended this classification into more refined levels involving multiple features. In particular, analysis bifurcates cybercriminals and their operations based on three factors: [a] educational-attainment, [b] modus-operandi, and [c] networks-collaborators. Results also suggest that these cybercriminals and their operations are embedded in "masculinity-and-material-wealth". These contributions thus have implications for a range of generally accepted viewpoints about these cybercriminals previously taken-for-granted. Since these criminals have victims all over the world, insights from our study may help various local and international agencies [a] to understand the actions/features of these two groups of cybercriminals better and develop more effective response strategies. [b] to appreciate the vulnerabilities of their victims better and develop more adequate support schemes. We also consider the limitations of social control agents' narratives on criminals.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

1. Introduction

"I went to Nigeria to meet the man who scammed me[1]*"*

In Nigeria, over 77% of youths live on less than USD2 per day (African Development Bank, 2018), and online and offline lives are inextricably intertwined (Lazarus, 2019a; Lazarus 2019b; Powell et al., 2018). Even though the link between offending and poverty is far from straightforward (Newburn, 2016), unemployment and poverty have strong connections with online crimes "within a given nation" (Kigerl, 2012, p. 483). What is notable is that the Nigerian youths have been disproportionately implicated in defrauding victims all over the world (Akanle et al., 2016). Internet crimes are global issues (Kirillova et al., 2017; Wall, 2007; Yar, 2017), and millions of people with email accounts have undoubtedly encountered Nigerian scam emails (Rich, 2017). Consequently, recent years have witnessed an upsurge of research on victims of cyber-fraud that supposedly originates from Nigeria (Cross et al., 2018; Owen et al., 2017; Sorell and Whitty, 2019). We still, however, know very little about Nigerian cyber-fraudsters (Lazarus, 2018). Remarkably, no study has attempted to explore the narratives of officers who have close interactions with these cybercriminals, even though frontline law enforcement officers who routinely investigate, arrest, interview, interrogate and prosecute these cyber- fraudsters have insiders' insights. The narratives of these frontline law enforcement officers,

[1] "I went to Nigeria to meet the man who scammed me", retrieved: https://www.bbc.co.uk/news/world-africa-37632259

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

therefore, merit examination. This study asks: "what are the narratives of frontline law enforcement officers about cyber-fraudsters and their activities in Nigeria?".

This contextual inquiry concerns the Nigerian cybercriminals, the narratives of law enforcement agents on the ground about these cybercriminals, and the implications of these narratives. A primary objective of this study is to shed light on the characteristics of the Nigerian cyber-fraudsters. Doing so is prompted by a central motive: to enlighten government agencies around the world about these cybercriminals so that they are in a better position to: [a] understand the actions/features of these cybercriminals better and develop more effective response strategies; and [b] appreciate the vulnerabilities of their victims better and develop more adequate support schemes. The study examines life on the ground in Nigeria and Nigerian law enforcement officers' own thoughts about cyber-fraud and cybercriminals. Since situations must be understood from the inside, this article sets out to explore the narratives of people (social actors) regarding their fellow men and women, which are the most meaningful within their particular cultural dynamics. Since cyber-frauds are social products, they must also be read, in Hayward and Young's (2004, p. 259) words, "in terms of the meanings they carry." This article assesses the connections between the indigenous worldview and cyber-fraud activities, looking for, in Swidler's (1990) term, the empirical traces of "culture in action." In particular, it harnesses law enforcement officers' narratives on cybercriminals and their activities to shed light on how indigenous worldviews may be connected with offending in the virtual world. Henceforth, the article is presented in five sections [i.e. section 2 to 6]: Firstly, the literature review (section 2) attempts to position the research topic within the existing literature by providing an overview of

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

what we currently know, which helps to shed light on the phenomenon we are investigating. The literature review is followed by a theoretical background (i.e. section 3), which provides a lens from which to analyse, interpret and discuss data. The article then presents the remaining three sections in the following order: method (section 4), findings/discussion (section 5) and conclusion (section 6).

2. Literature review

2.1. Indigenous worldviews on wealth acquisition

Contexts are the resources for understanding "the ways in which local worldviews on wealth acquisition give rise to contemporary manifestations of spirituality in cyberspace" (Lazarus, 2019a, p.1). Indigenous spiritual worldviews are central to the discussion of wealth acquisition and the meaning of such wealth within the particular cultural dynamics from which they have emerged (Akanle and Adejare, 2018; Ellis, 2016). Many Nigerians "feed on the red blood corpuscles of the primal world and spiritual shrines" to generate material wealth (Kalu, 2002, p. 674; see also Ekeh, 1975). In this respect, "the intersectionality of the spiritual world and the acquisition of wealth" discussed in Lazarus's (2019a) recent work is revealing. While some Nigerians tap into religious resources for wealth accumulation, it is a misconception to group all such people into just one group (Lazarus, 2019a). Indeed, there is a distinction between benevolent and malevolent intentionality and, consequently, tapping into religious resources for wealth accumulation could be "licit or illicit" (Lazarus, 2019a, p.12). Either way, spirituality is a "critical factor in the activities of the criminals involved in organized and non-organized crimes"

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

(Melvin and Ayotunde, 2010, p. 364). Life in the virtual world embodies cultural nuances in society (Jones, 2018; Powell et al., 2018). Thus, Lazarus (2019a), by specifically exploring the occult economy in a variety of different manifestations, concluded that the physical world concurrently extends into the virtual world as far as the generation of wealth is concerned. The occult economy can be defined as the deployment, real or imagined, of spiritual/magical means for material ends (Comaroff and Comaroff, 1999). Given that earthly riches are believed by some Nigerians to have a spiritual aetiology (Ekeh, 1975; Ellis, 2016; Kalu, 2002; Lazarus, 2019a), this worldview has consequences for many Nigerian institutions.

Traditional shrines, churches, mosques, and many religious institutions generally serve as lubricants of commercial relationships' between spiritualist and many ordinary Nigerians (Ellis, 2016). In this way, the spiritual world maintains its efficacy as the true source of wealth and its cultural potency is continuously legitimized, produced, and reproduced through interactional processes between ordinary citizens and the spiritualists (Lazarus, 2019a). Through these processes, a client–patron relationship between the gate-keepers of the shrines and sacred sites and ordinary citizens is negotiated and nurtured (Ekeh, 1975; Ellis, 2016). In turn, the cultural and symbolic "handshaking" between clients and patrons not only helps to harness this type of relationship, but it also blurs the boundary between the meaning of "bribe" and that of "dash" (Lazarus, 2019a). "Dash" is a local term for a gift in a Nigerian context. The exchanges of "dashes" between the representatives of many institutions, such as banks and ordinary Nigerians, including cybercriminals, are commonplace (e.g. Aransiola and Asindemade, 2011; Ibrahim, 2017). The underlying factor is that, while bribery and corruption are symptoms and outcomes of

institutional deficiency (Dasgupta and Ugur, 2011), expertise in bribery has been culturally deemed necessary, and sufficient, for holders of public posts to be successful in Nigeria (Ellis, 2016). These money-oriented social/cultural processes in Nigerian society extend to cyberspace and, consequently, have implications for this article's positioning.

2.2. Cybercrime and cultural relativism

Many scholars (Bae, 2017; Donner et al., 2015; Hutchings and Chua, 2017; Ibrahim, 2016; Lazarus, 2019b; Selwyn, 2008; Yar, 2017) have observed that the term "cybercrime" is an umbrella term for a wide spectrum of crimes, such as revenge pornography, cyber-stalking, cyber-bullying, cyber-espionage, and cyber-fraud. For Wall (2007, p. 185), for example "cybercrimes are the product of networked computers, [and] must be defined in terms of the informational, networked, and globalised transformation of deviant or criminal behaviour by net- worked technologies". However, 'a computer may be materially the same, but placed in different cultures, a computer holds different meanings and generates different problems shaped by cultural factors in which the computer sits' (Jones, 2018 p. 18). To search for empirical clues of "culture in action" (Swidler, 1990), therefore, this study mobilizes marginal literature about the cultural dynamics of Nigerian cyber-fraudsters, as Cross's (2018) literature review suggested. The above author elaborated that the narratives of current cyber- fraud research are only reflective of the mainstream perspectives at the expense of the marginalised voices. In other words, the voices of scholars from the global South especially Nigeria, are ignored,

and by implication, the narratives of scholars from the global North exclusively inform the global cyber-fraud discourse. A better understanding of this phenomenon lies in our capacity to unconditionally value all insights across the global South and global North (Lazarus, 2018, Lazarus, 2019a). For example, "listed in the prevalence of cybercrime perpetrators, Nigeria, the United Kingdom, and the United States are at the top of the FBI's league-table" (Ibrahim, 2016, p.44). However, a critical analysis of the FBI's league-table has pointed out that the statistics the FBI relied upon to inform the state of cybercrime perpetrators across nations, even when they represent the underlying reality, are socially and selectively constructed (Ibrahim, 2016, pp. 50–52). Nigeria, arguably, is not less significant than nations from the global North.

While what constitutes cybercrime issues in most Western nations such as the UK and the US may involve many aforementioned types of cybercrime, the meaning of cybercrime in Nigeria is fundamentally rooted in socio-economics (Ibrahim, 2016). Therefore, in critiquing the dominant cybercrime classifications, Ibrahim (2016, p. 55), despite lacking primary empirical data, argued that "the conceptual 'pipelines' of the cybercrime in the Global North may not hold water in Nigeria" (see also sets of primary empirical data on the topic e.g., Ibrahim 2017; Lazarus 2018).

Thus, as Cross's (2018) work pointed out, the inclusion of Nigerian scholars' narratives is central and necessary to discussions about cyber-fraud, not least because they provide invaluable layers of explanation regarding the cultural dimensions of cyber-fraudsters. One way to rectify this type of omission is to mobilise literature about Nigerian culture that interacts with cyber-fraud presently

missing in the mainstream narratives (e.g. the lens of "digital spiritualization", Lazarus, 2019a, p. 3–5). Such aspects of Nigerian culture are "critical to building a more effective and holistic approach to target online fraud, not only within Nigeria but worldwide" (Cross, 2018, p. 261). Based on the preceding insights, this article relies on marginal voices more than the broader body of research on cybercriminals.

While one might be inclined to suggest that a broader canon of cyber- fraud (e.g. Button and Cross, 2017; Howard, 2009; Schoepfer et al., 2017) is needed in research on the cultural accounts of the agency of social control on cybercriminals, our strategy is based on the principles of cultural relativism. This strategy connects with the belief that one cannot impose meanings on another culture or context as each situation must be understood from the inside (Beirne, 1983; Ribbens McCarthy and Gillies, 2018). This strategy also connects with the belief that there are no "universal" "truths" about the contextual contours of digital crimes such as cyber-fraud (Ibrahim, 2016; Lazarus, 2019a). Accordingly, this current study goes in searches of "local truths" about cybercriminals through the lens of law enforcement officers on the ground in Nigeria.

Monetary benefits are central to the meaning of cybercrime in Nigeria, popularly referred to as "419 fraud" (e.g. Ibrahim, 2016; Igwe, 2007); historically, 419 is derived from section 419 of the Nigerian Criminal Code dealing with fraud. Though there are many types of cyber-fraud (Button and Cross, 2017; Schoepfer et al., 2017), here we examine multiple variations of Advance Fee Fraud (AFF) or 419 (Igwe, 2007; Rich, 2017; Whitaker, 2013). AFF is a confidence trick in which victims (e.g. victims

of romance scams) are deceived into advancing relatively small sums of money in the hope of realizing a much larger gain (Chang, 2008; Rich, 2017; Whitaker, 2013). This form of fraud (AFF or 419) is embedded in Nigerian history because they are social products and the term is directly coined from section 419 of the code. The online versions of AFF are locally known as "Yahoo-Yahoo" (e.g. Adeniran, 2011). The term "Yahoo-Yahoo" was coined based on the dominance of Yahoo emails, apps, and instant messaging in perpetrator–victim communications in the mid-2000s (Lazarus, 2018; Trend Micro and INTERPOL, 2017) during the Internet boom in Nigeria. The perpetrators of "Yahoo-Yahoo" were hence popularly called "Yahoo-boys" (Aransiola and Asindemade, 2011; Tade & Aliyu 2011).

2.3. Yahoo-boys and cultural cues

The term "Yahoo-boys" signifies that the perpetrators of the infamous "Yahoo-Yahoo" are predominantly male (Lazarus, 2018, p. 67). The use of emails served as the initial communication phase for some Yahoo-boys, and many victims have been deceived and defrauded all over the world (EFCC, 2018; Whitaker, 2013). Rich's (2017) comprehensive content analysis of a large corpus of AFF emails is revealing (see also Chang, 2008). These researchers observed that authors of AFF emails commonly use a "trust rhetoric" (e.g. Rich, 2017) and "authoritative and urgent" language (e.g. Chang, 2008) to defraud their victims. This body of research (e.g. Adogame, 2009; Chang, 2008; Rich, 2017) sheds light on cyber-fraudsters and their art of persuasive language. However, in recent years, "Yahoo- Yahoo" has shifted from merely sending multiple emails to unsolicited recipients to the targeting and

befriending of victims on dating websites or Facebook (EFCC, 2018). While Yahoo-boys generally prefer victims from foreign nations with high currency value (Akanle et al., 2016), remarkably, most victims of Yahoo-boys are swindled in the context of "love" and "friendship" with charms and magic (Lazarus, 2019a). Because "love" and "friendship" are specific aspects of "Yahoo-Yahoo" narratives (Lazarus, 2018), victims' plights are not only financial but also psychological (Cross et al., 2018; Ibrahim, 2016; Sorell and Whitty, 2019). Yahoo-boys control their "clients" (victims) with various spiritual means, such as invoking of spells on victims' photographs in shrines and communicating with them through words-of-power (locally known as "do as I say") on the telephone (Lazarus, 2019a). "Do as I say" spells or "words-of-power [can] unlock cosmic forces that can make the spiritual manifest into the physical" and, in this way, spells can be invoked or undone by words-of-power (Peavy, 2016, p. 101). While it may be critical to investigate the symbolic roles of love potions and the mystical powers that can make the spiritual manifest into the physical, there is a dearth of research on Yahoo-boys and the occult economy.

Accordingly, some interview studies refer to cybercriminals who defraud their victims with supernatural powers as "Yahoo-boys plus" (e.g. Melvin and Ayotunde, 2010; Tade, 2013). These prior studies (e.g. Melvin and Ayotunde, 2010) noted that only a group of cybercriminals make use of magic/spiritual powers to defraud victims, whereas no study has extended this implicit classification beyond this method of operation. This article sets out to fill this gap. The bottom line is that like some law-abiding Nigerians, the cybercriminals (Yahoo-boys) find the use of magical powers meaningful (Lazarus, 2019a) as exemplified in popular music. A recent study, which is the first to examine the representations of cybercriminals (and

cyber-fraud) in Nigerian hip-hop music suggests that cyber-fraud embodies the occult economy (Lazarus, 2018). Nowhere is the link between the occult economy and Nigerian hip-hop music more evident than in Kelly Handsome's song which depicted Yahoo-boys as follows:

"…Maga don pay/Mugu don pay/shout hallelujah…/…hallelujah owo…/…/…hallelujah ego…/… hallelujah, hallelujah kudi, kudi../I don suffer, but I now don hammer, papa God don bless me, no one can change it…/…

("The gullible has paid, the senseless has remitted/ shout hallelujah…/…hallelujah, hallelujah money…/…hallelujah, hallelujah money…./…/ hallelujah, hallelujah money, money…I have suffered a lot, but now I have hit the jackpot, Almighty God has blessed me, [and] no one can change it")" (Lazarus, 2018, p. 73).

The above song attributes the acquisition of wealth to "real or imagined" spiritual powers, but that is not all. While this prior study (i.e. Lazarus, 2018) noted that cybercriminals and musicians are connected, it has homogenised these cybercriminals as a single group. Bearing this in mind, this current study aims to bifurcate the characteristics of these criminals beyond the use of magical powers. Nonetheless, it is also remarkable that this type of lyrical representation shows that Yahoo-boys glamorize cyber-fraud.

So, while some researchers implicated poverty and/or unemployment as the causes of cyber-fraud among Nigerian youths (e.g. Adesina, 2017; Akanle et al., 2016), other

researchers have pointed out that conspicuous consumption (Ibrahim, 2017; Ojedokun and Eraye, 2012) and masculinity or "doing gender" (e.g. Lazarus, 2019b; Smith, 2017) are also fundamental to the discussion of "Yahoo- Yahoo." Since "Yahoo-Yahoo" is primarily motivated by monetary rewards and most Yahoo-boys implicated in such crimes have no employment records (EFCC, 2018), it is reasonable therefore to concede that crime may be one of the Yahoo-boys' ways of "doing gender, when legitimate means of demonstrating their masculinity are denied" (Lazarus, 2019b, p.10; see also Messerschmidt, 1993; West and Zimmerman, 1987). For symbolic interactionists (Carter and Fuller, 2016; West and Zimmerman, 1987), the concept of "doing gender" demonstrates the socially constructed nature of masculinity as developing out of repeated, patterned interaction and socialization processes.

Accordingly, cultural expectations of masculinity and femininity "perpetuate heterosexual male-domination over women" (Connell and Messerschmidt 2005, p.832) and, in Nigeria, men (and boys) are socialised to be sole bread-winners and the principal head of the household (Eboiyehi et al., 2016; Ibrahim, 2015; Smith, 2017), which increases their financial responsibilities as Lazarus (2019b) noted. On the flipside, women's possession of high economic power can have detrimental effects on their marriages and their chances of remarriage in Nigeria (Lazarus et al., 2017). Indeed, gender is a central source of social disadvantages that positions these women between exclusion and belonging (Lazarus, 2019b). "In virtually every arena of Nigerian men's lives, money's value is closely tied to the social work that it does in men's relationships with women" (Smith, 2017, p. 160). Since gender-category membership is attached to the cultural expectations and performativity (Connell and

Messerschmidt 2005; West and Zimmerman 1987), in this context, "men's cultural positionality in society influences them to be generally more 'desperate' to achieve financial success than women online" by any means possible such as cyber-fraud (Ibrahim, 2016, p.54). So, the meaning "wealth" has for men in relation to women may be related to the predomination of young men being involved in "Yahoo-Yahoo." Cultural contexts in Nigeria "serve as a resource for understanding gender and crime connections, and offer additional layers of explanation" (Lazarus, 2019b, p.10). These cultural forces resonate with the view that gender is constructed through interaction and that men and women are culturally assessed for their gender performances in both interactional and institutional contexts (Carter and Fuller, 2015; West and Zimmerman, 1987). Closely related to the above are the expectations of people in tertiary institutions and the associated consequences.

Dominant perspectives further suggest that education increases the returns to legitimate work, and legitimate work generally raises the opportunity costs of offending (e.g. Lochner, 2004; Machin et al., 2011). However, university education does not by itself provide an automatic ticket to conventional employment or economic stability in Nigeria (Ibrahim, 2016). Even if a graduate secures legitimate employment, many conventional occupations leave workers vulnerable to financial predicaments that imperil their capacity to provide for themselves and their dependents (Smith, 2017). In these contexts, research on cybercriminals in universities has demonstrated that young adult male Nigerians, mainly university students/graduates, constitute the bulk of cyber-fraudsters (Aransiola and Asindemade, 2011; Ojedokun and Eraye, 2012; Tade, 2013; Tade and Aliyu, 2011). While one may be inclined to point out that the selective sample of these studies (i.e.

solely university students) may have shaped their findings, Ibrahim's (2017) interview study, which explored the views of 17 Nigerian parents, agreed with the above authors. A more critical issue is that as Helfgott (2013) and Payne (2018) noted, researchers value using a categorisation approach to studying crime and criminals. Such an approach, for example, helps to map out 'links between different types of behaviors within specific crime categories' (Payne, 2018, p.18). "Knowing the social and situational-contextual factors that distinguish particular categories of criminals is crucial to theoretical understanding and policy practice" (Helfgott, 2013, p.21). However, no study has considered classifying the Nigerian cybercriminals on the basis of critical themes in literature such as musicians-cybercriminals linkages and university education. To fill this gap (and extend the existing classification beyond the issue of spirituality as previously mentioned), it is critical to explore the narratives of the Economic and Financial Crimes Commission (EFCC) frontline agents. As far as this current study is concerned, no study has sought the narratives of the Economic and Financial Crimes Commission (EFCC) frontline agents (or law enforcement officers for that matter) regarding Yahoo-boys.

2.4. The Economic and Financial Crimes Commission (EFCC)

The EFCC was established in 2002 primarily to deal with all "corruption issues" in Nigeria (Obuah, 2010; Pierce, 2016), as corruption is a complex social, political, and economic phenomenon that affects all countries (UNODC, 2017). Some researchers claim that, in Nigerian society, political impunity, bribery, and corruption have created a social environment in which fraudulent practices are normative for

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

ordinary Nigerians (Pierce, 2016; Smith, 2008). Therefore, the EFCC was established to serve as a national coordinator for investigating money laundering and other economic crimes (Obuah, 2010; Pierce, 2016; Umar et al. 2016). Regional policy responses to crime problems are the concerns of international communities (Newburn and Sparks, 2004) and the concerns of international communities in particular played a role in motivating the Nigerian government to set up the EFCC (Obuah, 2010; Umar et al. 2016) and update its laws. Nigeria enacted the 2015 Cybercrime Act to "provide an efficient and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime in Nigeria" (Cybercrime Act, 2015).

The EFCC is the law enforcement agency that investigates and prosecutes financial and economic crimes such as AFF, corrupt practices, illegal bunkering, tax evasion, and all aspects of money laundering in Nigeria (UNODC, 2017). No human organization is perfect, however, and there are often corrupt officials within law enforcement institutions (Reiner, 2010). For example, some re- searchers have implicated prominent politicians in using the EFCC as tools to oppress and intimidate their political opponents (e.g. Adeniran, 2011). Despite such challenges, the EFCC has been acknowledged in general academic research (Pierce, 2016; Umar et al. 2016) and media discourse (The Nation, 2017) as having had substantial achievements and "zero tolerance for corruption and fraud." In 2017, it was reported that the agency had secured 340 convictions in six months and recovered millions of dollars (e.g. The Nation, 2017). Also, until the creation of the EFCC, law enforcement in Nigeria had been exclusively focused on crimes of the powerless, such as the youth, rather than the powerful, such as corrupt bankers (Pierce, 2016). Indeed, "the

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

creation of the EFCC in Nigeria marked a significant shift from rhetoric about fighting corruption, fraud and money laundering to actually fighting these types of crimes" (Obuah, 2010, p. 24). Since the EFCC is the principal law enforcer of 419 fraud/AFF, the narratives of the frontline EFCC agents will, in Polkinghorne's (1988, p. 19) words, "serve as a lens through which the apparently independent and disconnected elements [of cyber-fraudsters] may be seen as related parts of a whole" (see also Longo, 2015). While many studies have benefited from the interactionist perspective, as Carter and Fuller (2015) noted, no study on cybercrime has used the interactionist perspective in a Nigerian context as far as this research is concerned. This study goes in search of the empirical traces of "culture in action" (Swidler, 1990). Consequently, it will benefit from the symbolic interactionist basic premises, based on the above discussions (e.g. masculinity, occult economies, and local worldviews).

3. Theoretical background

This study will benefit from the symbolic interactionism position, which rests on the three premises of Blumer's (1969b/1998, p. 2) original formulation. The first premise is that the meanings that the things and social objects (persons) have for people are the basis of their actions. The second premise is that these meanings are derived from social interactions. The third premise is that these meanings are modified in the process of interaction of individuals over time. There is no objective viewpoint for the critique or compliment of an "immoral" act (Becker, 1967/1997; Reiner, 2016). Indeed, 'people's experience of the world is always mediated by culturally defined

meanings, which, although adopted by their personal experience, condition how and what they conceive as reality in their narratives' (according to symbolic interactionist perspectives) (Longo, 2015). Arguably insights from symbolic interactionist perspectives will be useful to make sense of the narratives of officers regarding cyber-fraudsters (fellow Nigerians).

4. Methods

4.1. Participant description and interview data

This study sought the views of EFCC officers concerning Nigerian cyber-fraudsters (Yahoo-boys) and their operations. To explore the narratives of law enforcement officers regarding Yahoo-boys, 40 EFCC officers (70% male and 30% female) from two Nigerian cities (Abuja & Lagos) were recruited. While many agents of state apparatus have been implicated in corrupt practices (Ibrahim, 2017), EFCC officers strive to draw a clear line between the agency and corrupt institutions in Nigeria (Umar et al., 2016). In this context, EFCC officers, if interviewed by "outsiders" outside the agency, could, for example, easily be accused for "passing sensitive information to outsiders" for material gains. This explains why, to date, to the best of our knowledge, no one has been able to access this "hard-to-reach data." However, we circumvented this practical problem by adopting an innovative strategy.

Because one of the authors is an EFCC officer as well as a researcher, the authors were able to access the "impossible" data set. The involvement of the officer as a researcher (i.e., "insider-researcher") facilitated access negotiations with other

gatekeepers and helped the research team to develop a high level of rapport with the interviewees. The establishment of rapport between a respondent and the interviewer, or lack thereof, is a critical aspect of the interviewer gaining the respondents' cooperation to complete a meaningful interview. Also, because the interviewer and interviewees were members of the agency (EFCC), they were able to harness a deep, in a Weberian term, "verstehen" (understanding) of their roles while having open and engaged discussions on topics that may not have been otherwise possible. While interviews are products of social encounters involving co-construction, mutual agreement, and trust (Morris, 2018; Ribbens, 1989), the "insider-researcher" emphasized confidentiality/anonymity and informed fellow officers that the study was to gather data for academic research on the subject.

To increase the level of rapport between the interviewer and the interviewees in this study, the "insider-researcher" recruited and individually interviewed fellow officers (70 to 80 minutes each). All officers were interviewed in the EFCC headquarters in Abuja, with the officers based in Lagos being interviewed during their various assignments in the headquarters. Involvement in the study was formalized through the obtaining of the interviewees' consents for the interview. Officers (interviewees) were asked about their experiences with offenders, particularly the cybercriminals' characteristics. The importance of sharing their thoughts about cyber- criminals with a fellow officer who was also a researcher appears to have encouraged the participants to consent to the interviews. Gathering data from law enforcement officers about criminals is consistent with prior research such as Hutchings and Chua's (2017) study which interviewed Australian police officers. In-depth, semi-structured interviews were used, and all interviews were

tape- recorded and transcribed verbatim. The selection criteria were that the officers had at least four years of work experience as a frontline law enforcement agent and at least a university degree.

These officers were considered to be appropriate interviewees for our study because they had worked on a significant number of cases regarding cyber-fraudsters according to EFCC's (2018) records. Participants ranged in age from 27 years to 52 years, and their work experience ranged from five to 14 years. A total of 26 frontline investigators and 14 frontline prosecuting lawyers were interviewed between September 2017 and January 2018. While the investigating officers routinely interview complainants and suspects, including Yahoo-boys, they also interrogate them when necessary. Additionally, they give testimony in court for the prosecuting counsel (lawyers). The lawyers (prosecutors) are responsible for crime-data synthesis and prosecuting EFCC cases, including cyber-fraud. The reason for their inclusion was that lawyers' courtroom experience in cyber-fraud cases might complement that of the investigators in generating a rich data set. Enhanced by in-group trust and rapport, the interviewees, due to the role that the "insider-researcher" played as the interviewer and an EFCC officer, provided significant insights into the topic. Given that our data would have been almost "impossible" to reach without the interviewer's in-group membership, we believe that the data we present in this study is priceless. Data was subjected to the principles of a directed approach to qualitative content analysis (DAQCA) (Hsieh and Shannon, 2005).

4.2. Identification of themes and coding of data

In line with DAQCA (Hsieh and Shannon, 2005), data were coded and analyzed as follows. First, coding began with reading the transcripts and highlighting all text that, on first impression, appeared to represent critical aspects of the materials gathered. The next step in the analysis was to code all the highlighted passages using predetermined codes, because "the goal of a directed approach to content analysis is to validate prior research or theory" (Hsieh and Shannon, 2005, p.1281). So, we derived the sensitising concepts from the main themes of the literature review: [1] "socio-demographic and gender," [2] "spiritual dimension of cyber-fraud", [3] "university students/graduates," and [4] "popular music and cyber-fraud connections". These themes served as an initial and sub- sequent framework to highlight and recognise themes from the data, as suggested by Hsieh and Shannon (2005). While the above four themes identified in the literature were the high-level codes we used, these themes intertwined with our empirical data. Because different coders may vary in their interpretation of the text's content, inter-coder reliability is essential (Hruschka et al., 2004; Hsieh and Shannon, 2005). Accordingly, two researchers independently coded the data. While one researcher coded the whole data, the other (i.e. insider-researcher) reviewed 30% of the data set with the same codes from the literature review (previously mentioned). The degree of similarities between both coders was 98%. It is conceivable that DAQCA has some inherent limitations in that re- searchers have approached the data with an informed but unintended bias to some extent. The researchers, however, "tested" to see if these themes outlined in the literature and background information appeared as expected. Also, most respondents (n = 34) went straight to the main themes in the existing literature such as "male domination of cybercrime," in their first response without further probing questions. The following is an example of the first interview question: Interviewer: "My first question is, based on your experience as a law

enforcement officer, how do you describe or define the main perpetrators of cybercrime in Nigeria?" Respondent (over five years of experience): "Oh, you mean the boys that normally go to the Internet to defraud people?"

This type of dialogue suggests that the core limitation of a DAQCA did not have a substantial negative effect on the findings. All direct quotes presented below represent widely shared beliefs of the social control agents interviewed involving the following findings: social-demographic features; the bifurcation of Yahoo-boys; and masculinity and material wealth. These are discussed sequentially below.

5. Findings and discussions

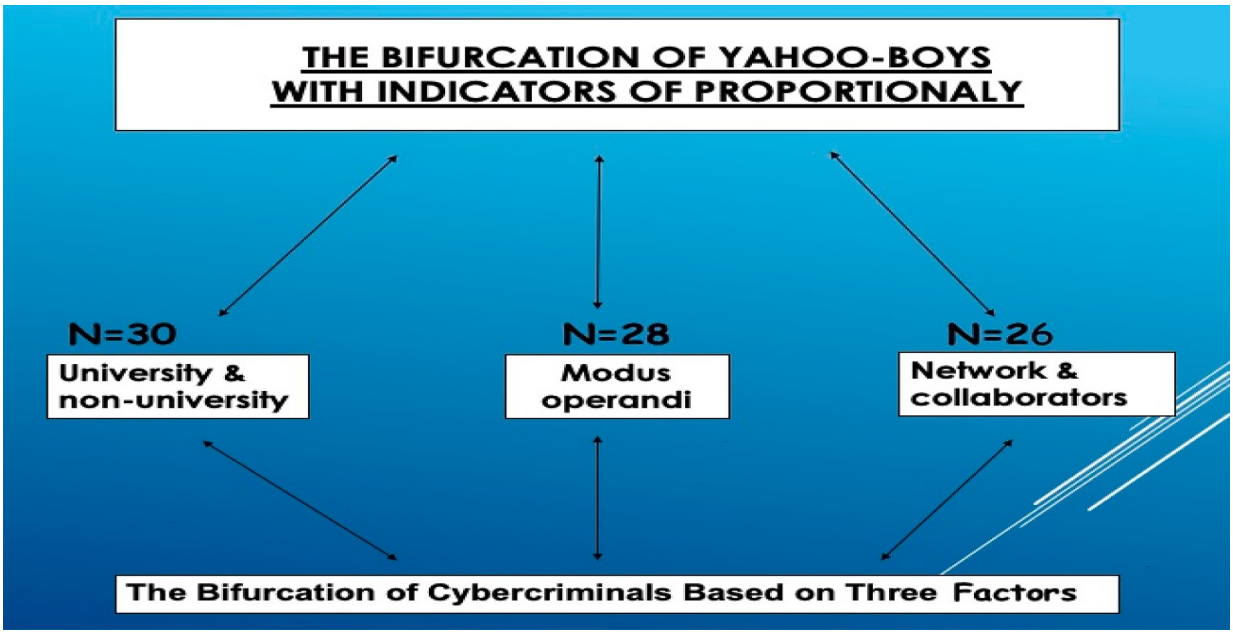
5.1. Socio-demographic features

All interviewees (n = 40) reported that Yahoo-boys are predominantly young male university students and graduates. However, 30 participants reported that the socio-demographic features of these cyber-fraudsters are diverse and include people from affluent, poor, Christian, and Muslims backgrounds. For example, in the words of one prosecutor (over 10 years of experience):

"I can say concerning the perpetrators of cybercrime really, I think there are certain stereotypes that are there, which may not necessarily be the truth. We expect that every Yahoo-boy is that somebody [paused], even the idea that you call him a

Yahoo-boys paints an image in your mind that he is a young man, university educated, conversant with the computer and internet, but it is not normally the case... based on my experience as a law enforcement agent, I can say that regardless of economic background or tribe or religion and all that, any ye-ye person [good-for-nothing person] who wants to make it fast in Nigeria goes into internet fraud. Number one, the internet gives anonymity, and low risks. You know, because no police or army checkpoints are online [because no perfect security online]. Secondly, the Internet is a flow, no boundary. It gives you access to people [victims] in real time, quick, quick ... there's no barrier online, and for example, they don't need a visa to talk to somebody in the UK."

Figure. 1. The bifurcation of Yahoo-boys with indications of proportionality.



Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

Notably, the last sentence is reminiscent of Wall's (2007, p. 185) observation that life online has the capacity for distributing "peer to peer networking and a panoptic gaze that creates an asymmetric ability to enable one person to simultaneously reach many." Equally, despite the idea the there is no clear boundary between cyber-fraudsters and non-cyber-fraudsters, interviewees (n = 40) stated that, based on their experiences on frontline duties as EFCC officers, cyber-fraudsters are exclusively "young" males. It is noteworthy that the chronological meaning of "age" as the dominant benchmark for the definition of "youth" does not hold true across cultures (e.g. in Nigeria). The determinants of "youthhood" in a Nigerian context transcend age and encompass multiple cultural dimensions such as political affiliation and positionality as well as marital status. The underlying idea is that, while some Nigerian researchers have implicated "youths" as responsible for the bulk of cyber-fraud originating from Nigeria, some of these researchers (e.g. Jegede et al., 2016) use the cultural meaning of "youth/age" rather than the chronological meaning because they also include people above 30 years of age as "youths." In fact, critical perspectives suggest that the meanings of youthhood are not constituted similarly across cultures (e.g. Cain, 2000). Therefore, it is conceivable that the meaning of "young men" or "youths" in Nigeria is culturally constructed and must be read in terms of the definitions they carry in a Nigerian context.

5.2. The bifurcation of Yahoo-boys

Apart from the demographic characteristics of Yahoo-boys, some respondents divided Yahoo-boys into two main groups (Yahoo- boys-digital and Yahoo-boys-

analogue) based on their experiences as frontline law enforcement officers. As shown in Fig. 1, the bifurcation of Yahoo-boys was not only based on educational background (n = 30), as previously noted, but also included other characteristics (e.g. "network and collaborators," "modus operandi").

Support for the distinctions between these broad groups of Yahoo-boys in the majority of the officers' reports is exemplified by the following responses:

"The word 'analogue' and 'digital' is just a reference point. Yahoo analogue are those people who are local, opportunists, without a secondary education, they see Yahoo-Yahoo, and they jump into it. If you look at their patterns, they are quite different from those who have passed through universities or those who are fully educated or those who studied info-tech. You see, they are two different sets of people, and their modus operandi, everything, are different. Somebody who just picked up the trade from the street would not be as advanced as somebody who has acquired university education…passed through the educational process … So, they are two different people." (Male investigator with over 11 years of experience):

"The Yahoo-boys-analogue generally sends thousands of scam emails to potential victims. They do it randomly, and pray that some of targets would respond … give them their pictures or send them personal items. They would now work on the victims' photos in shrines to cast spells on them and remove difficulties in controlling and manipulating them for financial purposes. But the digitally advanced Yahoo-boys, I think, do not rely on juju [spiritual/magical powers] a lot. Because they rely on advanced tech to defraud victims. You can even see all these

differences when you arrest them and search their apartments. Sometimes, you find a lot of spiritual items, victims photos in private juju alters and some amulets. They [these types of evidence] tell you the type of person you are dealing with." (Male investigator with seven years of experience)

5.2.1. University and non-university education

As previously emphasized, Yahoo-boys can be divided into two broad groups based on education and those who have a university education are quite different from non-university educated Yahoo-boys. Education is the engine of social mobility in modern society, whereby the time people spend in education may limit the time they are available for participating in criminal activities (e.g. Hjalmarsson et al., 2015; Machin et al., 2011). These authors' ideas do not necessarily apply to "Yahoo-Yahoo." The time people spend in Nigerian universities does not limit the time they are available for participating in "Yahoo-Yahoo." Everyone can be an achiever once the skill sets are acquired on the street. However, Yahoo-boys who generally get ahead in "Yahoo-Yahoo" business ventures and are most sophisticated in the "scam game" are the university-educated Yahoo-boys, according to most respondents. Individuals who have higher educational attainment are most likely to have a higher level of connections with the broader body of educated Nigerians in higher socio-economic positions. The higher levels of exposure to the elite group and technological environments may also be related to advanced knowledge and skills in technology.

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

Similarly, previous research on crime and education linkage has suggested that education can also increase the earnings from crime as specific skills acquired in school may be inappropriately used for criminal activities (e.g. Lochner, 2004; Machin et al., 2011). Yahoo-boys-digital (university-educated cyber-fraudsters) are not only more advanced than those who are non-university educated, they are also more difficult for law enforcement agents to criminalize because in the words of one respondent, "they [Yahoo-boys-digital] are always conducting their own research even more than law enforcement." Like the EFCC in Nigeria, law enforcement agencies in general, even in most advanced nations, as Broadhurst (2006, p. 4) noted, "play catch-up with cyber-savvy criminals." Equally, while one might question why college education may be needed in "Yahoo-Yahoo" business, email scams are saturated with unskilled or average computer users, and technological expertise and English language proficiency are currently needed to succeed in "Yahoo-Yahoo" contexts. A total of 30 participants not only suggested that a large number of university students/graduates and non-university students/graduates are involved in perpetrating cyber-fraud, but they also supported the distinctions between the groups of Yahoo-boys based on the theme: "university and non-university education." For example, ac- cording to one investigator (over 11 years of experience):

"The digital Yahoo boys are more advanced. As an investigator, if you are dealing with a Yahoo analogue group, the applications they normally use are the ones you can buy online. But Yahoo-boys-digital, they don't just buy applications online, they've people who design them [Trojan or other malicious software applications] according to their needs. They've their contacts who they can just say, do this and

this for me; I want a computer program that can perform this, maybe a Trojan horse that can perform specific duties. He tells the programmer, this is how I want the Trojan to work, behave and all that. Because Yahoo-boys-digital have more analytic minds than Yahoo analogue guys. The digital guy would take his time, study the system, identify weaknesses, think of how to beat the system. So, if you look at the systematic way, you would see that the digital boys are more difficult to catch. And that also indicates that they make more money than Yahoo analogue ones."

It is noteworthy that there is a general consensus in existing studies (e.g. Jegede et al., 2016; Ibrahim, 2017) that university students and graduates (including dropouts) are the main perpetrators of cyber-fraud that emanates from Nigeria. Similar to existing studies, our current study supports the idea that Nigerian university students/graduates are the major culprits in terms of "Yahoo-Yahoo" business. Unlike extant studies, however, our current study has, through the bifurcation of Yahoo-boys, deconstructed the homogenization of Yahoo-boys as one group under the umbrella of "university students/graduates." As one agent described it, unlike Yahoo-boys-analogue, "the more sophisticated we [agents] become, the more re-organized with their complex syndicates they [Yahoo-boys-digital] become."

5.2.2. Modus operandi

Since some Nigerians believe that true wealth is rooted in the spiritual realm, they view those who have the knowledge to appease the gods and ancestral spirits as

being rewarded in material terms (e.g. Lazarus, 2019a). The interviewees (n = 40) mentioned the issue of "spiritualism in cybercrime.", which aligns with the existing interview studies (e.g. Melvin and Ayotunde, 2010). In particular, it was observed that Yahoo-boys-analogue tended to use magic powers more than Yahoo-boys-digital in their attempts not only to defraud victims but also to avoid prosecution. To avoid prosecution here means that these criminals use spiritual/magical powers to: [a] increase the chances of their crimes escaping the EFCC officers' surveillance and [b] reduce chances of the EFCC officers investigating their crimes. In a similar vein, Frankle and Stein (2005) noted: many peoples do not distinguish in practice between technological knowledge and magical knowledge. In line with Frankle and Stein's (2005) insights, we argue that with regards to online frauds that emanate from Nigeria, the line dividing goals of technological knowledge and magical knowledge is blurred (see also Lazarus, 2019a). Thus, it would be an oversight to pay attention to one and ignore the other.

Indeed, the goals of technological knowledge and mystical knowledge in the "Yahoo-Yahoo" context are the same: to maximize benefits; and to avoid prosecution. However, there are notable differences between these two spheres of knowledge. One might argue, as Malinowski (1954/2014, p. 17) pointed out, that "we do not find magic wherever the pursuit is certain, reliable, and well under the control of rational methods and technological processes." Hence, it is conceivable that cyber-fraudsters who rely more on magical knowledge (Yahoo-boys-analogue) than technological knowledge may be facing a less certain situation in "Yahoo-Yahoo" business than the Yahoo-boys-digital group. It is plausible that higher computer/technology expertise reduces the uncertainty associated with "Yahoo-Yahoo" business ventures such as the trial-and-error scam email format popularly

used by the Yahoo-boys- analogue category. Equally, it is conceivable that Yahoo-boys-analogue, facing a technological competition they cannot win (Yahoo- boys-digital group always does), they subscribe to the occult economy to achieve their goals. A more critical issue is that our current study helps to illuminate the specific category of Yahoo-boys that usually depend more on mystical powers in cyber-fraud perpetration that originates from Nigeria. A total of 28 participants supported the distinctions between the groups of Yahoo-boys based on the theme "modus operandi." In the language of one investigator:

"Yahoo digital depend mostly on 'info tech' ... another thing about Yahoo analogue is that you see most of them dey use juju [magical and spiritual powers] to operate [you see, most of them use magical powers to defraud their victims]. In the sense that when they start communicating with you [referring to victims], they would put your picture under their laptop. Even some of them use blood, cut their hand and put the blood on the picture and all that. You see, that is the way of a typical Yahoo analogue guy."

These narratives from the agent support the observation that Yahoo-boys-analogue associate mostly with spiritualists who usually assist clients with their spiritual needs. This category of cybercriminals depends on the spiritualists more than their counterparts (i.e., Yahoo-Boys digital group) which resonates with the view that people do not generally subscribe to magical/spiritual powers wherever the pursuit is certain, reliable, and well under the control of rational methods and technological processes. To put a victim's picture under their laptop symbolizes the spiritual

dimension of cyber-fraud because it is a ritualized practice commonly prescribed by spiritualists. After the spiritualist (native doctor) might have "worked on" the picture (cast a spell on it possibly in his/her shrine), it is then necessary and sufficient for fraudsters to simply place the photograph under the computer while chatting/messaging the victims of fraud. Also, in the words of one respondent, "fraudsters also talk to the [victims'] pictures repeatedly" which represent the words-of-power ("do as I say" rhetoric), this being a spiritual way of manipulating victims for material rewards. It may be plausible that the "authoritative language" (Chang, 2008) and "trust rhetoric" (Rich, 2017) commonly used by some cybercriminals to communicate with their victims could be linked to "do as I say" rhetorical spells or words-of-power. If cyber-fraudsters believe they have spiritual authority over victims, they may be more inclined to deploy excessive "authoritative language" than otherwise. This spiritual worldview illuminates how, and to what extent, the relationship between the spiritualists and Yahoo-boys-analogue is a critical dynamic for the social construction and negotiation of identity and belonging in "Yahoo-Yahoo" contexts. It also illuminates Kalu's (2002, p. 674) idea that some Nigerians could be viewed as "feeding on the red blood corpuscles of the primal world and spiritual shrines in rural areas," as mentioned previously. The spiritual manipulation of victims highlighted here, indeed, urges cyber- fraud researchers "to look beyond normal 'scientific evidence' and consider the traces of spiritual manipulations of victims for material gains that are all too often ignored in 'normal' social science" (Lazarus, 2019a, p.1).

Notably, previous studies (e.g. Melvin and Ayotunde, 2010; Tade, 2013) have explained that Yahoo-boys exploit the spirit world to maximize their chances of

success in defrauding victims online and called them "Yahoo-boys plus." While our current study builds on these existing bodies of knowledge, it finds that it may be misleading to dichotomize or homogenize Yahoo-boys solely based on the exploitation of the spiritual world for wealth accusation. The dichotomization of these cyber-fraudsters (Yahoo-boys-analogue and Yahoo-boys-digital) includes other factors such as networks and collaborators in the social domain, which supports the notion that the cyberspace is a mere extension of the indigenous worldviews in Nigerian society.

5.2.3. Networks and collaborators

While Yahoo-boys-analogue associate more with spiritualists than Yahoo-boys-digital, the latter exclusively have connections with new music industries and musicians. In other words, some musicians and Yahoo-Boys 'reciprocally construct the destiny of one another' (Lazarus, 2018, p.74). According to Lazarus's (2018) study, while some musicians and Yahoo-boys are "birds of a feather that flock together", the core aspects of their relationship are based on reciprocal economic benefits and determined by them. This study grouped Yahoo-boys as one group in its analysis of con-artists' and musical-artists' connections, whereas the current study sheds more light on this linkage. Unlike Yahoo-boys- analogue, Yahoo-boys-digital predominantly "club together" with musicians who represent them in their lyrics. For Blumer (1969a), interaction occurs within a particular social and cultural context in which physical and social objects (persons), as well as situations, must be defined or categorized based on individual meanings. Accordingly, the interactions

and social intercourses between musicians and Yahoo- boys were critical in what one respondent called the "cybercrime money laundry." And a total of 26 participants supported the distinctions between the groups of Yahoo-boys based on the theme of "networks and collaborators." According to investigators:

"But for those who are really educated [Yahoo-boys-digital] they invest the money and through that investment, they launder the money. If you look at all these new music industries, most of them are used to launder money. Let me give you an example, if you listen to one music, Oshozondi by Slimcase. Have you heard of it before? [researcher responded, no!]. If you listen to Oshozondi, he listed names of all the popular Yahoo Boys in Lagos. You understand. These are some of the differences [difference between the two groups of cyber fraudsters]." (Agent with over ten years of experience).

"Let me tell you; almost all the music labels that you see, they are being owned by Yahoo-digital guys. And that is why you need to study what we call, 'cyber money laundering'! … Because people would buy different properties in the name of music industries owned by Yahoo-boys [digital]. They're the ones who have registered music industries to cover the actual fraud that they are doing. They're making it, industry, industry, industry, but if you ask them where do you get the money to establish those companies, all those music industries, they cannot justify it. That's where the cyber money laundering is coming in now." (Agent with 12 years of experience).

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

It is conceivable that the link between Yahoo-boys-digital and musicians explains why the former (unlike Yahoo-boys-analogue) invest their income in the music industry in Nigeria. The Yahoo-boys-digital also have an extensive network that includes not only bank clerks who may assist ordinary Yahoo-boys-analogue to withdraw fraudulently obtained money without questions, but also hi- tech bankers. One male investigator described the involvement of these bankers in cybercrime money laundering as follows:

"For every transaction, they [corrupt hi-tech bankers] get 15%. Let me give you an example, like POS [point of sale]. For every POS, there's a particular threshold attached to that transaction. It means that an account is attached to POS, it might say that it cannot receive let's say credit transaction of more than two million a day. Somebody managing the POS programmed from the bank, maybe the network administrator or the application manager. What this boy [Yahoo-boy-digital] would do if he wants to move or receive a larger sum of money; he needs somebody with a company account. Yes? But that company has a threshold, let's say two million or five million. They [Yahoo-boy-digital] now need bankers to activate what we call 'code 002' which is a security dial monitoring the credit of that POS account. So, the IT guy in the bank can switch it off for the fraudulent money to enter. And the money would enter. It would not raise the alarm. You see he [the banker] has aided and abetted crime because he has 15% of the money."

Even if many legitimate occupations leave most workers vulnerable to financial difficulties that imperil their capacity to provide for themselves and their

dependents, bankers are not one of the poorest group of workers in Nigeria. Therefore, it is simplistic to assert that poverty may primarily motivate their actions. It is plausible that the corrupt bankers described above were acting toward material wealth on the basis of the meanings their collaborators (Yahoo-boys) have for them. If representative, legitimate institutions aid and abet cyber-fraud to add to their legitimate income streams. It suggests that there is a fine line between the cultural meaning of "Yahoo-boys" and some claiming to be law-abiding Nigerians. As indicated in the above narratives, the seeming boundary between Yahoo-boys and some representatives of legitimate institutions, such as bankers, is blurred because they engage in similar practices that constitute fraud and corruption.

Additionally, based on the above narratives, it is reasonable to deduce that corrupt bankers symbolize a store of value because wealth-in-people (e.g. bankers) could easily translate into wealth-in-money in "Yahoo-Yahoo" contexts. To have strong allies and networks of bankers is arguably a useful asset in the accumulation of wealth in "Yahoo-Yahoo" businesses. Similarly, previous studies (Aransiola and Asindemade, 2011; Ibrahim, 2017) have indicated that Yahoo-boys collaborate with bankers to maximize their chances of success in "Yahoo-Yahoo." Our current research, however, demonstrates that it is misleading to homogenize Yahoo-boys as a single group with respect to three related features: "university education;" "networks and collaborators;" and "method of operation." Concerning the links between legitimate institutions (banks) and the cyber-fraudsters, while Yahoo-boys-analogue commonly associate with junior bank officers, Yahoo-boys-digital group "club together" with senior bank officers. They generally collaborate with high-level bankers such as network administrators and application managers. The critical point

here is that in gift giving (e.g. bribery or "dash") the honor of giver and recipient are reciprocally engaged and gift exchanges represent ritualized bonding between the giver and the receiver (Droz and Gez, 2015; Mauss, 1925). While gift exchanges may strengthen the bond between the Yahoo-boys-digital group and high-level bankers, the lack of such exchanges may weaken the bond between high-level bankers and Yahoo-boys-analogue and limit their chances of "moving up the ladder" (social mobility in criminal career), given that collaborators are the integral part of "Yahoo-Yahoo." What is less distinguishable among Yahoo-boys is their lifestyle; we found that they generally live extravagant lifestyles, which supports previous studies (Lazarus 2018; Ojedokun and Eraye, 2012). The above issue (extravagant lifestyles) deserves a closer examination.

5.3. Masculinity and material wealth

Masculinity develops out of repeated, patterned interaction and socialization processes (West and Zimmerman, 1987). Men are culturally socialized to be the head of the household in economic terms and are expected to translate economic power into social prestige from time to time (Ibrahim, 2017; Lazarus et al. 2017; Smith, 2017). For example, a Nigerian man who has economic power, irrespective of his age, under customary and Islamic types of marriages, can marry multiple wives (Lazarus et al., 2017). Culturally, even his adultery is often seen in society as a prestigious act (Chinwuba, 2015; Smith, 2017). A total of 29 officers had a shared belief that men are more culturally expected to have economic power than women; for example, according to a female investigator with 12 years of experience:

"Our culture is that a man as a man you have to take the girl o-u-t! And when a man has one, two, three of them [women], he has to find means to support them. You see, some married men have concubines. You also see some married men; their religion allows them to marry three, four! So, a man with four wives in a culture where the man has to be the provider, the bait would be much more for him than women whose business it is to receive and look good."

Indeed, the manifestation of conspicuous consumption in Yahoo-boys' lives has to be understood as a masculinity performance. The cultural and social positionality of Nigerian men as reported above resonates with Lazarus's (2019b, p.10) position that "men's hegemonic role in cyber-fraud as perpetrators is the mirror of, and made possible by, women's subordinate positionality in society". 'In virtually every arena of Nigerian men's lives, money's value (and its stigma) is closely tied to the social work that it does (or fails to do) in their relationships with other citizens' (Smith, 2017, p. 160). Young men generally fasten their aspirations on material wealth and "assemblage of goods," to live a meaningful life according to the dictates of the Nigerian society (Ellis, 2016). When a man spends money on occasions such as his parents' burial rites, girlfriends' parties or wedding ceremonies, "part of what he is doing is converting wealth into prestige" (Smith, 2017, p. 210). In Blumer's (1969b/1998, p. 4) words, "[T]he meaning of a thing for a person grows out of the ways in which other persons act toward the person with regard to the thing." Thus, "doing gender" for Yahoo-boys is unavoidable because gender-category membership is attached to the allocation of power and cultural expectation for men to generate

wealth (almost by any means necessary). Accordingly, the symbolic meaning of material wealth here underscores that it embodies not only a mechanical reflection but the imputed sentiments.

For Cooley (1909/1998), the thing that moves us to our pride or our shame is not the mere mechanical reflection of ourselves, but an imputed sentiment and the imagined effect of this reflection upon another's mind and society. Given the socially constructed nature of masculinity as developing out of repeated, patterned interaction and socialization processes (West and Zimmerman, 1987), the seemingly obvious officers' narratives on Yahoo-boys are far from straightforward. The Yahoo-boys' actions in the virtual world must be read in the light of cultural cues on wealth generation and masculinity as well as the glamorization of wealth in the broader Nigerian society. The social communities of Nigeria glamorize wealth irrespective of the source of the wealth (Adeniran, 2011; Ibrahim, 2017; Lazarus, 2018). The fraudulent actions of Yahoo-boys are even glamorized in Nigerian popular music (Lazarus, 2018). This reinforces the notion that life online is a mere extension of life in society (Lazarus, 2019b; Mumporeze and Prieler, 2017).

6. Conclusion

While this study has examined the intersections between cultural factors and information and communication technologies, it is the first study to explore the narratives of EFCC officers in bifurcating Yahoo-boys and their operations. While

prior studies, for example, indicated that only a group of cybercriminals deploy spiritual and magical powers to defraud victims (i.e., modus operandi), our study has extended this classification into more refined levels in its bifurcation of cybercriminals. 'Distinguishing between categories of criminals is critical to theoretical advancement, policy and practice' as Helfgott (2013, p.21) reminded us. In particular, the narratives of officers have provided insights which may help various local and international agencies [a] to understand the actions/features of these two groups of cybercriminals better and develop more effective response strategies; and [b] to appreciate the vulnerabilities of their victims better and develop more adequate support schemes. Indeed, insights from our study could help various local and international agencies, as well as social scientists around the world, to understand the actions/features of these two groups of cybercriminals better (as illustrated in Figure 1). One might also be inclined to suggest that, for example, these insights may help relevant agencies in understanding the best strategy to reduce the occurrences of these crimes. By benefitting from the basic premises of the interactionist position, this study has proposed that, since indigenous worldview and masculinity emerge out of repeated, patterned interaction and socialization processes, "Yahoo-Yahoo" may be one of the ways these Yahoo-boys construct their culturally expected identity regarding wealth acquisition in society. Because of this, we believe insights from this research have implications for the value of the interactionist perspective in making sense of crimes on the Internet. Unlike the existing studies on Yahoo-boys, our study has found evidence to deconstruct the homogenization of these cyber- fraudsters as one group (e.g. with respects to "educational attainment" and "networks/collaborations"). Specifically, it has instead pro- posed rather dualistic groups based on three factors

(educational attainment, modus operandi, networks and collaborators) that shed fresh light on a range of prevailing perspectives on Yahoo-boys.

First, there is consensus that young male university students/graduates are predominantly the perpetrators of cyber-fraud (Adeniran, 2011; Ibrahim, 2017); the current study, however, demonstrates that a considerable number of non-university students are also involved in perpetrating cyber-fraud. Second, prior qualitative studies identified that some Yahoo-boys use magical/spiritual powers to defraud victims (Melvin and Ayotunde, 2010; Tade, 2013). Like these previous studies, the current study indicates that a group of these cybercriminals (Yahoo-boys-analogue) depends more on spiritual powers for their "Yahoo-Yahoo" business than others (Yahoo-boys-digital). Unlike the prevailing studies, the current study also indicates Yahoo- boys can be divided with respect to other attributes: "university education;" "networks and collaborators;" and "method of opera- tion." Third, while our study concurs with previous qualitative studies that suggests Yahoo-boys live extravagant lifestyles (Lazarus, 208; Ojedokun and Eraye, 2012), the current study has additional contributions. First, it explains that, although most Yahoo-boys live a lavish lifestyle, a group of them (Yahoo-boys-digital) invest their illicit income predominantly in legitimate businesses, such as the music industry. Second, it notes that a conspicuous lifestyle for male Nigerians in itself is a mere reflection of gender nuances in society.

While our study provides valuable contributions to the existing body of knowledge, it should be viewed in light of a few fundamental limitations. Its primary weakness is that it offers only a top-down view of a selected group on Yahoo-boys. The

perspectives of some frontline enforcers of the law on criminals, as Reiner (2016) noted, are commonly susceptible to prejudice, given that the human narratives about their fellow men/women are culturally defined. "People's experience of the world is always mediated by culturally defined meanings, which, although adopted by their personal experience, condition how and what they conceive as reality" (Longo, 2015, p. 34) as previously mentioned. Equally, we acknowledge the potential dangers of using interviews with social-control agents to discuss offenders because some of them may not (and often do not) have the full picture of the criminals. Additionally, caution should be applied in the interpretation of the officers' narratives concerning Yahoo-Boys and their activities. This is because, we cannot escape the conclusion that all interviews, and interview data, as Morris (2018) and Ribbens (1989) observed, are socially constructed and are products of social encounters within a particular social structure.

The above limitations by no means undermine the importance of this study's main achievement: the bifurcation of Yahoo-boys. Our analyses have helped to propose that these cybercriminals can be grouped into two main categories, based on the multiple axes of differentiation discussed. In Nigeria, "cybercrime" may be fundamentally rooted in socioeconomics (Ibrahim, 2016; Ojedokun and Eraye, 2012) and indigenous worldviews within the occult economy (Lazarus, 2019a; Tade, 2013). Indeed, online behaviors are mere reflections of the symbolic meaning and consequences of social products (e.g. the occult economy and the prestige of material wealth) and social actors such as the Yahoo-boys, corrupt bankers, and spiritualists. By implication, the different "business associates," as well as preferred methods of operations of Yahoo-boys-digital and Yahoo-boys-analogue, reinforce the idea that

life online is an extension of life offline, reflecting contextual and cultural nuances (Lazarus, 2019b; Mumporeze and Prieler, 2017).

This article has therefore proposed that, since the occult economy and masculinity develop out of repeated, patterned interaction and socialization processes, cyber-fraud may be one of the ways Yahoo-boys and their associates construct culturally expected identities in society. This, in particular, may be responsible for rendering fraudulent practices acceptable career paths for Yahoo-boys and some representatives of legitimate institutions. Since Yahoo-boys defraud a multitude of victims globally, as Cross (2018) and Lazarus (2018, 2019a) suggested, a better understanding of this phenomenon lies in our capacity to unconditionally value all insights across the global South and global North.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics*, *40*, 14-26.

Author contribution statements

[a] S.L. conceived & designed the study. [b] G.U.O. recruited & interviewed the participants. [c] S.L. analyzed & interpreted the data. [d] G.U.O. verified the interpretation of data. [e] S.L. drafted the whole article. [f] S.L. carried out the critical revisions of the article. [g] S.L. & G.U.O. read & approved the published version.

Acknowledgements

The authors thank all the participants who gave their time and shared their stories. The authors are fully responsible for the views expressed in this article: the article does not represent the views of the authors' institutional affiliations.

Authors-Information

Dr Suleman Lazarus is a qualitative sociologist and his research interests include the cultural dimensions of digital crimes. While he completed an empirical study on the connections between hip hop artists and cybercriminals in 2018, one of his theoretical works in 2019 nuances "the synergy between feminist criminology and the Tripartite Cybercrime Framework." He is also a published poet and his most recent poem is entitled, "Betrayals in Academia and a Black Demon from Ephesus." **Email**: Suleman.lazarus@gmail.com

Geoffrey U. Okolorie is a digital forensics expert, a fraud examiner and cybercrime investigator who is currently a postgraduate research student in the UK. He is a member of the Economic and Financial Crimes Commission (EFCC), Nigeria, as well as a member of various local and international professional organizations. **Email**: gokolorie@efccnigeria.org

References

Adeniran, A.I., 2011. Café culture and heresy of Yahooboyism in Nigeria. In: Jaishankar, K. (Ed.), Cyber criminology: Exploring internet crimes & criminal behaviour. CRC Press, New York.

Adesina, O.S., 2017. Cybercrime and poverty in Nigeria. Can. Social Sci. 13 (4), 19–29.

Adogame, A., 2009. The 419 code as business unusual: Youth and the unfolding of the advance fee fraud online discourse. Asian J. Social Sci. 37 (4), 551–573.

African Development Bank, 2018. 'African Development Bank reported in 2018 that about 78% Nigerians live on less than $2 daily', retrieved: https://www.concisenews.global/business/150m-nigerians-lve-on-less-than-2-daily-afdb/, accessed, 28/02/18.

Akanle, O., Adejare, G.S., 2018. Contextualizing pentecostal gatherings in southwestern Nigeria: Social drivers and significance. In: Religion in Context. Nomos Verlagsgesellschaft, Baden-Baden, pp. 145–158.

Akanle, O., Adesina, J.O., Akarah, E.P., 2016. Towards human dignity and the internet: the cybercrime (yahoo yahoo) phenomenon in Nigeria. Afr. J. Sci. Technol. Innov. Development 8 (2), 213–220.

Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol. Behav. Social Networking 14 (12), 759–763.

Bae, S.M., 2017. The influence of strain factors, social control factors, self-control and computer use on adolescent cyber delinquency: Korean National Panel Study. Children Youth Services Rev. 78, 74–80.

Becker, H., [1967]1997. Outsiders: Studies in Sociology of Deviance. New York, NY: Simon and Schuster.

Beirne, P., 1983. Cultural relativism and comparative criminology. Contemporary Crises 7 (4), 371–391.

Blumer, H., 1969a. Symbolic Interactionism: Perspective and Method. Prentice Hall, Eaglewood Cliffs.

Blumer, H., 1969b/1998. Symbolic Interactionism: Perspective and Method. Berkeley: University of California Press.

Broadhurst, R., 2006. Developments in the global law enforcement of cyber-crime. Policing 29 (3), 408–433.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

Button, M., Cross, C., 2017. Cyber Frauds, Scams and Their Victims. Taylor & Francis, New York.

Cain, M., 2000. Orientalism, occidentalism and the sociology of crime. Br. J. Criminol. 40 (2), 239–260.

Carter, M.J., Fuller, C., 2015. Symbolic interactionism. Sociopedia. ISA 1, 1–17.

Carter, M.J., Fuller, C., 2016. Symbols, meaning, and action: the past, present, and future of symbolic interactionism. Curr. Sociol. 64 (6), 931–961.

Chang, J.J., 2008. An analysis of advance fee fraud on the internet. J. Financial Crime 15 (1), 71–81.

Chinwuba, N.N., 2015. Human identity: child rights and the legal framework for marriage in Nigeria. Marriage Family Rev. 51 (4), 305–336.

Comaroff, J., Comaroff, J.L., 1999. Occult economies and the violence of abstraction: Notes from the South African postcolony. Am. Ethnol. 26, 279–303.

Connell, R.W., Messerschmidt, J.W., 2005. Hegemonic masculinity: rethinking the concept. Gender Soc. 19 (6), 829–859.

Cooley, C., [1909] 1998. On Self and Social Organisation. Chicago: The University of Chicago Press.

Cross, C., Dragiewicz, M., Richards, K., 2018. Understanding romance fraud: insights from domestic violence research. Br. J. Criminol. 58 (6), 1303–1322.

Cross, C., 2018. Marginalized voices: The absence of Nigerian scholars in global examinations of online fraud. In: The Palgrave Handbook of Criminology and the Global South. Palgrave Macmillan, Cham, pp. 261–280.

Cybercrime Act, 2015. 'Cybercrime, Prohibition, Prevention Act', retrieved: https://cert.gov.ng/images/uploads/CyberCrime_(Prohibition,Prevention,etc)_Act,_2015.pdf, ac- cessed 14/03/18.

Dasgupta, N., Ugur, M., 2011. Evidence on the economic growth impacts of corruption in low-income countries and beyond: a systematic review. London: EPPI-Centre, Social Science Research Unit, Institute of Education, University of London.

Donner, C.M., Jennings, W.G., Banfield, J., 2015. The general nature of online and off-line offending among college students. Social Sci. Computer Rev. 33 (6), 663–679.

Droz, Y., Gez, Y.N., 2015. A God trap: seed plan ng, gi logic, and the prosperity gospel. In: Heuser, A. (Ed.), Pastures of Plenty: Tracing Religio-scapes of Prosperity Gospel in Africa and Beyond. Lang, Frankfurt, pp. 295–307.

Eboiyehi, F.A., Muoghalu, C.O., Bankole, A.O., 2016. In their husbands' shoes: feminism and political economy of women breadwinners in Ile-Ife, Southwestern Nigeria. J. Int. Women's Stud. 17 (4), 102–121.

EFCC, 2018. 'The United Nations Office on Drug and Crime Survey', retrieved: https://efccnigeria.org/efcc/9-uncategorised/2714-efcc-adjudged-mst-effective-govt-agency, 13/ 03/18.

Ekeh, P.P., 1975. Colonialism and the two publics in Africa: a theoretical statement. Comparative Stud. Soc. History 17 (1), 91–112. Ellis, S., 2016. This Present Darkness: A History of Nigerian Organized Crime. OXford University Press, OXford.

Frankle, R.L.S., Stein, P.L., 2005. The anthropology of religion, magic and witchcraft. Pearson Allyn and Bacon, Boston.

Hayward, K.J., Young, J., 2004. Cultural criminology: Some notes on the script. Theor. Criminol. 8 (3), 259–273.

Helfgott, J.B., 2013. Criminal psychology and criminal behavior. In: Helfgott, J.B. (Ed.), Criminal Psychology. Praeger, Santa Barbara, pp. 3–42.

Hjalmarsson, R., Holmlund, H., Lindquist, M.J., 2015. The effect of education on criminal convictions and incarceration: causal evidence from micro-data. Econ. J. 125 (587), 1290–1326.

Howard, R., 2009. Cyber Fraud: Tactics, Techniques and Procedures. Auebach Publications, Boca Raton, FL.

Hruschka, D.J., Schwartz, D., St. John, D.C., Picone-Decaro, E., Jenkins, R.A., Carey, J.W., 2004. Reliability in coding open-ended data: Lessons learned from HIV behavioral research. Field methods 16 (3), 307–331.

Hsieh, H.F., Shannon, S.E., 2005. Three approaches to qualitative content analysis. Qual. Health Res. 15 (9), 1277–1288.

Hutchings, A., Chua, Y., 2017. Gendering cybercrime. In: Holt, T.J. (Ed.), Cybercrime through an Interdisciplinary Lens. Routledge, New York, pp. 167–188.

Ibrahim, S., 2015. A binary model of broken home: Parental death-divorce hypothesis of male juvenile delinquency in Nigeria and Ghana. In: Royo Maxwell, S., Lee Blair, S. (Eds.), Contemporary Perspectives in Family Research. vol. 9. Emerald Group Publishing Limited, New York, pp. 311–340.

Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. Int. J. Law Crime Justice 47, 44–57.

Ibrahim, S., 2017. Causes of socioeconomic cybercrime in Nigeria. In: IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada, pp. 1–9.

Igwe, C.N., 2007. Taking Back Nigeria from 419: What to Do about the Worldwide E-mail Scam – Advance-fee Fraud. iUniverse, Toronto.

Jegede, A.E., Elegbeleye, A.O., Olowookere, E.I., Olorunyomi, B.R., 2016. Gendered alternative to cyber fraud participation: an assessment of technological driven crime in Lagos State, Nigeria. Gender Behav. 14 (3), 7672–7692.

Jones, M.L., 2018. Ctrl+ Z: The Right to be Forgotten. NYU Press, New York.

Kalu, O.U., 2002. The religious dimension of the legitimacy crisis, 1993–1998. In: Falola, Toyin (Ed.), Nigeria in the Twentieth Century. Carolina Academics Press, Durham, Durham, NC, pp. 667–685.

Kigerl, A., 2012. Routine activity theory and the determinants of high cybercrime countries. Social Sci. Comput. Rev. 30 (4), 470–486.

Kirillova, E.A., Kurbanov, R.A., Svechnikova, N.V., Zul'fugarzade, T.E.D., Zenin, S.S., 2017. Problems of fighting crimes on the internet. J. Adv. Res. Law Econ. 8 (3), 849–856. Lazarus, S., 2018. Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo boys) and hip hop artists. Criminol. Criminal Justice Law Soc. 19 (2), 63–80.

Lazarus, I., Rush, M., Dibiana, E.T., Monks, C.P., 2017. Gendered penalties of divorce on remarriage in Nigeria: a qualitative study. J. Comparative Family Stud. 48 (3), 351–366.

Lazarus, S., 2019a. Where is the money? The intersectionality of the spirit world and the acquisition of wealth. Religions 10 (3), 146 1–20.

Lazarus, S., 2019b. Just married: The synergy between feminist criminology and the tripartite cybercrime framework. Int. Soc. Sci. J. 1–19.

Lochner, L., 2004. Education, work and crime: a human capital approach. Int. Econ. Rev. 45, 811–843.

Longo, M., 2015. Fiction and Social Reality: Literature and Narrative as Sociological Resources. Ashgate Publishing Limited, Surrey.

Machin, S., Marie, O., Vujić, S., 2011. The crime reducing effect of education. Econ. J. 121 (552), 463–484.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

Malinowski, B., [1954]2014. Magic, Science and Religion and Other Essays. New York: Read Books Ltd.

Mauss, M., 1925. The Gift. Routledge, London.

Melvin, A.O., Ayotunde, T., 2010. Spirituality in cybercrime (Yahoo Yahoo) activities among youths in South West Nigeria. In: Youth Culture and Net Culture: Online Social Practices. IGI Global, pp. 357–376.

Messerschmidt, J., 1993. Masculinities and Crime: Critique and Reconceptualization of Theory. Rowman and Littlefield, Lantham.

Morris, C., 2018. 'You can't stand on a corner and talk about it…': medicinal cannabis use, impression management and the analytical status of interviews. Methodol. Innov. 11 (1), 1–12.

Mumporeze, N., Prieler, M., 2017. Gender digital divide in Rwanda: a qualitative analysis of socioeconomic factors. Telematics Inform. 34 (7), 1285–1293.

The Nation, 2017. 'EFCC secure 340 convictions in siX months', available at: http://thenationonlineng.net/efcc-secures-340-convictions-si-months/, accessed, 20/12/17.

Newburn, T., 2016. Social disadvantage: crime and punishment. In: Dean, H., Platt, L. (Eds.), Social Advantage and Disadvantage. Oxford University Press, Oxford.

Newburn, Tim, Sparks, Richard, 2004. Policy transfer and lessons drawn. In: Newburn, Tim, Sparks, Richard (Eds.), Criminal Justice and Political Cultures: National and International Dimensions of Crime Control. Routledge, London.

Obuah, E., 2010. Combatting corruption in Nigeria: the Nigerian economic and financial crimes (EFCC). African Stud. Q. 12 (1), 17.

Ojedokun, U.A., Eraye, M.C., 2012. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol. 6 (2), 1001–1013.

Owen, T., Noble, W., Speed, F.C., 2017. The challenges posed by scammers to online support groups: the 'deserving' and the 'undeserving' victims of scams. In: New Perspectives on Cybercrime. Palgrave Macmillan, London, pp. 213–240.

Payne, B., 2018. White-collar cybercrime: white-collar crime, cybercrime, or both? Criminol. Criminal Justice Law Soc. 19 (3), 16–32.

Peavy, D., 2016. The Benin Monarchy, Olokun and Iha Ominigbọn. J. Benin Edo Stud. 1 (1), 95–127.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

Pierce, Steven, 2016. Moral Economies of Corruption. Duke University Press, Durham, NC, pp. 328.

Polkinghorne, D., 1988. Narrative Knowing and the Human Sciences. State University of New York Press, Albany.

Powell, A., Stratton, G., Cameron, R., 2018. Digital Criminology: Crime and Justice in Digitalsociety. Routledge, New York.

Reiner, R., 2010. The Politics of the Police. OXford University Press, OXford.

Reiner, R., 2016. Crime, the Mystery of the Common-Sense Concept. John Wiley & Sons, New York.

Ribbens, J., 1989. Interviewing—an "unnatural situation"? Women's Stud. Int. Forum. 12 (6), 579–592.

Ribbens McCarthy, J., Gillies, V., 2018. Troubling children's families: who is troubled and why? Approaches to inter-cultural dialogue. Sociol. Res. Online 23 (1), 219–244.

Rich, T., 2017. You can trust me: a multimethod analysis of the Nigerian email scam. Security J. 1–18.

Schoepfer, A., Baglivio, M., Schwartz, J., 2017. Juvenile hybrid white-collar delinquency: an empirical examination of various frauds. Criminol. Criminal Justice Law Soc. 18 (1), 18–21.

Selwyn, N., 2008. A safe haven for misbehaving? An investigation of online misbehavior among university students. Social Sci. Comput. Rev. 26 (4), 446–465.

Smith, D.J., 2008. A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria. Princeton University Press.

Smith, D.J., 2017. To be a Man is Not a One-day Job: Masculinity, Money, and Intimacy in Nigeria. University of Chicago Press, Chicago.

Sorell, T., Whitty, M., 2019. Online romance scams and victimhood. Secur. J. 1–20.

Swidler, A., 1990. Culture in action: symbols and strategies. Am. Sociol. Rev. 51 (2), 273–286.

Tade, O., 2013. A spiritual dimension to cybercrime in Nigeria: the 'yahoo plus' phenomenon. Human Affairs 23 (4), 689–705.

Tade, O., Aliyu, I., 2011. Social organization of internet fraud among university undergraduates in Nigeria. Int. J. Cyber Criminol. 5 (2), 860–875.

Trend Micro and INTERPOL, 2017. 'Cybercrime in West Africa: Poised for an Underground Market'.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.

Umar, I., Samsudin, R.S., Mohamed, M., 2016. Understanding the successes and challenges of anti-corruption agency (ACA) in Nigeria: a case of economic and financial crimes commission (EFCC). Asian J. Multidisciplinary Stud. 4 (5).

UNODC, 2017. 'Supporting the EFCC and Nigerian Judiciary', retrieved: https://www.unodc.org/nigeria/en/s08anticorruption.html, accessed 3/3/18.

Wall, D.S., 2007. Policing cybercrimes: situating the public police in networks of security within cyberspace. Police Practice Res. 8 (2), 183–205.

West, C., Zimmerman, D.H., 1987. Doing gender. In: Fenstermaker, S., West, C. (Eds.), Doing Gender, Doing Difference. Routledge, New York, pp. 3–24.

Whitaker, R., 2013. Proto-spam: Spanish prisoners and confidence games. Retrieved from. The AppendiX 1 (4). http://theappendiX.net/issues/2013/10/protospam-spanish- prisoners-and-confidence-games.

Yar, M., 2017. Online crime. In: Pontell, Henry (Ed.), OXford research Encyclopedia of Criminology: Criminology & Criminal Justice. OXford University Press, OXford.

Cite as

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. *Telematics and Informatics, 40,* 14-26.