



Research article

Advantageous comparison: using Twitter responses to understand similarities between cybercriminals (“Yahoo Boys”) and politicians (“Yahoo men”)



Suleman Lazarus^{a,*}, Mark Button^b, Afe Adogame^c

^a Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), Houghton Street, London, WC2A 2AE, United Kingdom

^b Centre for Counter Fraud Studies at the Institute of Criminal Justice Studies, University of Portsmouth, PO1 2HY, Portsmouth, United Kingdom

^c Princeton Theological Seminary, Princeton University, P.O. Box 821, 64 Mercer Street, Princeton, NJ 08542-0803, United States

ARTICLE INFO

Keywords:

Online fraud
Public opinion
Corruption
Cybercrime
Moral disengagement mechanism
Rationalization
West Africa
Tweets
Nigeria
Romance scam
Business email compromise
419 fraud
Sociology of deviance
Cyber criminology

ABSTRACT

This article is about the manifestations of similarities between two seemingly distinct groups of Nigerians: cybercriminals and politicians. Which linguistic strategies do Twitter users use to express their opinions on cybercriminals and politicians? The study undertakes a qualitative analysis of ‘engaged’ tweets of an elite law enforcement agency in West Africa. We analyzed and coded over 100,000 ‘engaged’ tweets based on a component of mechanisms of moral disengagement (i.e., advantageous comparison), a linguistic device. The results reveal how respondents defend the actions of online fraudsters (“the deviant group”) by strategically comparing them to the wrongful acts of corrupt politicians (“the respectable group”). Similarly, the results show how respondents positioned this linguistic strategy to compare “the powerless group” (online fraudsters) and “the powerful group” (politicians) in society. Indeed, tweet responses suggest that the Economic and Financial Crimes Commission (EFCC) generally looks downwards for culprits (i.e., online fraudsters) while ignoring fraudulent politicians. We conclude that the process by which some actions are interpreted as a crime compared to others is a moral enterprise.

1. Introduction

Public opinion on Twitter offers opportunities to explore contestations between diverse standpoints (Karamouzas et al., 2022; Tournay et al., 2020). This article examines how Twitter users employ moral disengagement as a strategy to rationalize the activities of online criminals. Contextually, Nigerian cyber-fraudsters in Ibadan, Canadian cyberbullies in Toronto, Russian ransomware criminals in Moscow, Chinese political hackers in Harbin, and Jamaican lottery scammers in Montego Bay often have materially identical computers. However, computers hold different meanings and generate various social issues influenced by the socio-cultural, economic, and political contexts in which the computers and their users are located (Hall et al., 2020; Lazarus & Okolorie, 2019; Lewis, 2020). So, Nigerian society is a resource for understanding social forces in the virtual world concerning its citizens (Lazarus and Okolorie, 2019). The article undertakes a qualitative analysis of tweets of the Economic and Financial Crimes

Commission (EFCC), an elite law enforcement agency, to understand public attitudes, sentiments, and expressions concerning the prosecutions of Nigerian cybercriminals. Studies about multiple social contexts such as Colombia (Correa and Camargo, 2017), Belgium (Kurten and Beullens, 2021), Japan (Mason, 2019), Finland (Koiranen et al., 2019), India (Ahmed et al., 2018), the United States (Lim and Lee-Won, 2017), Spain (Santoveña-Casal et al., 2021), Thailand (Leelawat et al., 2021), and the United Kingdom (Asher et al., 2019) have shown how Twitter served as a lens through which the seemingly disorganized social issues are organized as connected parts of a whole.

However, the authority has always suppressed and controlled negative expressions of Nigerians about government representatives (Adibe et al., 2017; Ellis, 2016). The tendency of the Nigerian government to suppress public opinion is exemplified in Mrs. Aisha Buhari’s public speech (i.e., the current first lady of Nigeria): “If China can control over 1.3 billion people on social media, I see no reason why Nigeria cannot attempt controlling only 180 million people” (The Cable, 2019, p. 1).

* Corresponding author.

E-mail addresses: suleman.lazarus@gmail.com, S.Lazarus@lse.ac.uk (S. Lazarus), mark.button@port.ac.uk (M. Button), afe.adogame@ptsem.edu (A. Adogame).

Some studies investigated perceptions of corruption and cybercrime in a Nigerian context (e.g., Daxecker et al., 2019; Lazarus and Button, 2022; Ojeka et al., 2019; Zakari and Button, 2021). None of them used Twitter as a data source except Lazarus and Button's (2022) study, which used post-colonial perspectives to examine the North-South divide in Nigerian society and the legacies of colonialism. Therefore, it is vital to conduct this study because of the following additional rationales.

Nigerian online criminals have had many victims worldwide since the early 2000s (Lazarus and Okolorie, 2019). From 2006 to 2010, the United States, the United Kingdom, and Nigeria, in descending order of significance, were on top of the global league table regarding the prevalence of cybercrime perpetrators (Ibrahim, 2016). Historically, nonetheless, such league tables constructed by the Federal Bureau of Investigation – FBI, ceased to exist from 2011 to date) (see Ibrahim, 2016, pp. 44–54 for more detailed discussions). Therefore, public opinion about Nigeria would generate fresh insights invaluable to many regional and international stakeholders (e.g., law enforcement agencies, policymakers and researchers). Such an achievement would help to underscore that the social and cultural realities on the internet (e.g., Twitter) should be the basis of policymaking in a society that has a politically embedded economy and criminal justice, such as Nigeria. A primary objective of this article is to shed light on how Twitter users rationalize and interpret the policing and incarcerations of cyber fraudsters.

Since the Nigerian cybercriminals are primarily implicated in economic crimes on the internet (Ibrahim, 2016) and the Economic and Financial Crimes Commission (EFCC), as its name implies, is the prime enforcer of economic crimes (Lazarus and Okolorie, 2019), it is logical to infer that the destiny of these criminals and that of the EFCC are reciprocally constructing one another. Crimes on the internet are social products (McGuire, 2017; Hall et al., 2020; Ibrahim, 2016; Timofeyev and Dremova, 2022). Hence, it is logical to suggest that Twitter users' expressions, sentiments, and worldviews reflect their lives in society. Yet, no study has thus far harnessed Twitter comments about the arrests, and convictions of cyber fraudsters by the EFCC, even though this topic merits examination. To explore how Twitter users interpret and rationalize the EFCC's actions against cyber fraudsters, this study asks:

1. How do Twitter users interpret and rationalize the EFCC's actions against cybercriminals?
2. Which techniques and linguistic strategies do Twitter users deploy to describe and express their opinions regarding the EFCC tweets?
3. What might the techniques say about cybercrime in a Nigerian context?

2. Literature review

2.1. Socioeconomic cues

Nigeria has always lacked social welfare, and most youths have no opportunities in the legitimate economy – they live in abject poverty (Adeduntan, 2022; Ibrahim, 2016; Lazarus and Okolorie, 2019). In part, Nigerian youths have been disproportionately implicated in internet crimes (Adogame, 2009; Ibrahim, 2016; Hall et al., 2020). Likewise, in a digital age, local criminals' actions have international connections and consequences, as many authors have suggested (Hall et al., 2020; Hall and Hudson, 2022; Jaishankar, 2018; Leukfeldt et al., 2020; Lewis, 2020; Ndubueze, 2020; Šupa, 2021; Rich, 2017; Wall, 2013; Zakari and Button, 2021). Similarly, a study interviewed 40 EFCC officers (Lazarus and Okolorie, 2019), and another interviewed 40 cybercriminals (Aransiola and Asindemade, 2011). Both studies agree that the actions of cybercriminals have global consequences, not the least because these criminals defraud victims worldwide. While many online users often fail to apply appropriate measures to reduce their risk of victimization, they rarely receive adequate safety advice from stakeholders (Whittaker et al., 2022). Consequently, recent years have seen a significant upsurge studies

on victims of online fraud within Nigeria (Idom and Tormusa, 2016; Mba et al., 2017; Ndubueze, 2020) and outside Nigeria (e.g., Leukfeldt et al., 2020), all originating from Nigerian cybercriminals.

2.2. Cybercrime and cybercriminals

First, online fraud is an aspect of cybercrime (Akanle et al., 2016; Lazarus & Button, 2022). Second, cyberbullying is another part of cybercrime (Khlokov et al., 2019; Zsila et al., 2019). Third, cyber espionage is yet another element of cybercrime (Gilli and Gilli, 2018; Rivera et al., 2022). Along these lines, the word cybercrime has three motivational parts that are broadly based on a strand of socio-economic reasons (e.g., online fraud, psychological motives (e.g., cyber bullying), or geopolitical explanations (e.g., cyber espionage), according to the Tripartite Cybercrime Framework (Ibrahim, 2016; Lazarus et al., 2022). Thus, contextual cues and terminologies matter when considering these cybercrime types. Cybercrime that emanates from Nigerian cybercriminals is primarily propelled by socio-economic reasons and determined by them (Lazarus, 2020)¹. It is generally referred to as “Nigerian 419 fraud” in many discourses (Adogame, 2009; Chawki et al., 2015; Ibrahim, 2016; Mba et al., 2017). The term “419” is contextually and socially derived from the Nigerian Criminal Code, section 419, which deals with many fraudulent offenses. 419 fraud is a confidence trick in which con artists deceive victims into advancing considerable sums of money, sometimes in ascending order of value, hoping to obtain a much more significant gain (Adogame, 2009; Chawki et al., 2015; Lazarus, 2019a; Mba et al., 2017). The digital form of the Nigerian 419 fraud is “Yahoo Yahoo” (Egielewa, 2022; Ojedokun and Eraye, 2012).

In the late 2000s, under the canopy of “Yahoo Yahoo”, cybercriminals generally victimize individuals by developing fake love affairs for material gains on social media in general and dating websites or apps in particular (i.e., romance scams) (Hai-Jew, 2020; Wang and Zhou, 2022). On the flip side, cybercriminals commonly deploy Business Emails Compromise (BEC) to take over or duplicate the business emails of organizations and businesses to trick unsuspecting representatives of the companies into transferring large amounts of funds or sensitive information to criminals (Meyers, 2018; Okpa et al., 2022). In the mid-2000s, the term “Yahoo Yahoo” was contextually derived from the predominant use of Yahoo email applications and instant messaging in offender-victim communications (Lazarus and Okolorie, 2019). The perpetrators of “Yahoo Yahoo” are consequently called “Yahoo Boys” (Ojedokun and Eraye, 2012; Melvin and Ayotunde, 2010). Equally, the term Yahoo Boys signifies that cybercriminals are predominantly men and boys (Lazarus, 2018). This suggests that gender forces and socialization in society have a differential impact on the actions of men and women online (Lazarus, 2019b; Alzubaidi, 2021; Holt, Navarro & Clevenger, 2020; Ricciardelli & Adorjan, 2019; Zsila et al., 2019).

Of course, the socialization of boys/men as masculine individuals in society makes “Yahoo Yahoo” predominantly boys/men's work (Lazarus & Okolorie, 2019; see also Newburn, 2011; Newburn and Stanko, 2013 on youth crimes in general). Concerning “Yahoo Yahoo” activities, some researchers (Aransiola and Asindemade, 2011; Melvin and Ayotunde, 2010; Ojedokun and Eraye, 2012; Tade and Aliyu, 2011; Ogunleye et al., 2019) provided qualitative evidence for the prominence of men and boys as Yahoo Boys (i.e., online fraudsters). The above interview studies

¹ Not every form of cybercrime is rooted in socioeconomic reasons and determined by them (Ibrahim, 2016; Lazarus, 2019b; Lazarus, 2020; Lazarus, Button & Kapend, 2022). Accordingly, a typology suited to investigating “cybercrime” in a Nigerian context is the “Tripartite Cybercrime Framework”, which Ibrahim (2016) developed to achieve the following objectives: (1) illuminate that the cybercrime category to which Nigeria is most vulnerable is socioeconomic cybercrime (financial crimes); (2) underline that the conceptual “pipelines” of the cybercrime framework in the Global North cannot hold water in Nigeria; and (3) illustrate that the mainstream perspectives that describe Nigeria as a global cybercrime player are misplaced.

converge that: (a) university students and graduates who are men are predominantly implicated in cybercrime offenses.² (b) Cybercriminals are primarily motivated by financial gains. (c) Corrupt practices of some civil servants, e.g., politicians, enable the activities of cybercriminals. Also, Ogunleye et al.'s (2019) research, which solely interviewed 17 female undergraduates, is revealing. All interviewees primarily play subordinate roles for monetary gains in cybercrime perpetration (Ogunleye et al., 2019). To illustrate, all 17 women have men as mentors (e.g., brothers, boyfriends) playing superordinate and supervisory roles in their cybercrime career paths.

However, it is noteworthy that the empirical foundations of all the above studies are university students as participants (i.e., Aransiola and Asindemade, 2011; Ogunleye et al., 2019; Ojedokun and Eraye, 2012; Tade and Aliyu, 2011), and a similar set of participants (university students in Nigeria) can lead to uninformed assertions. Remarkably, other qualitative studies that focused on different sources of data, e.g., interviews with spiritualists (Melvin and Ayotunde, 2010), EFCC officers (Lazarus and Okolorie, 2019), parents (Ibrahim, 2017), arrived at similar conclusions. Likewise, researchers who examined music lyrics (Adeduntan, 2022; Lazarus, 2018), fraudulent emails (Adogame, 2009; Rich, 2017), and Twitter data (Lazarus and Button, 2022) concur with the above conclusions. Apart from empirical studies above, literature reviews (e.g., Cross, 2018; Lazarus, 2019a; Okosun and Ilo, 2022) also support the view that: (a) men are predominantly implicated in cybercrime offenses. (b) Cybercriminals are primarily motivated by financial gains. (c) Corrupt practices of some civil servants, such as politicians, enable the activities of cybercriminals. Having discussed Yahoo Boys, we now discuss the Economic and Financial Crimes Commission (EFCC) that prosecutes them.

2.3. Economic and Financial Crimes Commission (EFCC)

In 2002, the Nigerian authority founded the Economic and Financial Crimes Commission (EFCC) to deal with many economic crimes, such as crimes on the internet, to repair Nigeria's image (Lazarus & Okolorie, 2019; Pierce, 2016). Yahoo Boys are not the only group accountable for sullyng the country's image. Many public officials are also responsible for the stained image of Nigeria globally (Ibrahim, 2016; Hall et al., 2020), and the EFCC's primary aim is to address fraudulent and corrupt practices (Lazarus and Okolorie, 2019). However, the EFCC, like any other organization, is not perfect. To illustrate, some prominent politicians have used the EFCC as an instrument to intimidate their political opponents (Pierce, 2016). Similarly, some EFCC officers have collected bribes from high-profile Yahoo Boys (Aransiola and Asindemade, 2011). Furthermore, the previous chairman of the EFCC, from 2015 to 2020, Mr. Ibrahim Magu, was involved in bribery and corruption (BBC, 2020). As a result of fraudulent and corrupt practices like the offenses of Yahoo Boys, this representative of authority, the previous chairman of the EFCC, was suspended in July 2020 (BBC, 2020).

Such comparisons between online fraudsters (Yahoo Boys) and politicians have at least two consequences (explicit and implicit). Firstly, it tends to explicitly render the condemnable actions of Yahoo Boys benevolent (advantageous comparison). Thus, Advantageous comparison covers injuries from condemnable actions and consequences (Bandura, 1999). Hence, closer attention to society deepens our understanding of cybercriminals' activities and that of the EFCC agency that polices them. Such more immediate attention to society would help highlight cybercriminals' similarities to claimed law-abiding citizens rather than their differences, deepening our understanding of Twitter users' comments (drawing from Sykes and Matza, 1957). Secondly, it implicitly portrays

² However, the evidence supporting the predominance of university students and graduates in the scam/fraud perpetration oversimplifies a rather complex constituency because many unemployed high school students participate in this online 'scam industry.'

Yahoo Boys as victims of circumstances outside their control since the system is corrupt (i.e., "denial of responsibility", Matza and Sykes, 1961 or "displacement of responsibility", Bandura, 1999).

3. Conceptual background

3.1. Constructionist/interpretivist lens

Specifically, this study is based on the premise that the process by which some actions are interpreted as a crime in comparison to other actions is a "moral enterprise" (Becker, 1967). How Nigerians, at home or abroad, see, compare, or contrast politicians and Yahoo Boys is a "moral enterprise". Early social psychologists believe this idea intersects constructionist and interpretivist positions (Thomas, 1923; Tannenbaum, 1938). The two theoretical parts are closely related, but they are also distinct. The constructionist perspective flows in the vein and arteries of macro levels of societal affairs; hence, it generally refers to the social construction of reality (Becker, 1967; Reiner, 2016). On the contrary, interpretivism works more on micro levels and individual social psychology, seeking meaning in actions (Thomas, 1923). However, the core foundation of constructionist and interpretivist perspectives is premised on accounting for the social origins of knowledge (Tannenbaum, 1938; Thomas, 1923). Indeed, in seeking to advance our understanding of social life, both standpoints agree that "the interpretations of actions and actors are ultimately socially and situationally constructed" (Lazarus, 2020, p. 21; see also Tannenbaum, 1938). Therefore, there is no objective viewpoint for rationalizing immoral actions (Bandura, 1999; Becker, 1967). It is challenging to categorize cybercriminals' actions as a 'sub-culture', i.e., a subset detached and different from the dominant culture's body.

3.2. Advantageous comparison

One linguistic device – "advantageous comparison", offers a unique subjective standpoint for criticizing or complimenting condemnable conduct (Bandura, 1999). Advantageous comparisons with more reprehensible activities render blameworthy behaviors benevolent, i.e., according to Bandura's (1999) theory. The mechanisms of moral disengagement (Bandura, 1999) are based on the premise that people, irrespective of their class, gender, sexuality, and so on, offend only insofar as they find excuses to rationalize their actions and disconnect the feelings of blame from themselves (see also a similar theory, neutralization techniques, developed by Sykes and Matza, 1957). In Table 1, we summarize segments of the moral disengagement mechanisms, as Bandura (1999) discussed.

Remarkably, the "advantageous comparison" or "exonerative comparison" device has a knock-on effect on other mechanisms (e.g., diffusing/displacing responsibilities). The advantageous comparison produces something new. Specifically, it bridges the gap between mechanisms of distorting/disregarding consequences and diffusing/displacing responsibilities and creates an overlap between them (Bandura, 1999). We extend this Bandura's (1999) idea to include people's expressions and sentiments, not necessarily about their own actions but other people's conduct (see also Lazarus, 2018, which examined expressions/sentiments of hip hop musicians concerning cyber fraudsters). Hence, we focus on one of the components of "cognitive restructuring" in Table 1: an advantageous comparison. This psychological mechanism (advantageous comparison) will help to illuminate how Twitter users compare cybercriminals to other citizens in society (e.g., politicians). By comparing condemnable actions to more reprehensible actions, Twitter comments may render cybercriminals' actions far less malevolent. The value of 'advantageous comparison' becomes more apparent when one considers that it obscures the seeming differences between the "respectable group" and the "deviant group" But that is not all. The deployment of advantageous comparison may facilitate new ways of seeing previously invisible relationships between "criminals"

Table 1. Cognitive Restructuration: Advantageous comparison.

Cognitive Mechanism	Moral Disengagement
Cognitive Restructuration	1. Moral Justification 2. Euphemistic Labelling 3. Advantageous Comparison
Minimising Own Agency	1. Displacement of Responsibility 2. Diffusion of Responsibility
Disregarding/Distorting Negative Impact	1. Disregarding Consequences 2. Distorting Consequences
Blaming/Dehumanising Victim	1. Attribution of Blame 2. Dehumanization

Table Modified from Lazarus (2018), p. 68.

(Yahoo Boys) and "non-criminals" (politicians) in Nigerian society. Advantageous comparisons thus provide a lens to analyze, interpret and discuss tweets.

4. Method

4.1. Methodological theory

The constructionist/interpretivist lens discussed above (Section 3.1.) has also shaped the methods deployed in this study. In line with Geertz's (1973) famous work, *The Interpretation of Cultures*, this study acknowledges that 'a man is like an insect suspended and enveloped in spider webs of culture; the analysis of it and its actions, therefore, must go in search of meaning and subjective experience' (Geertz, 1973, p. 3). Accordingly, the study focused on meanings and understandings – "advantageous comparison" (a linguistic device) rather than statistical trends. Twitter users' words are revealing. Tweets reveal Twitter users' worldviews, sentiments, and experiences more than the statistical trends of such data (Lazarus, 2008). Consequently, a qualitative approach is appropriate for this study.

4.2. Data collection

This study is an emic approach to understanding social media responses to the EFCC's tweets about Yahoo Boys' arrests, convictions, sentencing, and dramatization. The official Twitter handle of the EFCC – @officialfec, has about 1 million followers. One of the researchers is one of these followers. From July 2019 to July 2020, the research team read every tweet originating from @officialfec to identify relevant tweets included in the study. Relevant tweets are about cybercriminals, and each of them was accompanied by photo image(s) of the suspected/arrested or jailed criminals. From 31 July 2019 to 31 December 2020, the research team manually bookmarked all EFCC's tweets concerning Yahoo Boys. Examples of such tweets include (a) "Court Jails Fifteen Fraudsters in Enugu" and (b) "EFCC Arrests Eleven Internet Fraudsters in Lagos". We manually retrieved the data³. At the same time, tweets received more than 20 responses, and most received over 50 responses when we retrieved the data. Notably, the EFCC rarely respond to their own tweets or others who comment on their original posts – naturally occurring expressions. It is naturalistic in that it might be more honest than what one might generate in an interview, but also unnatural in that it is forced to be condensed into a certain number of characters. Because the authors

³ One would imagine that doing this task in practice is quite time-consuming. In actuality, it is not as difficult as it seems. A person can manually retrieve +1000 responses in less than a minute. To illustrate, practically, a researcher could harvest over a thousand comments by pressing and holding the first word they want to highlight, dragging their finger across the responses under the umbrella of a tweet they wish to copy, and then tapping "COPY" on Twitter. The researcher would then "PASTE" these responses to Microsoft app they wish for the data.

used Twitter data in the public domain, it became unnecessary to seek ethical approval for this study.

4.3. Data analysis

Data analysis in this article represents a systematic approach, careful consideration, and the role of the researchers as experts in the field. Anyone with the proper skillset and tools can discover the origins of quoted tweets in research reports. So, one must put original tweets into their own words in research reports to shield the discoverability of their origins, as Mason and Singh's (2022) comprehensive study discussed. However, direct quotes from tweets are necessary to address our research questions to discuss the linguistic strategy: an advantageous comparison. Also, fending off the discoverability of tweets' origins by omitting direct quotes would lead to losing layers of tweets' linguistic "authenticity". More importantly, if there were potentially harmful consequences or risks to commentators from the EFCC or Nigerian authority, they would have been repercussions irrespective of our research report since the tweets themselves were directly anchored to the EFCC's Twitter handle.

Thus, taking the above considerations into account, the authors began by removing the commentators' Twitter usernames from the data. The inclusion of such usernames would not improve this publication output. The rest of the data was analyzed following a directed approach to qualitative content analysis (DAQCA), as Hsieh and Shannon (2005) recommended. Thus, we coded the data based on a component of mechanisms of moral disengagement (i.e., advantageous comparison) proposed by Bandura (1999) because the goal of a DAQCA is to validate prior theory or conceptual lens (Hsieh and Shannon, 2005).

- First, in accordance with the DAQCA, coding commenced with reading tweeted comments and highlighting every tweet that, on first impression, seemed to signify, show or suggest features of the "advantageous comparison".
- Second, all highlighted passages were coded using predetermined high-level codes (listed in the left-hand column of Table 2) to identify predominant themes from the data (according to the principles of a DAQCA).
- Third, we extended the classifications/themes into more refined sub-categories (listed in the right-hand column of Table 2).
- Fourth, while new categories were allocated to data segments that could not be grouped in the initial and subsequent coding scheme listed in Table 2, they were omitted because they were considered irrelevant. For instance, one of these minor categories excluded was Twitter users' attempts to advertise their businesses, e.g. (a) "Please support my hustle. While y'all are here, I sell the best designer perfumes that last 48 hours on fabrics. Send a DM, WhatsApp 0809660**** to order. Prices start from N6000"; (b) "I sell good quality handmade Palm slippers at an affordable rate of ₦8000 Kindly send a DM Or WhatsApp Message to 0705433**** Worldwide delivery"; and (c) We sell used Generators, 20–2500 kVA. Call or WhatsApp 0803823****. The unsolicited advertising above also suggests that comments were from Nigerians.
- We acknowledge how authors interpret data distinctively. Indeed, every coder may interpret the data code distinctively (Hsieh and Shannon, 2005). Thus, while author number one coded 100% of the data, authors two and three independently reviewed 30% of the data applying the identical code: "advantageous comparison". The degree of similarities between the three coders was 96%.
- Lastly, we also acknowledge that the codes in Table 2 below are not the only codes derivable from the dataset had we followed alternative approaches to qualitative data analysis. We present the result based on these codes.

5. Results

As per the data analysis, a systematic approach, careful consideration, and the role of the researchers as experts yielded two themes derived

from advantageous comparisons: (1) politicians versus Yahoo Boys and, (2) the powerful versus the powerless. These themes, representing sub-categories listed on the right-hand side of Table 2, are new findings. Notably, relying on these codes is the first study to provide empirical support regarding the uber-criminalization of the powerless and the non-criminalization of the powerful by the EFCC, Nigeria.

5.1. Advantageous comparisons

5.1.1. Fraud: politicians versus Yahoo Boys

The endemic corruption associated with those in positions of power stimulates a significant grievance in Nigerian society as evidenced by tweets, with much-juxtaposing enforcement actions directed at the Yahoo Boys next to the perceived lack of action against the powerful elites who engage in corruption, as the following illustrates:

How is this guy [Yahoo Boy] different from the man [public office holder] that swallowed recovered loot, sold confiscated property to his friends? How is this case different from that man that built his son mansions and bought him cars?

As an organization that wants to be recognized internationally with the likes of FBI, this is the kind of people you arraign on daily basis? Little boys with "Aba nodi ji" clothes and walkabout slides? When the big games (politicians) steals and have polices escort them. Shame.

EFCC ignoring the real political thieves only to be chasing small small boys that couldn't settle them at the point of arrest.

See EFCC happy harassing Nigerian youths, but their oga [their boss] who stole billions of dollars wasn't jailed. I mean Hush Magu or Puppi Ibrahim. Choose one!

I'm sick of you people @officialEFCC you're quick to send internet fraudsters to jail, yet you turn a blind eye to the Nigerian politicians who are wrecking this country, stealing billions of naira every chance they get. You're all very disgusting beings!!!

What about the politicians who loot from the national treasury that made many of those internet fraudsters jobless? Those who loot money for power supply, access to good roads, infrastructure for effective running a business?

You be posting everyday parading internet fraudsters while your leaders are out there looting money, or your own agency doesn't involve apprehending politicians?

Some tweets highlighting the differences between the two groups also focused on the harm caused. Specifically, tweets highlighted that while Yahoo Boys focus on defrauding victims overseas and often small sums of money, the politicians focus on defrauding the treasury of the Federal Republic of Nigeria, where fellow Nigerians are the victims, and the harm is much greater:

The Different between Yahoo boys and Nigeria politicians is... Yahoo boys fraud out side country while Our so called government Fraud us

@officialEFCC, you are busy scratching ground for hungry thieves [Yahoo Boys] and protecting the politicians who are looting our treasury with impunity.

Stop nabbing people that are not stealing Nigeria's money and focus more on people that are not providing jobs for millions of graduates

out there, please let us be sensible and stop being slaves to those [politicians who] no nothing about governing a country

As mentioned above, another narrative in the juxtaposition was the 'looting', 'greed' and 'extravagance of the politicians against the Yahoo Boys, who achieve only 'small pickings' or do it to survive:

Instead of catching politicians who are the general overseer of corruption, you people are catching innocent people that take peanuts to survive. You're all ITT [International Thief Thief]

You guys should go after politicians, the real thieves. Those syphoning public money in billions. You know them, and stop deceiving us with small boys fraudsters.

Until the EFCC begins to arrest and label politicians same way the hunt and label these fraudsters, I do not believe they are fighting corruption...the sons and daughters of Nigerian politicians fly to texas [Texas, USA] blowing thousands of dollars in the club how that shit sounds??

This EFCC people, una no dey shame? How u go see a poor person [Yahoo Boy] like this and arrested him? Even his body will tell u that he's very hungry. U people should start u work from the top politicians.

5.1.2. Criminalisation: the powerful versus the powerless

Tweets that juxtaposed the powerless versus the powerful were partly related to the previous theme (i.e., Section 5.1.1.). In this theme, we focus more on the powerless in society beyond the Yahoo Boys, juxtaposed to those that hold power in society both within and beyond the politic.

Look at Uzor Kalu [a Nigerian politician, and former governor of Abia State] escaping justice because he has money. In the name, of technicality he is free. What does the poor man have? He tries to survive yet being thrown in jail. No technicalities or no money to bribe his way through. But look at thieves like Akpabio moving with escort.

you go for the lesser thieves and couldn't get the bigger thieves. Pls try to balance am.

Our resources that has been embezzled without genuine accountability, you'll not make proper investigation into the matter, una go dey find people without power in d society

Null and void. You keep pulling out the ones with no power while you cover the real fraudsters (the ones in power). Stop going for smaller thieves. Go for the bigger ones. The ones paying you! Until you do that, I have no ounce of respect or love for you

Once na poor man or poor man pikin [Yahoo Boys], the eagle is fast in picking...but if na big man or big man pikin especially politician-s..ha!!! The eagle will have malaria

EFCC, its a big shame to you guys, you love it when you show your prowess with poor people, amateurs, ...that can't really say for themselves [i.e., Yahoo Boys], meanwhile you leave the main culprits in power because they feed you in millions. Damn you guys.

You guys are just bunch of Jokers... You sentence people to jail term of 5 yr and more for internet Fraud and impersonation less than 50 million Yet your Boss Ibrahim Magu (Anini of 2020) ["Anini" was a notorious arm robber who terrorize Nigeria in the 1980s] walks free with all the Billions of Dollars.

Is this Agency meant only for Internet fraudsters? How many public office holders have you jailed?

It is noteworthy that apart from these major themes, there was a minor category of comments, which was supportive of the EFCC's actions, e.g. (a) Keep up the good job; (b) Good one, Well done; and (c)

Table 2. Codes and themes.

Main theme	Sub-themes/codes
Advantageous comparisons	<ul style="list-style-type: none"> • Fraud: Politicians versus Yahoo Boys • Criminalization: the powerful versus the powerless

Good work guys!. Interestingly, while all of the supportive comments are generally the briefest responses among all categories of comments, one of such supportive comments generally inspired a multitude of unsupportive comments such as this one below:

You've a lot to learn ode! [You have a lot to learn, stupid person!]. Let us see politicians arrested too, and we will know EFCC's doing a good job.

6. Discussion

This paper has explored how Twitter users deploy a linguistic strategy as an analytic device to rationalize the actions of cybercriminals. Specifically, the article has outlined how using advantageous comparison as an analytical device aids the understanding of Twitter users' opinions about the actions of the EFCC and cyber fraudsters. The respondents' views on Twitter, coded based on "advantageous comparison", formed the central themes, which are most basic to the discussion that follows: (a) Fraud: politicians versus Yahoo Boys; (b) criminalization: the powerful versus the powerless. The two themes are related because, on the one hand, tweets compared Nigerian politicians to cybercriminals (Yahoo Boys) regarding fraudulent practices. On the other hand, the powerful group of Nigerian citizens, in general, compared to the powerless group regarding the criminalization of offenders by the EFCC.

6.1. Fraud: the politicians versus Yahoo Boys

The Twitter users' expressions and rationalizations about Yahoo Boys normalize and accommodate the conduct of these cyber fraudsters. By applying a neutralization technique – advantageous comparison, rule-breaking received a collective response from Twitter audiences who defended it. Twitter users' application of this linguistic technique to defend cybercriminals' actions is remarkable. Indeed, it is reminiscent of the Durkheimian perspective, which posits that criminal conduct is not defined by the intrinsic quality of the act but by the definition that audiences confer on it (see also [Becker, 1967](#)). The Durkheimian perspective implies that an action is criminal when it offends a strong collective conscience, whereas the predominant concept of crime is legally defined (see also [Reiner, 2016](#)).

The above interpretation also resonates with [Becker's \(1967\)](#) idea that the process by which actions are defined as a crime or otherwise is a "moral enterprise". While "respectable" citizens (politicians) may see themselves as staunchly law-abiding and condemn the fraudulent practices of a deviant group (Yahoo Boys), politicians engage in similar practices that constitute fraud, according to the shared opinions of Twitter users. The use of advantageous comparisons has additional benefits. It exposes the similarities between "Yahoo Boys" (cyber fraudsters, the deviant group) and "Yahoo Men" (i.e., politicians, the "respectable" group) in Nigerian society in a brighter light. This contribution reinforces that the process by which actions are interpreted as a crime or otherwise is a moral enterprise. But that is not all.

The harm resulting from the fraudulent practices of politicians is far from minor. It is no less significant than the harm resulting from the fraudulent practices of Yahoo Boys. While politicians' victims are millions of fellow Nigerians, Yahoo Boys' victims are predominantly foreigners. According to shared opinions of Twitter users, the harm caused by the politicians is much more significant than that of the Yahoo Boys. Yahoo Boys often defraud small sums of money compared to the politicians who embezzle billions of dollars. While the politicians steal billions of public funds, many ordinary Nigerians die daily due to abject poverty and the absence of medical and social welfare, e.g., according to respondents' opinions such as this one below: "Stop nabbing the boys 4 stealing kobo kobo [a monetary unit of Nigeria, equal to one-hundredth of a naira] instead of arresting the politicians who are stealing billions \$\$\$ which's multiplying poverty, hunger & making the masses die prematurely". Based on the above comparison, we argue that the lines

dividing Yahoo Boys' actions and politicians' actions are not clear regarding fraudulent practices. The critical difference between Yahoo Boys (deviants) and politicians ("respectable" citizens) is the appropriateness of time and place for cultural definitions of their actions. The Twitter platform offers a cloak of anonymity to commentators to share their opinions without any negative repercussions from the authority. In contrast, sharing such a sharp comparison between Yahoo Boys and politicians in Nigerian society is most likely to attract negative repercussions from the authority.

Nonetheless, the critical point is that such a comparison has at least three enduring consequences. First, it explicitly renders the condemnable actions of Yahoo Boys benevolent (advantageous comparison), at least in the eyes of many ordinary Nigerians on Twitter. Advantageous comparison, thus, serves to cover up injuries of condemnable actions as well as their consequences (e.g., social harm). Second, it implicitly portrays cybercriminals as victims of circumstances outside their control since the system is corrupt. Third, it spotlights that while corrupt politicians and Yahoo Boys are clearly in different spectrums of economic situations, the motivation for fraudulent practices on the part of politicians was not related to absolute economic deprivation, unlike some cybercriminals (Yahoo Boys).

The authors' identification of similarities between politicians and cybercriminals, in general, is new in cybercrime scholarship. Even though the statistical data concerning the severity of harm and number of victimizations resulting from the fraudulent actions of cybercriminals and of politicians does not exist, we argue that this dimension of the information is critical in understanding Twitter users' opinions. The harmful aspect of criminal conduct may have influenced Twitter users' views in trivializing the actions of cybercriminals. They trivialized Yahoo Boys' reprehensible actions by exploiting a distinct "vocabulary of motive" – i.e., advantageous comparisons with more reprehensible actions in society.

Also, the authors' contributions are the mirror of and made possible by their unique approach to collecting naturalistic online datasets on Twitter. To illustrate, prior interviews with 40 cybercriminals ([Aransiola and Asindemede, 2011](#)), 17 parents ([Ibrahim, 2017](#)), and 40 EFCC officers ([Lazarus and Okolorie, 2019](#)) are ill-equipped to identify the similarities between politicians and Yahoo Boys. Unlike interviews, Twitter data is an invaluable 'qualitative' resource for understanding Nigerians' worldviews and attitudes toward politicians versus Yahoo Boys. The value of Twitter data is worth much more, recognizing that the authority has always suppressed and controlled negative expressions of Nigerians about government representatives. For instance, there is no explicit negotiating with gatekeepers, or leading questions, which are features of interview fieldwork, as [Morse \(2019\)](#) noted. Also, participants often manipulate impressions and expressions during interviews ([Goffman, 1978](#)). These factors (e.g., leading questions, manipulation of impressions and expressions) in themselves shape interview data. On the contrary, this study is an emic approach based on naturalistic Twitter data that is not a well-traveled path to understanding public attitudes, sentiments, and expressions concerning Nigerian cybercriminals (deviant groups) and "respectable" groups in society (e.g., politicians).

Like claimed law-abiding Nigerians (e.g., politicians), cybercriminals, far from deviating, conform to the common method of wealth acquisition (fraudulent actions) by most Nigerian politicians from 1960 to date (see [Ibrahim, 2016; Lazarus, 2019a](#)). So, in "devil advocating" the "righteousness" of this respectable group (politicians), Twitter responses' critical point here is that both groups (cybercriminals and politicians) are similar. Yahoo Boys and politicians have tainted the image of Nigeria ([Ibrahim, 2017](#)), but the EFCC generally looks downwards for culprits (Yahoo Boys), not upwards (politicians), according to Twitter users' responses. Since the EFCC represent the hegemonic political viewpoints and tendencies, it is persuasive to suggest that the powerful Nigerian politicians ("Yahoo Men") may have been applying their power to influence criminal justice to favor them at the expense of Yahoo Boys.

The cultural dimensions of cyber fraud in a Nigerian context become more evident when we cast light on the similarities between cyber fraudsters (Yahoo Boys) and politicians in place of their similarities. So, the deployment of advantageous comparison as an analytic tool is priceless. The advantageous comparison, the linguistic strategy, thus casts a critical gaze on similarities between cyber fraudsters and Nigerian politicians, often ignored or even denied. Therefore, we argue that “[T]he delinquent may not stand as an alien in the body of society but may represent a disturbing reflection or a caricature instead” (Matza and Sykes, 1961, p. 717). The theoretical value of this specific contribution becomes more evident when one contemplates that in the criminology discipline specifically, ‘theoretical originality’ from marginalized voices (e.g., Africans) is emergent because of long-standing historical, political, economic, and colonial reasons.

6.2. Criminalization: the powerful versus the powerless

The authors have more contributions. Explanations of Yahoo Boys generally place massive stress on their deviance and their dissimilarities to society (e.g., Melvin and Ayotunde, 2010). Specifically, these existing explanations interpret Yahoo Boys’ moral beliefs as sub-cultural values (a subset detached and different from the body of the mainstream cultures) (e.g., Aransiola and Asindemade, 2011). In contrast, we disagree with the sub-cultural explanations. To illustrate, our results show that the line dividing Yahoo Boys’ activities and the conduct of claimed law-abiding citizens are blurred regarding fraud. By distancing ourselves from sub-cultural theories, a unique contribution of our results has revealed that several supposedly criminal conducts of Yahoo Boys (commonly seen as sub-cultures) are closely akin to those of respectable groups of people (dominant cultures). Indeed, Twitter comments exposed that both groups (politicians and Yahoo Boys) engage in similar practices that constitute fraud and corruption. Thus, the authors argue that Yahoo Boys are attracted to cyber-criminality, not primarily because of oppositional morality from that of Nigerian society.

Specifically, the value of ‘advantageous comparison’ becomes more apparent because it highlights cybercriminals’ similarities to Nigerian society instead of their dissimilarities. By the same token, it obscures the seeming differences between the ‘respectable group’ and the ‘deviant group’. But that is not all. The deployment of advantageous comparison facilitates new ways of seeing previously invisible relationships between the uber-criminalization of the powerless and the non-criminalization of the powerful in Nigerian society.

Bandura’s (1999) original formulation of “advantageous comparison” as a sub-set of cognitive restructuring conceived it as a neutralization technique, which offenders use to sanitize their reprehensible actions and minimize the feeling of guilt from those actions. Ribeaud and Eisner (2010) elaborated that exploiting exonerative comparisons with more reprehensible conduct to neutralize injurious conduct or make it appear of little consequence produces an overlap with mechanisms of distorting consequences and displacing responsibilities. However, the authors of this article extend these ideas to encompass people’s rationalizations and expressions about other people’s actions. The extension of advantageous comparison and its by-products (distortion of consequences and diffusion of responsibilities) to cover people’s sentiments and attitudes toward condemnable conduct is new in the field. It is also a unique theoretical contribution in its own right. Our extension of Bandura’s (1999) conceptual lens is invaluable in multiple fields of study, such as social psychology, cyberpsychology, cyber criminology, and cultural sociology.

By exploiting advantageous comparison in their discussions of the tweets of the EFCC, Twitter users highlight that the portrayed view that the values and actions of the powerful and “respectable” group of Nigerians are less deviant than that of Yahoo Boys is misplaced. On the flip side, the manifestation of advantageous comparison as a preferred technique of choice by Twitter users exposes their unified trivialization of Yahoo Boys’ economic actions and, by implication, denies the sufferings of their victims worldwide. For example, many respondents innovatively merged the

names of a former chairman of the EFCC (Mr. Ibrahim Magu) and an alleged high-profiled cybercriminal (popularly known as HushPuppi) as “Hush Ibrahim”, “Hush Magu”, and “Puppi Magu”). The new usage of these phrases is essential linguistic manoeuvring, enabling a comprehensive and sharp comparison of the similarities between cyber fraudsters (Yahoo Boys), generally dramatized as offenders, and politicians, often and uncritically seen as law-abiding citizens. So, the linguistic juxtapositions of the “bad” and the “worse” actions and groups by Twitter users serve as exonerative devices on social media and have real-life consequences. By implication, if what was once morally condemnable becomes a source of valuation, it becomes a source of valuation in its consequences in society.

There are multiple possible explanations for the prominence of negative responses on Twitter-verse concerning the conduct of the EFCC in enforcing cybercrimes in the Nigerian context discussed above. First, it could be that a significant number of the tweets come from Yahoo Boys and their allies themselves. Second, it could also be that bots are flooding the Twitter account of the EFCC with negative responses on Twitter-verse. Third, the worldviews of the “respectable” Nigerian population could be underrepresented as most of them may not have Twitter accounts. Fourth, many Twitter users who posted negative responses about the EFCC did so under the cloak of anonymity. Their negative expressions may not reflect the subtleties of their worldview. Fifth, as researchers pointed out, as researchers pointed out, social desirability plays a role in the architecture of Twitter data (Bartley et al., 2021; Lazarus and Button, 2022).

For example, if a Twitter user sees a post with ten comments supporting a strand of opinion, they might be more likely to tweet in support of that line of thought too, or else they might not comment if you had an opposing view. Ultimately, social media data sets do, through their algorithms, dictate what posts we see. Thus, if Twitter users have previously engaged with anti-EFCC content, they are more likely to see pro-cybercriminals and anti-EFCC content. But that is not all. The Twitter users’ connections are more likely to see similar content (anti-EFCC and pro-cybercriminals) because they are more likely to connect with like-minded people on Twitter. So, we concede that this form of ‘gatekeeping’ could be implicated in the architecture of Twitter data sets. Either way, based on the evidence that came to light, i.e., our data collection from 31 July 2019 to 31 December 2020, comprising N = 101,518 comments of Twitter users, we argue that the EFCC uber-criminalizes the powerless (e.g., Yahoo Boys). Of course, the same cannot be said about the powerful group (e.g., politicians). Equally, this position facilitates new ways of seeing previously invisible similarities between the ‘deviant group’ (Yahoo Boys) and ‘respectable group’ (politicians) in Nigerian society concerning fraudulent practices (as previously mentioned).

It is noteworthy that the Nigerian government, from mid-2021 to early 2022, banned tweets originating from Nigeria possible because public opinions about the ‘respectable group’ (politicians) are highly negative (Guardian, 2021). By implication, Twitter users based in Nigeria could not say anything negative about the system when Twitter was banned. Although this ban happened after our data collection, it suggests that some of the negative responses of Nigerians about the system are well-placed. This position also aligns with our data, as illustrated above. Only by following the proper data analysis steps can ‘authentic’ accounts be generated, as Komulainen (2007) and Ribbens (1989) discussed. Indeed, the method described above has enabled us to arrive at the empirical insights presented in this discussion. Again, it has helped us shed light on the opinions of Twitter users of one society at one point in time and space, which is critical to the claims. Hence, our evidence and claims are based on comments of Twitter users that we analyzed and coded the data based on a component of mechanisms of moral disengagement (i.e., advantageous comparison).

6.3. Limitations

First, using Twitter data is that it might not fully represent society partly because Twitter users are a selective group. Many ordinary Nigerians live in abject poverty and have no access to the appropriate

technology required to use Twitter. Similarly, only a group of computer-literate people are motivated to use Twitter, follow the EFCC, and tweet their views. Second, some Twitter users who tweet their expressions may be cybercriminals and their allies. Third, the relative anonymity of social media might lead some respondents to espouse more extreme and controversial comments. For example, had we interviewed the same tweeters face-to-face, they might have been reluctant to reveal their 'authentic' views about cyber fraudsters and politicians. Fourth, the codes in Table 2 are not the only codes derivable from the dataset had we followed alternative approaches to qualitative data analysis. Hence, the findings of our study are based on these codes in Table 2.

7. Conclusion

In conclusion, the article has presented unique findings on Nigerian perspectives on the enforcement action of the EFCC on Yahoo Boys, highlighting the value of local worldviews and epistemologies. Doing so has shown that people's expressions on Twitter served as a lens through which the seemingly disorganized social issues are organized as connected parts of a whole. Specifically, advantageous comparison, the linguistic strategy, thus, has cast a critical gaze on similarities between cyber fraudsters (Yahoo Boys) and Nigerian politicians, often ignored or even denied. Hence, it is illogical to consider Yahoo boys 'alien' to the body of Nigerian society. On the contrary, these cyber fraudsters are but a disturbing reflection of society instead. "Like claimed law-abiding Nigerians, Yahoo Boys, far from deviating, conform to the commonly held indigenous worldview" (Lazarus, 2019a, p.12). While Yahoo Boys are online fraudsters, many affluent Nigerians, especially politicians ("Yahoo Men"), engage in similar practices that constitute fraud.

Thus, the study has presented a qualitative analysis of engaged tweets to explore how people harnessed Twitter to bring public attention to otherwise ignored social-cultural issues about the production and policing of cybercrime that emanates from Nigeria. Because the line dividing non-offenders and cybercriminals is not clear, it is challenging, therefore, to categorize cybercriminals' actions as a 'subculture', i.e., a subset detached and different from the body of the dominant culture. Hence, we term this phenomenon of tweeting about Nigerian cybercriminals as *hostis humani generis*: "media trials". They are "media trials" since the EFCC's tweets about cybercriminals trigger public sentiments, expressions, testimonies, and verdicts.

Using Twitter to share their views and advocate for more transparent policing regarding Yahoo Boys, everyday Nigerians may increase mainstream attention to this layer of cybercrime. Indeed, the Twitter platform gives a voice to people who are otherwise powerless to advocate for social change about the uber-criminalization of the powerless and the non-criminalization of the powerful. Thus, the advantageous comparison has served as vital linguistic manoeuvring that facilitates a sharp comparison of the similarities between the Yahoo Boys (deviant and powerless group) and politicians ("respectable" and powerful group). By implication, people's actions and expressions online reflect their attitudes and sentiments in society. Online fraud is a globalized phenomenon. Therefore, our article's discussions on cybercrime issues in a Nigerian context regarding the similarities between fraudulent politicians ("Yahoo Men") and cyber fraudsters ("Yahoo Boys") have international significance and consequences.

Declarations

Author contribution statement

Suleman Lazarus: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools, or data; Wrote the paper.

Mark Button: Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools, or data; Wrote the paper.

Afe Adogame: Analyzed and interpreted the data; Contributed reagents, materials, analysis tools, or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability statement

Data will be made available on request.

Declaration of interest's statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

Acknowledgements

We thank Professor Shannon Mason (University of Nagasaki), Professor Tim Newburn (London School of Economics and Political Science), and Professor Radosveta Dimitrova (Stockholm University) for their comprehensive, insightful, and helpful comments on parts of our initial draft.

References

- Adibe, R., Ike, C.C., Udeogu, C.U., 2017. Press Freedom and Nigeria's Cybercrime Act of 2015: An Assessment. *Africa Spectrum* 52 (2), 117–127.
- Adogame, A., 2009. The 419 code as business unusual: youth and the unfolding of the advance fee fraud online discourse. *Asian J. Soc. Sci.* 37 (4), 551–573.
- Adeduntan, A., 2022. Rhyme, reason, rogue: Yoruba popular music and the hip hop amoral turn. *J. Popular Music Stud.* 34 (1), 44–67.
- Ahmed, S., Cho, J., Jaidka, K., 2018. Leveling the playing field: the use of Twitter by politicians during the 2014 Indian general election campaign. *Telematics Inf.* 34 (7), 1377–1386.
- Akanle, O., Adesina, J. O., & Akarah, E. P., 2016. Towards human dignity and the internet: The cybercrime (yahoo yahoo) phenomenon in Nigeria. *African Journal of Science, Technology, Innovation and Development* 8 (2), 213–220.
- Alzubaidi, A., 2021. Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon* 7 (1), e06016.
- Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychol., Behav. Soc. Netw.* 14 (12), 759–763.
- Asher, M., Leston-Bandeira, C., Spaiser, V., 2019. Do parliamentary debates of e-petitions enhance public engagement with parliament? An analysis of twitter conversations. *Pol. Internet* 11 (2), 149–171.
- Bandura, A., 1999. Moral disengagement in the perpetration of inhumanities. *Pers. Soc. Psychol. Rev.* 3 (3), 193–209.
- Bartley, N., Abeliuk, A., Ferrara, E., Lerman, K., 2021. Auditing algorithmic bias on twitter. In: *13th ACM Web Science Conference 2021*, pp. 65–73.
- BBC, 2020. EFCC Chairman Ibrahim Magu wey chop suspension for an allegation of corruption don comot from detention on bail. Retrieved from: <https://www.bbc.com/pidgin/tori-53420184>. Accessed 22/07/20.
- Becker, H., 1967. *Outsiders: Studies in Sociology of Deviance*. Simon & Schuster, New York, NY.
- Chawki, M., Darwish, A., Khan, M.A., Tyagi, S., 2015. 419 scam: an evaluation of cybercrime and criminal code in Nigeria. In: Chawki, M., Darwish, A., Khan, M.A., Tyagi, S. (Eds.), *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing, Berlin, pp. 129–144.
- Correa, J.C., Camargo, J.E., 2017. Ideological consumerism in Colombian elections, 2015: Links between political ideology, Twitter activity, and electoral results. *Cyberpsychol., Behav. Soc. Netw.* 20 (1), 37–43.
- Cross, C., 2018. Marginalized voices: the absence of Nigerian scholars in international examinations of online fraud. In: *The Palgrave Handbook of Criminology and the Global South*. Palgrave Macmillan, Cham, pp. 261–280.
- Daxecker, U., Di Salvatore, J., Ruggeri, A., 2019. Fraud is what people make of it: election fraud, perceived fraud, and protesting in Nigeria. *J. Conflict Resolut.* 63 (9), 2098–2127.
- Egielewa, P.E., 2022. Yahooism or Internet Fraud in the Nigerian Higher Education System. *Journal of Ethics in Higher Education. Journal of Ethics in Higher Education* 1, 75–101.
- Ellis, S., 2016. *This Present Darkness: A History of Nigerian Organized Crime*. Oxford University Press, Oxford.
- Geertz, C., 1973. *The Interpretation of Cultures*. Fontana, London.

- Gilli, A., Gilli, M., 2018. Why China has not caught up yet: military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage. *International Security* 43 (3), 141–189.
- Goffman, E., 1978. *The Presentation of Self in Everyday Life*, vol. 21. Harmondsworth, London.
- Guardian, 2021. Nigerian government threatens to rein in the press after the Twitter ban. Retrieved from: <https://www.theguardian.com/world/2021/jun/29/nigerian-government-threatens-to-rein-in-press-after-twitter-ban>. Accessed 14/07/21.
- Hai-Jew, S., 2020. The remote Woo: exploring faux transnational interpersonal romance. In: Hai-Jew, S. (Ed.), *Social Imagery. Social World Sensing via Social Image Analysis from Social Media*. New Prairie Press., New York. <https://newprairiepress.org/ebooks/37>.
- Hall, T., Hudson, R., 2022. The economic geographies of transactional organized crime. In: Allum, F., Gilmour, S. (Eds.), *The Routledge Handbook of Transnational Organized Crime*. Routledge, Abingdon, Oxon.
- Hall, T., Sanders, B., Bah, M., King, O., Wigley, E., 2020. Economic geographies of the illegal: the multiscale production of cybercrime. *Trends Organ. Crime* 24 (2), 282–307.
- Holt, T.J., Navarro, J.N., Clevenger, S., 2020. Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency* 66 (11), 1533–1555.
- Hsieh, H.F., Shannon, S.E., 2005. Three approaches to qualitative content analysis. *Qual. Health Res.* 15 (9), 1277–1288.
- Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals. *Int. J. Law Crime Just.* 47, 44–57. In this issue.
- Ibrahim, S., 2017. Causes of socioeconomic cybercrime in Nigeria. In: Paper Presented at IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). Canada, Vancouver, BC, pp. 1–9.
- Idom, A.M., Tormusa, D.O., 2016. Causes, Types and Likely Victims of Cybercrimes in Selected Higher Institutions in South-South, Nigeria. *FULafia Journal of Social Sciences* 1 (1), 209–224.
- Jaishankar, K., 2018. Cyber criminology as an academic discipline: history, contribution, and impact. *Int. J. Cyber Criminol.* 12 (1), 1–8.
- Karamouzas, D., Mademlis, I., Pitas, I., 2022. Public opinion monitoring through collective semantic analysis of tweets. *Social Network Anal. Min.* 12 (1), 1–21.
- Khlomov, K.D., Davydov, D.G., Bochaver, A.A., 2019. Cyberbullying in the experience of Russian teenagers. *Psychol. Law* 9 (2), 276–295.
- Koiranen, I., Koivula, A., Keipi, T., Saarinen, A., 2019. Shared contexts, shared background, shared values—Homophily in Finnish parliament members' social networks on Twitter. *Telematics Inf.* 36, 117–131.
- Komulainen, S., 2007. The ambiguity of the child's 'voice' in social research. *Childhood* 14 (1), 11–28.
- Kurten, S., Beullens, K., 2021. # Coronavirus: monitoring the Belgian twitter discourse on the severe acute respiratory syndrome coronavirus 2 pandemic. *Cyberpsychol., Behav. Soc. Netw.* 24 (2), 117–122.
- Lazar, D., 2008. Selected issues in the philosophy of social science. In: Seale, C. (Ed.), *Researching Society and Culture*. SAGE Publications, London, pp. 7–20.
- Lazarus, S., 2018. Birds of a feather flock together: the Nigerian cyber fraudsters (yahoo boys) and hip hop artists. *Criminol., Crimin. Just., Law Soc.* 19 (2), 63–80.
- Lazarus, S., 2019a. Where is the money? The intersectionality of the spirit world and the acquisition of wealth. *Religions* 10 (3), 146.
- Lazarus, S., 2019b. Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *Int. Soc. Sci. J.* 69 (231), 15–33.
- Lazarus, S., 2020. Establishing the Particularities of Cybercrime in Nigeria: Theoretical and Qualitative Treatments. Doctoral dissertation. University of Portsmouth.
- Lazarus, S., Button, M., 2022. Tweets and reactions: revealing the geographies of cybercrime perpetrators and the North-South divide. *Cyberpsychol., Behav., Social Network.* 25 (8), 504–511.
- Lazarus, S., Okolorie, G.U., 2019. The bifurcation of the Nigerian cybercriminals: narratives of the economic and financial crimes commission (EFCC) agents. *Telematics Inf.* 40, 14–26.
- Lazarus, S., Button, M., Kapend, R., 2022. Exploring the value of feminist theory in understanding digital crimes. *Howard J. Crim. Justice* 61 (3), 381–398.
- Leelawat, N., Jariyapongpaiboon, S., Promjun, A., Boonyarak, S., Saengtabtim, K., Laosunthara, A., et al., 2021. Twitter data sentiment analysis of tourism in Thailand during the COVID-19 pandemic using machine learning. *Heliyon* 8 (10).
- Leukfeldt, E.R., Notté, R.J., Malsch, M., 2020. Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Vict. Offenders* 15 (1), 60–77.
- Lewis, J.S., 2020. *Scammer's Yard: the Crime of Black Repair in Jamaica*. U of Minnesota Press.
- Lim, Y.S., Lee-Won, R.J., 2017. When retweets persuade: the persuasive effects of dialogic retweeting and the role of social presence in organizations' Twitter-based communication. *Telematics Inf.* 34 (5), 422–433.
- Mason, S., 2019. Teachers, Twitter, and tackling overwork in Japan. *Issues Educ. Res.* 29 (3), 881–898.
- Mason, S., Singh, L., 2022. Reporting and discoverability of "Tweets" quoted in published scholarship: current practice and ethical implications. *Res. Ethics*.
- Matza, D., Sykes, G.M., 1961. Juvenile delinquency and subterranean values. *Am. Socio. Rev.* 26 (5), 712–719.
- Mba, G., Onaolapo, J., Stringhini, G., Cavallaro, L., 2017. Flipping 419 cybercrime scams: targeting the weak and the vulnerable. In: *Proceedings of the 26th International Conference on World Wide Web Companion*, pp. 1301–1310.
- McGuire, M.R., 2017. Technology crime and technology control: contexts and history. In: *The Routledge Handbook of Technology, Crime and Justice*. Routledge, London, pp. 35–60.
- Melvin, A.O., Ayotunde, T., 2010. Spirituality in cybercrime (yahoo yahoo) activities among youths in southwest Nigeria. In: *youth culture and net culture: online social practices*. IGI Global 357–376.
- Meyers, A., 2018. Not your fairy-tale prince: the Nigerian business email compromise threat. *Comput. Fraud Secur.* 2018 (8), 14–16.
- Morse, Y.L., 2019. Elite interviews in the developing world: finding anchors in weak institutional environments. *Qual. Res.* 19 (3), 277–291.
- Ndubueze, P.N., 2020. Cybercrime and legislation in an African context. In: *The Palgrave Handbook of International Cybercrime and Cyber Deviance*, pp. 345–364.
- Newburn, T., Stanko, E.A., 2013. Just boys doing business? men, masculinities and crime. Routledge, London.
- Newburn, T., 2011. Policing youth anti-social behaviour and crime: time for reform? *Journal of children's services*, 6 (2), 96–105.
- Ogunleye, Y.O., Ojedokun, U.A., Aderinto, A.A., 2019. Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-West Nigeria. *Int. J. Cyber Criminol.* 13 (2), 309–325.
- Ojedokun, U.A., Eraye, M.C., 2012. Socioeconomic lifestyles of the yahoo-boys: a study of university students' perceptions in Nigeria. *Int. J. Cyber Criminol.* 6 (2), 1001–1013.
- Ojeka, S., Adegboye, A., Adegboye, K., Umukoro, O., Dahunsi, O., Ozordi, E., 2019. Corruption perception, institutional quality and performance of listed companies in Nigeria. *Heliyon* 5 (10), e02569.
- Okosun, O., Ilo, U., 2022. The evolution of the Nigerian prince scam. *Journal of Financial Crime*, (ahead-of-print). *Journal of Financial Crime*.
- Okpa, J.T., Okorie, A.B., Nzeakor, O.F., Eshiotse, E., Abang, T.A., 2022. Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Secur. J.* 1–23.
- Pierce, S., 2016. *Moral Economies of Corruption*. Duke University Press, Durham, NC.
- Reiner, R., 2016. *Crime, the Mystery of the Common-Sense Concept*. John Wiley & Sons, New York.
- Ribbens, J., 1989. Interviewing—an "unnatural situation"? *Wom. Stud. Int. Forum* 12 (6), 579–592.
- Ribeaud, D., Eisner, M., 2010. Are moral disengagement, neutralization techniques, and self-serving cognitive distortions the same? Developing a unified scale of moral neutralization of aggression. *Int. J. Conflict Violence* 4 (2), 298–315.
- Ricciardelli, R., Adorjan, M., 2019. "If a girl's photo gets sent around, that's a way bigger deal than if a guy's photo gets sent around": Gender, sexting, and the teenage years." *Journal of Gender Studies* 28 (5), 563–577.
- Rich, T., 2017. You can trust me: a multimethod analysis of the Nigerian email scam. *Secur. J.* 31 (1), 208–225.
- Rivera, R., Pazmiño, L., Becerra, F., Barriga, J., 2022. An Analysis of Cyber Espionage Process. In: *Developments and Advances in Defense and Security*. Springer, Singapore, pp. 3–14.
- Santoveña-Casal, S., Gil-Quintana, J., Ramos, L., 2021. Digital citizens' feelings in national# Covid 19 campaigns in Spain. *Heliyon* 7 (10).
- Šupa, M., 2021. Social research about online crime: global range of topics and a systematic analysis of research in Lithuania. *Kriminologijos Studijos* 9, 8–46.
- Sykes, G.M., Matza, D., 1957. Techniques of neutralization: a theory of delinquency. *Am. Socio. Rev.* 22 (6), 664–670.
- Tade, O., Aliyu, I., 2011. Social organization of internet fraud among university undergraduates in Nigeria. *Int. J. Cyber Criminol.* 5 (2), 860–875.
- Tannenbaum, F., 1938. *Crime and the Community*. Columbia University Press, New York.
- The Cable, 2019. "China controls its 1.3 bn people — Aisha Buhari backs regulation of social media" in the Cable. Retrieved: <https://www.thecable.ng/china-controls-its-1-3bn-people-aisha-buhari-backs-regulation-of-social-media>. Accessed 20/06/21.
- Thomas, W.I., 1923. *The Unadjusted Girl*. Little Brown and Company, Boston.
- Timofeyev, Y., Dremova, O., 2022. Insurers' responses to cyber crime: evidence from Russia. *Int. J. Law, Crime Just.* 68, 100520.
- Tournay, V., Jacomy, M., Néculea, A., Leibing, A., Blasimme, A., 2020. A new web-based big data analytics for dynamic public opinion mapping in digital networks on contested biotechnology fields. *OMICS A J. Integr. Biol.* 24 (1), 29–42.
- Wall, D.S., 2013. *Cybercrime*. Polity, Cambridge.
- Wang, F., Zhou, X., 2022. Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (杀猪盘) in China. *Victims & Offenders*, 1–28.
- Whittaker, J.M., Edwards, M., Cross, C., Button, M., 2022. "I Have Only Checked after the Event": Consumer Approaches to Safe Online Shopping. *Victims & Offenders* 1–23.
- Zakari, M.B., Button, M., 2021. Confronting the monolith: insider accounts of the nature and techniques of corruption in Nigeria. *J. White Collar Corp. Crime*.
- Zsila, Á., Urbán, R., Griffiths, M.D., Demetrovics, Z., 2019. Gender differences in the association between cyberbullying victimization and perpetration: The role of anger rumination and traditional bullying experiences. *International Journal of Mental Health and Addiction* 17 (5), 1252–1267.