Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals

Suleman Ibrahim

The Center for Doctoral Training in Cyber Security, The Information Security Group, Royal Holloway University of London, TW20 0EX, Surrey, UK

Abstract

This article aims to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. Nigeria is representative of the Sub-Saharan region, and an exemplary cultural context to illustrate the importance of incorporating social and contextual factors into cybercrime classifications. This paper anchors upon a basic principle of categorisation alongside motivational theories, to offer a tripartite conceptual framework for grouping cybercrime nexus. It argues that cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. Whilst this contribution challenges the statistics relied on to inform the prevalence of cybercrime perpetrators across nations, it provides new ways of making sense of the voluminous variances of cybercrime. Concomitantly, it enables a clearer conceptualisation of cybercrime in Nigeria and elsewhere, because jurisdictional cultures and nuances apply online as they do offline.

© 2016 The Author. Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

This paper sets out with the aim of developing and improving upon existing taxonomies used in cybercrime scholarship. Listed in prevalence of cybercrime perpetrators, Nigeria, the UK and the USA (in ascending order of significance) are on top of the ‘league table’ (Internet Crime Complaint Center - ICCC, 2006–2010). Considering Nigeria as an exemplary social context – representing the Sub-Saharan world region - this article will emphasise the need to incorporate social and contextual factors into the classification schemas. Whilst the establishment of the particularities of cybercrime in Nigeria will concomitantly suggest problems with prevailing taxonomies of cybercrime, it will also render problematic, the basis for ICCC’s (2006–2010) claim on the prevalence of cybercrime perpetrators.

Whilst cybercrime primarily operates in the realm of cyberspace, terrestrial crimes operate in physical spaces (Manjikian, 2010). Seeking to summarise and encapsulate various conceptualisations within cybercrime literature, Yazdanifard et al. (2011) defined ‘cybercrime’ as ‘any type of intentional criminal scheme that is computer or/and internet-mediated’. However, whilst such a description describes a wide spectrum of cybercrime, it fails to account for the dual model of criminal schemes within cyberspace. Ogwezzy (2012, p.91) elaborated that the term ‘cybercrime’ implies “offences committed through the use of the computer in contrast to ‘computer crime’ which refers to offences against the computer and data or

E-mail address: suleman.ibrahim.2014@rhul.ac.uk.

Cyberspace is a borderless global space, a site for the globalization of threats as well as benefits (Manjikian, 2010).
program therein’. Whilst the computer and its content are the primary targets in computer crimes, the meaning of cybercrime is wrapped around the use of a computer or/and the Internet to commit age-old crimes (Ogwezzy, 2012; McGuire and Dowling, 2013).

Conceptions of ‘computer crime’ and ‘cybercrime’ interpenetrate one another; their entities are intertwined and therefore difficult to disentangle. The intertwining of computer crime and cybercrime further challenges the simplistic rendering of cyberspace and physical space as two different entities with easily defined boundaries. Regarding ‘cybercrime’, there are over 30 types identified in existing literature, since cyberspace-crime linkage was first constructed in cyberpunk stories (Wall, 2008). Most of them are listed in Table 1 below. These numerous variances are implicated in obscuring the effective conceptualisation of ‘cybercrime’. Yet, whilst the existing dichotomised categories (Gordon and Ford, 2006; McGuire and Dowling, 2013) adhere to the basic psychological principle of categorisation (Rosch, 1978), they fail to acknowledge the roles of motivations in offending. Relatedly, when the existing motivational categories (Chawki et al., 2015a; Wall, 2013) do consider the motivational element of offending, they take for granted the basic psychological principle of categorisation. Insights from Rosch’s (1978, p.28) general and basic principles for the formation of categories stipulate that:

“the task of category systems is to provide maximum information with the least cognitive effort [and] the perceived world comes as structured information rather than as arbitrary attributes. Thus maximum information with least cognitive effort is achieved if categories map the perceived world structure as closely as possible. This condition can be achieved either by the mapping of categories to given attribute structures or by the definition or redefinition of attributes to render a given set of categories appropriately structured”.

In line with motivational theories framed within the basic psychological framework of categorisation, this current endeavour will, firstly, aim not only to complement the existing categories but also offer a more conceptually robust framework for grouping cybercrime. The implication being that whilst cybercrimes constitute a global problem, recognising the limits of a ‘one size fits all’ binary of taxonomies is of utmost importance. Secondly, Nigeria will be presented as an exemplary cultural context to illustrate certain aspects of these limitations (binary model) and the importance of social/contextual factors in the classification schemas. Through the precise delineation of the particularities of cybercrime in Nigeria, this article aims to determine the extent to which this exemplar problematises or contradicts prevailing taxonomies of cybercrime. At its core, this paper has three research questions, which it will aim to answer: firstly, how useful are the existing cybercrime taxonomies in making sense of social and contextual factors (such as the category of cybercrimes that the Nigerian cybercriminals exclusively commit)? Secondly, since ‘cybercrime’ is a globalised phenomenon, how is the Nigerian case—representing the Sub-Saharan region, any different from Western regions? Thirdly, what exactly is ‘cybercrime’ in a Nigerian context?

2. A dual model of cybercrime

The word ‘cybercrime’ comprises a wide range of online crimes. For McGuire and Dowling (2013, p.5), “[C]yber-dependent crimes are offences that can only be committed by using a computer, computer networks, or other forms of ICT [Information and Communications Technology]” such as creation or/and distribution of malwares/viruses. On the other hand, cyber-enabled crimes “can still be committed without the use of ICT” such as cyber fraud. These dual categories are illustrated in Fig. 1. Unlike traditional crimes however, one criminal scheme in the realm of cyberspace may involve multiple nations and actors and even impact on multiple nations simultaneously (Yazdanifard et al., 2011). Thus whilst traditional crime tends to be regarded locally, cybercrime is usually considered on a global scale (Yar and Jewkes, 2010). For example, if a person in Russia creates computer ‘viruses/malwares’ while another person in Nigeria rents it to send credit scam e-mails and a third party in the USA transfers funds using the illegally acquired data, (Wall, 2013), all three individuals are implicated in different strands

<table>
<thead>
<tr>
<th>Table 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tripartite cybercrime framework (TCF).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Socioeconomic cybercrime</th>
<th>Psychosocial cybercrime</th>
<th>Geopolitical cybercrime</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Hackers and crackers</em></td>
<td><em>Hackers and crackers</em></td>
<td><em>Hackers - Hacktivist</em></td>
</tr>
<tr>
<td>Cyber fraud</td>
<td>Child pornography</td>
<td>Cyber spies</td>
</tr>
<tr>
<td>Cyber embezzlement</td>
<td>Cyber stalking</td>
<td>Cyber espionage</td>
</tr>
<tr>
<td>Cyber piracy</td>
<td>Cyber bullying</td>
<td><strong>Cyber terrorism</strong></td>
</tr>
<tr>
<td>Cyber blackmail</td>
<td>Revenge porn</td>
<td>Cyber Vandalism</td>
</tr>
<tr>
<td>Romance scam</td>
<td>Cyber rape</td>
<td>Cyber assault</td>
</tr>
<tr>
<td>Online drug trafficking</td>
<td><em>Cyber hate speech</em></td>
<td>Cyber hate speech</td>
</tr>
<tr>
<td>Cyber prostitution</td>
<td><em>Cyber extortion</em></td>
<td>Cyber riot</td>
</tr>
<tr>
<td><em>Cyber extortion</em></td>
<td>Obscenity</td>
<td>Cyber sabotage</td>
</tr>
<tr>
<td>Illegal online gambling</td>
<td><em>Cyber-prostitution</em></td>
<td>Cyber-colonialism</td>
</tr>
<tr>
<td><em>Cyber Trespass</em></td>
<td><em>Cyber Trespass</em></td>
<td>Cyber rebellion</td>
</tr>
<tr>
<td><em><strong>Cyber terrorism</strong></em></td>
<td><em>Cyber homicide</em>**</td>
<td><em><strong>Cyber terrorism</strong></em></td>
</tr>
</tbody>
</table>

*Where the type of cybercrime appears in more than one column.

***Where the type of cybercrime appears in more than two columns.
of cybercrime. Whilst all three actors are motivated by monetary benefits, they are in fact involved in cyberspace in varying degrees. The virus/malware creator has committed a cyber-dependent offence, whereas the other two have committed cyber-enabled offences. This existing traffic between cyber-enabled and cyber-dependent categories clearly illustrates the complexity of cybercrime and how one criminal act can impact on multiple nations and involve various networks of actors simultaneously.

Closely related to cyber-enabled and cyber-dependent categories are ‘techno-centric (type I) and people-centric (type II) subsets’. Gordon and Ford (2006, p.15) specifically posited that techno-centric and people-centric cybercrime are at the opposite ends of a continuum; dichotomising cybercrime based on the strength of the cyber-element versus people-component of the criminal act in question. They distinguished Type I (techno-centric) crimes such as e-commerce fraud, cyber-vandalism, data manipulations through hacking, phishing, from Type II (people-centric) crimes such as cyber fraud, cyber bullying and cyber-stalking as illustrated in Fig. 1. The latter being less technologically oriented than the former and therefore grounded in perpetrator-victim interactions. These binary models (people-centric and techno-centric; cyber-enabled and cyber-dependent), anchoring on a basic psychological principle of categorisation, have no doubt offered a useful tool in looking at voluminous cybercrime variances.

However, motivational elements are not configured in the properties of these binary typologies. As a result, they are ill-equipped to differentiate between the psychological-motivated cybercrimes such as cyber stalking and cyber embezzlement. Simply put, they have taken for granted the motivational lens of looking at cybercrime, which renders them unable to answer a simple question: how exactly is a digital crime that is primarily geared towards defrauding a person or a group of persons, different to another online scheme intended to fundamentally disrupt a person’s psychological state of mind? It is essential to isolate the primary motive behind cybercrimes in the meaning-making of what any particular cybercrime is in a given context, as illustrated in Table 2 below.

It is reasonable therefore to argue for grouping cybercrimes according to criminals’ motivations. This could and would sharpen the distinction between cybercrimes that are rooted in financial gains such as cyber fraud, and psychologically motivated cybercrimes such as cyber stalking. However, conceptually, the above binary models appear to be ‘explanatory-tools’, which cannot capture the differences between cybercrimes primarily driven by financial rewards and cybercrimes fundamentally propelled by psychological benefits as shown in Table 2. Based on these rationales, it is reasonable to complement these models – ‘techno-centric and people-centric (Gordon and Ford, 2006) and cyber-enabled crime and cyber-dependent (McGuire and Dowling, 2013). That said, the existing motivational categories, despite usefulness in acknowledging the motivational element of cybercrime, have their limitations too.

3. Some existing motivational taxonomies

In endorsing motivational categories, Chawki et al. (2015a, p.16–17) argued that it is crucial to understand a person’s profile in the case of a particular cybercrime. Particular educational attainment, occupation and childhood experiences, he
argued, help shed light on the individual implicated in any cybercrime. As Chawki et al. (2015a) further postulated that cybercriminals can be categorized as: [a] children and adolescents [b] organized hackers [c] professional hackers [d] discontent employees. Whilst Chawki et al.’s (2015a) categories tell us about different levels of sophistication involved in offending (e.g., professional hackers and organized hackers), they also reveal the extent to which cybercriminals could be age-graded.

However, cross-cultural insights from young offenders have pointed out that age is not lived similarly across cultures and age-related behaviours are constituted differently across cultures (Brathwaite, 1996; Cain, 2000). For example, in line with Tade and Aliyu’s (2011) sociological work in Nigeria and Armstrong’s (2011) anthropological analysis in Ghana, most ‘young people’ in Nigerian and Ghanaian universities involved in cybercrime in general are involved in cyber fraud in particular. In contrast, studies on Canadian undergraduates (Cunningham et al., 2014; Faucher et al., 2014) university students in the USA (Lindsay and Krysk, 2012) ‘young people’ in Finland (Oksanen and Keipi, 2013) and higher education students in Britain (Benson et al., 2015; Boulton et al., 2012) suggest that young people in Canada, Finland, the USA, and Britain — the Western world region, are more involved in psychological-oriented cybercrime such as cyber bullying and cyber harassment than cyber-fraud. The key point is that “young people” as a category is insensitive to the differentiation between what is true of all societies and ‘what is true of one society at one point in time and space’ (Nelken, 2010). Another limitation is that, Chawki et al.’s (2015a) taxonomy does not adhere to the basic principles of categorisation.

In a similar vein, Wall 2007 (2013, p.62–65) proposed seven different motivational subsets, based on: self-satisfaction; the need for peer respect; to impress potential employers; criminal gain or commercial advantage; revenge; distance from victim; politically motivated protest. These motivational signposts help to illustrate that the specific motivations behind cybercrime are diverse. An equally important issue is that the seven subsets for cyber offenders, as revealed by their titles, shed more light on the drives, the ‘push and pull factors’ of cybercriminals to cybercrime (Wall, 2013). The value of this grouping is most evident in the ‘criminal gain or commercial advantage’, and ‘politically motivated’ categories. For example, whilst some types of cybercrime such as cyber extortion, cyber fraud and cyber embezzlement fit squarely under the canopy of the former, cyber espionage, cyber terrorism, cyber rebellion, can be located smoothly in the sphere of the latter.

There is however, a primary limitation of this taxonomy, as aforementioned, in that it neglects the basic principle of categorisation. Some of the proposed groups, such as ‘distance from the victim’ involve almost all types of cybercrime. Indeed, ‘distance from the victim’ is a specific aspect of most cybercrimes as Brown (2001) intimated in the analysis of cost-benefits and economics of criminal conducts. Similarly, ‘self-satisfaction’ – rooted in the utilitarian maximisation principle – may be in the form of tangible things such as monetary reward or intangible ones such as psychological thrill. Either way, ‘self-satisfaction’ is integral to almost all types of cybercrime, and arguably does not seem to represent a specific category of cybercrimes.

In the same vein, ‘revenge’ as a category could be the driver of cyber stalking, cyber fraud, or hacking. Whilst ‘revenge’ may be a principal impetus behind this range of cybercrimes, it requires a lot of cognitive effort to see the ‘rope’ that binds them together as a distinct subset. ‘Thus maximum information with least cognitive effort is only achievable if categories map the perceived world structure as closely as possible’ (Rosch, 1978, p.28). The crux is that existing motivational categories (Chawki et al., 2015a; Wall, 2013) have ignored a basic psychological principle of categorisation (Rosch, 1978, p.28): ‘to simplify a complex set of data and increase information intake with the least cognitive effort’.

4. The tripartite cybercrime framework (TCF)

In complementing the above taxonomies, this current endeavour anchors on the basic psychological principles of categorisation alongside motivational insights to offer a 2tripartite-cybercrime-framework (TCF). An individual is said to be motivated when such an individual is moved, energised, or inspired to do something (Deci and Ryan, 2011, 2000, 1985). Motivation is orientation graded; it varies according to the underlying variable behind the actions in question. It can also vary in terms of the intensity of occurrence, i.e., whether a person is highly motivated or otherwise. Whilst the latter centers on the amount or size of impetus behind the action, the former is concerned with the reason for the action. Arguably motivation can be conceptualised as the foundation of most crimes; it is reasonable therefore to offer a social/contextual basis for the

---

2 This article uses the tripartite cybercrime framework (TCF) or the tripartite conceptual framework (TCF) interchangeably.
categorizing of cybercrime. Self-Determination Theory (Deci and Ryan, 2011; 1985) specifically argues that motivational types - intrinsic and extrinsic, define the strength or intensity of motivation.

Motivation therefore can be schematised as a dual phenomenon; incorporating intrinsic and extrinsic motivations. This binary model is necessary for the precision of illustrations and the discussion that follows. Whilst extrinsic motivation is the doing of an activity solely to achieve a distinct result, intrinsic motivation is the demonstration of actions inherently for the mere satisfaction of doing them (Deci and Ryan, 2011; 1985). For example, a poet is more likely to write poems for the inherent satisfaction of such an activity rather than for the approval of his/her parents – intrinsic motivation; whereas a student is more likely to study hard for a good grades and a better future – extrinsic motivation. The majority of activities are generally propelled by extrinsic motivation, i.e., people fundamentally motivated to do something due to the direct and expected consequence of their actions (Deci and Ryan, 2011; 1985).

However, as Kshetri (2006), in describing cybercriminals — hackers — emphasised, intrinsic motivation may have a superior impact compared to extrinsic motivation. This paper conceptualises extrinsic and intrinsic motivations of cyber crimes as twin interlocking entities, which are difficult to disentangle, and, as Wehmeyer and Little (2009) note, extrinsically motivated behaviours can parallel intrinsically motivated activities if actors internalise their actions, and experience flow in their activities. Nevertheless, Layous et al. (2013) pointed out that intrinsically motivated people are more likely to experience flow than those who are extrinsically motivated. Nakamura and Csikszentmihalyi (2002, p.95) defined flow as “the balance of challenges and skills when both are above average levels for the individual”. This suggests that it is a state of profound task-absorption and task-enjoyment experience, most likely to condition the actor involved to lose sense of time in doing the task in question (Csikszentmihalyi, 1990, 2000, 2014). Flow experience has the following nine components: [a] Clarity of goals at every stage [b] Availability of immediate feedback [c] a balance between challenges and skills [d] Interpenetrations of action and awareness [e] Limited distractions from consciousness [f] Absence of concern in terms of failure [g] The disappearance of self-consciousness [h] The distortion of sense of time [i] The activity is autotelic (Csikszentmihalyi, 1990, 2000, 2014). Arguably, flow experience is crucial to the understanding of cybercrime motivations.

Given that the type of primary motivation behind an action matters in relation to the opposing forces that could inhibit the intended action, underlines the importance of incorporating social factors into classification schemas. This paper also acknowledges that certain types of cybercrimes listed in Table 1 fit into two or more motivational categories. Although there are some degrees of overlap between the categories, the primary motivation behind the action is the basic tool to differentiate between types of cybercrimes. For example, whilst cyber fraud is under the socioeconomic cybercrime category, revenge porn is under the umbrella of psychosocial cybercrime, as illustrated in Table 1. Theoretically therefore, in complementing the existing categories, this paper provides a more refined motivational taxonomy based on perpetrators’ primary benefits as well as victims’ primary loss, as shown in Table 2.

As Tables 1 and 2 fundamentally illustrate, in socioeconomic cybercrimes, the perpetrator often has a direct contact with his/her victim; this can be defined as financially motivated crimes that are computer/or and internet-mediated, such as online fraud, romance scam, and e-embezzlement. Psychosocial cybercrime are cybercrimes, which are principally psychologically driven such as cyber stalking, cyber harassment and cyber rape. Whilst socioeconomic cyber criminals may aim to deflate the economy of their victims, psychosocial cyber criminals focus fundamentally on inflicting psychological distress (full analysis of the implications of the TCF, can be found further down).

Yet there remains a considerable amount of similarity between the two loose categories. Unlike the viewpoint that not all actors are economically motivated (Hayward, 2007), the analysis of the motivational drives and economic decision-making in relation to crime in general is more refined (Farrell, 2010). According to Farrell (2010), the application of utility maximisation rather than monetary benefit or economic maximisation is a more appropriate term to deploy in conceptualising the general costs and benefits of crime. Hence, psychological benefits, including expressive emotional elements and sensations, are critical in determining if crime is economically motivated or not. Flowing from the above, different primary motivations underpin different types of cybercrimes identified in literature — listed in Table 1. Collaterally, victims of cybercrimes may suffer differently based on the primary motivation - the perpetrators of cybercrime in question as shown in Table 2. Therefore, this current paper proposes that cybercrimes are motivated in three different ways: socioeconomic, psychosocial and geopolitical.

In terms of the penetrator-victim transactions, the primary driving forces behind cyber bullying, online harassment and cyber stalking are psychological in nature. Unlike fraud-based cybercrimes, the injuries as well as the benefits lie within the realm of the mind. The above distinction is not to suggest that specific motivations involved in financial crimes are absolutely non-psychological. Insights from health psychology (Lazarus, 2006; Lazarus and Folkman, 1984a, 1984b) support the fact that financial loss (e.g. due to cyber fraud) can manifest physiologically as distress. However, the key element of differentiation between socioeconomic and psychosocial categories is that the primary benefits of the perpetrators as well as the primary losses of victims are different, as illustrated in Table 2. In contrast, under the binary model discussed above, both socioeconomic and psychosocial cybercrimes are grouped as one, that is, cyber-enabled crimes. Whereas the lens of the TCF can further differentiate between the two, as well as a third category: geopolitical (as discussed further below).

For example, when these ‘cybercriminals deploy the ‘Freestyle trick’ using accounts on dating sites to befriend/condition unsuspecting victims to the point that they ‘fall in love’ with them and support them financially, the victims of Nigerian
cybercriminals’ ‘Freestyle trick’, may suffer psychological distress as well as financial loss, but the primary aim of the perpetrators is commercial gain. In terms of the predicament of victims, economic losses are more grounded in the quantifiable realm than psychosocial cybercrimes that are in the sphere of the mind.

On the other hand, geopolitical cybercrimes can be defined as those e-crimes that involve agents of statecraft or/and industrial representatives (e.g. cyber espionage). Yet even geopolitical cybercrimes constitute some elements of socioeconomic and psychological cybercrimes as illustrated in Table 2. For example, Hacktivists, primarily aiming to make a political statement could expose sensitive data from the law enforcement agencies and their actions could have economic, psychosocial and geopolitical consequences on a person or group of people. The collective consequences of the tripartite categories could lead to a security fault, which this paper calls ‘cyber insecurity’, defined as a situation where security mechanisms in both the existing cyberspace and physical space cannot guarantee perfect security, nor have the full capacity to resist and respond to both intentional and unintentional cyberspace threats and hazards. In terms of victim-perpetrator interaction, while socioeconomic and psychosocial cybercrimes are fundamentally engineered and executed on individual levels, geopolitical cybercrimes, broadly speaking, are actions of state agents, groups of individuals against other groups, nations or industrial entities acting on behalf of more complex statecraft or vested interests. In other words, each group — especially but not limited to, socioeconomic and psychosocial cybercrimes - may involve individual actors or group actors as both targets and perpetrators. A crucial element of these categories – as illustrated in Table 2, is their capacity to simplify complex sets of information, given that there are over 30 types of cybercrimes identified in the existing literature. The TCF also help to enhance our understanding of ‘cybercriminals’, and their geopolitical, socioeconomic and psychosocial factors. Another significant issue is that, unless they go against the grain that constitutes ‘normality’ in their home country, agents of statecraft that commit geopolitical cybercrimes are rarely considered ‘criminals’ at all. The assumption underpinning this is that they represent authority, rather than subversion. Therefore it is the nation they represent that is categorized as criminal, unlike individual subcultural rule breakers such as the Nigerian 419 cybercriminals.

5. What is ‘cybercrime’ in Nigeria?

Drawing on the TCF as shown in Tables 1 and 2, the focus of this discourse confines itself to an examination of Nigeria — representing the Sub-Saharan region, as an exemplary cultural context. It is critical therefore to underscore the peculiar economic-benefit induced trend of cybercrime in Nigeria - generalisable to other Sub-Saharan nations such as Ghana, which may not represent squarely the hydra-headed nature of cybercrime in Western societies. Although there are multiple variations on how ‘419 fraud’ happens (e.g. Adogame, 2007; Igwe, 2007; Aransiola and Asindemade, 2011; FBI, 2016), monetary benefit is central to the Nigerian 419 fraud as illustrated in Fig. 2 (for fuller accounts on how 419 happens, see the above authors). Although cybercrime is a global phenomenon, in most Western nations, in addition to socioeconomic cybercrime, the term cybercrime represents a range of computer/Internet-mediated crimes under the umbrella of psychosocial and geopolitical cybercrimes – see Tables 1 and 2. Couched within the aim of establishing the particularities of cybercrime in Nigeria is a wider critique of prevailing taxonomies of cybercrime. Nigerian cybercriminals to date, have been consistently implicated in money-oriented rather than psychosocial and geopolitical cybercrimes. In fact, the convergence of emerging evidence reinforces that perpetrators of cybercrimes in Nigeria focus exclusively on cyber-fraud (Ojedokun and Eraye, 2012; Smith, 2008; Tade and Aliyu, 2011; Adogame, 2007; Doyon-Martin, 2015; Chawki et al., 2015b; Akpome, 2015; Ellis, 2016; Ibrahim, 2016). Arguably, the Nigerian 419 fraud invention and revolutionised by Nigerian kingspins such as Fred Ajudua (Longe et al., 2010) is rooted in socioeconomics.

Given the foregoing remarks, cybercrime in Nigeria can be conceptualised simply as the use of computer/Internet to commit fraud. According to the yardstick of the binary model, the use of computer/Internet to commit fraud falls under the scaffolding of cyber-enabled crime (see Fig. 1). Unlike ICCCs (2010) survey, which concentrated mainly on a range of cyber-enabled crimes as shown in Table 3, some recent enquiries which focused exclusively on cyber-dependent crimes could not locate Nigeria at the upper part of the cybercrime perpetrators’ hierarchy (e.g. Kaspersky, 2016). This comparison between these observations support the notion that Nigerian cybercriminals are more implicated in cyber-enabled than cyber-dependent (or techno-centric cybercrime) listed in Fig. 1. Does this not suggest problems with prevailing taxonomies of cybercrime?

If we look at the Nigerian case through the lens of the binary model (see Fig. 1), the problem is that we would be led to conclude that cybercrime in Nigeria is just cyber-enabled. Cybercrime in Nigeria is fundamentally rooted in socioeconomics, whereas the cyber-enabled crime framework encompasses a range of other crimes such cyber-bullying and cyber rape. This is problematic. In terms of cyber-bullying and cyber rape, the perpetrators’ gains and the victims’ losses, as illustrated in Table 2, are primarily psychosocial unlike cyber-fraud (which is primarily rooted in economic gains/losses). It suggests problems with

419 is coined from section 419 of the Nigerian criminal code (part of Chapter 38: Obtaining Property by false pretences; Cheating) dealing with fraud. Nowadays, the axiom ‘419’ generally refers to a complex list of offences which in ordinary parlance are related to stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts” (Chawki et al., 2015b, pp.129).

5 Nigeria and Ghana are Anglophone Sub-Saharan nations separated and surrounded by Francophone nations. Despite multiple ethnic variations within and across these two countries, they have similarities: British colonisation, English language, relatively, similar time of independence’ (Ibrahim, 2015, p. 312).

6 Cyber-enabled crime and people-centric cybercrime will henceforth be interchangeably used.
the binary model because these other crimes under the umbrella of psychosocial cybercrime may not be primarily rooted in economic gains/loss (as illustrated in Table 2). In other words, whilst socioeconomic cybercrime constitutes only a subcategory of cyber-enabled crime, a cyber-enabled conceptual framework comprises a range of crimes other than cyber-fraud. Therefore, clearly, the existing binary categories discussed above are ill equipped to differentiate between psychosocial, socioeconomic and geopolitical cybercrime. The crux is that the evidence that support the centrality of socioeconomic cybercrime in Nigeria, concomitantly suggest problems with the dual model of cybercrime. These illustrations highlight the usefulness or utility of the TCF, which is more robust than the prevailing taxonomies in dealing with the complexities of numerous varieties of cybercrime.

6. Internet crime complaint centre: the critique of evidence

Having offered a theoretical critique of the prevailing models of cybercrime, this article will render problematic the basis for ICCC’s (2006–2010) claim on ‘cybercrime perpetrators’ league table’, i.e., Nigeria being the third worst nation in the world. The FBI in partnership with the National White Collar Crime Center, aiming to reduce the volume of economic loss by

---

**Table 3**

<table>
<thead>
<tr>
<th>Type</th>
<th>Percentage</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Non-delivery Merchandise</td>
<td>21.1%</td>
<td>Purchaser did not receive items purchased, or seller did not receive payment for items</td>
</tr>
<tr>
<td>2. FBI-Related Scams</td>
<td>16.6%</td>
<td>Scams in which a criminal poses as the FBI to defraud victims</td>
</tr>
<tr>
<td>3. Identity Theft</td>
<td>10.1%</td>
<td>Unauthorised use of victim’s personally identifying information to commit fraud</td>
</tr>
<tr>
<td>4. Computer Crimes</td>
<td>9.3%</td>
<td>1) Crimes that target computer networks or devices directly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) Crimes facilitated by computer networks or devices</td>
</tr>
<tr>
<td>5. Miscellaneous Fraud</td>
<td>7.7%</td>
<td>Variety of scams meant to defraud the public such as work-at-home scams and fraudulent contests</td>
</tr>
<tr>
<td>6. Advance Fee Fraud</td>
<td>6.1%</td>
<td>Criminals convince victims to pay a fee to receive something of value, but do not deliver anything of value to the victim</td>
</tr>
<tr>
<td>7. Spam</td>
<td>4.1%</td>
<td>Mass-produced, unsolicited bulk messages</td>
</tr>
<tr>
<td>8. Auction</td>
<td>4.0%</td>
<td>Fraudulent transactions that occur in the context of an online auction</td>
</tr>
<tr>
<td>9. Credit Card Fraud</td>
<td>3.6%</td>
<td>Fraudulent, unauthorised charging of goods and services to a victim’s credit card</td>
</tr>
<tr>
<td>10. Overpayment Fraud</td>
<td>3.4%</td>
<td>An incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and send the deposited money back to the sender</td>
</tr>
</tbody>
</table>

---

It is noteworthy that unlike ICCC’s (2006–2010), ICCC (2011–2014) reports exclude the perpetrators’ league table.
Internet crime, established the Internet Crime Complaint Centre (ICCC or IC3) in May 2000. As its name implies, the ICCC is a center to receive victims’ complaints concerning ‘cybercrime’ and over the past years, the ICCC received about 300,000 responses annually (ICCC, 2008; ICCC, 2009; ICCC, 2010; ICCC, 2011; ICCC, 2012; ICCC, 2013; ICCC, 2014; FBI, 2015). These data appear to be robust because they come directly from the people who experience the offence. However, the accuracy of responses were only self-reportedly measured, which highlights the ICCC’s over-reliance on participants’ honesty and accuracy. Secondly, given that it is only a small percentage of people who voluntarily report themselves as victims of cybercrime (Bohme and Moore, 2012) or crime in general (Reiner, 2010), the generalisability of the populist claim is questionable. In fact, according to the FBI (2014), less than 10% of people report themselves as victims of cybercrime globally. Apart from cybercrime being underreported, the vast bulk of cybercrime as Brenner (2007) and Brenner (2012) pointed out, is undetected. Arguably, even if an average of 300,000 respondents could be seen as a huge sample size in itself, it is far from being representative of the general population of all victims of cybercrime on earth. Additionally, there is the possibility that a majority of responses obtained by the ICCC may represent a selective group. For example, people who perceive themselves as ‘victims’ of the law are unlikely to channel their predicaments to the FBI. Also, Asian and African populations in the ICCC’s global research were not significantly represented in comparison to North American and European populations. As Stevens (2011, p.9) reminded us, “statistics, even when they represent the underlying reality, are socially and selectively constructed, and cannot (or should not) simply speak for themselves”. Therefore, regarding the cases that come to light, even if their statistical basis should be taken at face value, the claim is far from straightforward. A league table therefore is a pictorial representation of that construction, which not only renders invisible the process of construction, but also obscures the entirety of what it represents.

Thirdly, whilst the media and the political discourses tend to amplify the moral panic on the Nigerian 419 fraud (e.g. Adogame, 2007), Akpome (2015), in ‘unsettling the myth of Nigerian exceptionalism’ contended, there is an impossibility of knowing if every cyber-criminal using the Nigerian 419 letter/email templates is actually a Nigerian citizen. It is reasonable also to point out that, there is an impossibility of knowing if some of those perpetrators grouped as ‘Americans’ or ‘British’ are not citizens of other nations. The key point here is that it is challenging to isolate cybercriminals from other nations and world regions who may have as Adogame (2007, p.7) pointed out, ‘masked themselves as Nigerians and entered the theatre of 419 fraud as actors’. One of the implications is that, as Reiner (2010) noted, most people depend on the media, law enforcement agencies and politicians for ‘authentic’ information on issues such as crime. Regarding the Nigerian case, bearing in mind that some victims may not have accurate information about the actual perpetrators’ identities, suggests that the media and political rhetoric on the ‘Nigerian’ fraud letter/emails may have unintended knock-on-effects on some victims reporting cybercriminals disproportionately as Nigerians. Given that ‘there is a long-standing demonisation of Nigeria in the West as being full of criminals’ (Agozino, 2003, p. 231) reinforces the notion that the ICCC’s league table framed with a loose term ‘cybercrime perpetrators’ may have factored and impacted on some victims’ perceptions.

Lastly, as shown in Table 3, over 90% of crimes covered (2006–2010) were primarily ‘cyber-fraud’ and under this specific category (which this article called socioeconomic cybercrime), Nigeria was found to be the third worst nation. Could the outcome be any different if geopolitical and psychosocial categories were covered? Given the limitations of the binary model, could the effect of the ICCC’s report on various discourses be any different if the exclusion of geopolitical and psychosocial categories were made explicitly? This highlights the usefulness of the tripartite framework as it helps to simplify such league-table-claim into a nuanced umbrella (e.g. socioeconomic cybercrime). Unlike the popular representation of the ICCC’s report in various discourses such as the media (e.g. ‘Nigeria ranked third in the world for cybercrime’ in Balancing Act, 2014), if we should view ICCC’s (2006–2010) reports through the lens of the TCF, we could interpret it differently: ‘cybercrimes are motivated by three possible factors: socioeconomic, psychosocial and geopolitical. As regards to the socioeconomic category, Nigeria was found to rank third in the world’. The term ‘cybercrime’ embodies multiple strands of crimes other than the socioeconomic category.

7. Further justifications for the usefulness of the TCF

In turn, this paper has developed another scope for categorizing cybercrime (TCF), having critiqued the prevailing taxonomies and rendered problematic the statistics relied on to inform the prevalence of cybercrime perpetrators across nations. Accordingly, it will henceforth offer further justifications for the usefulness of the TCF. One of the implications is that if the ICCC’s reports and the likes are framed with TCF, the outcomes could be most precise. Concurrently, both the immediate outcomes and their subsequent knock-on-effects could be different and to a great extent, less ambiguous.

Let us suppose, hypothetically, that river A, B and C have between them the greatest numbers of ‘animals’ (fishes and reptiles) in the world: river A has 4000 fishes, and 2000 reptiles, river B has 2000 fishes and 8000 reptiles, river C has 3000 fishes and 6000 reptiles. If we were required to count the numbers of all the ‘animals’ in them and reported only our findings about fish, without applying the basic categorisation of ‘animals’ already in place, which includes reptiles as well as fish, we could and would be led to say that: ‘regarding animals that live only in water, river A has 2000 more animals than river B and 1000 animals more than river C’. By the same token, river A, river C and river B — in descending order of significance, have the

---

8 For example, the first known exponent of the present day 419 fraud, a former employee of Marine Department of the colonial government of Lagos in 1920 — ‘Professor’ Crentsil, came from Ghana (Ellis, 2016).
greatest numbers of animals that live only in water. We would then be led to conclude that river A has the greatest number of animals in the world when it is only in ‘fish’ category that river A is dominant. River B and river C both have more animals than river A in terms of the other category of animals called ‘reptiles’. In fact, regarding the overall population of animals in these three rivers, in an ascending order of rank, river A, C, and B have the greatest number of animals in the world. This information is made easy because categories map the perceived world structure closely. The TCF could help to showcase data in a clear light by funneling information into nuanced umbrellas.

Beyond abstraction, TCF could be useful in policy-making processes, given that to simplify a complex set of data and maximise information intake with the least mental effort are at the heart of the TCF. The utilitarian value of the TCF could translate into policy-making processes because the instruments of persuasion in policy-making arenas, are often constructed with ‘killer-charts’ rather than elaborate text and analysis. ‘Many policy documents transmitted between policy making civil servants are mostly characterised by bullet points and simple diagrams — they do not grant lengthy analysis of imprecise nature of knowledge’ (Stevens, 2011, p.9). Arguably, bearing in mind the foregoing remarks on the nature of policy-making operational-practice, the TCF could be a useful ‘story telling’ tool in the hands of policy makers. This specific usefulness of the TCF emphasises that a robust taxonomy in cybercrime scholarship is by no means a sign of regress but on the contrary, an indication of progress.

Furthermore, given that everyone who may be interested in cybercrime reports may not be an ‘expert’ in cybercrime, the TCF would provide a simplified tool of making sense of the complexities around the conceptualisation of cybercrime. Simply put, the TCF would have helped to showcase the statistical results of the ICCC’s endeavours (and other cybercrime oriented undertakings) in a clearer light. In turn, it reinforces the elementary principles and the psychological benefits of categorisation (Rosch, 1978), which is central to the TCF. Therefore, the inability to differentiate between socioeconomic, geopolitical and psychosocial cybercrime is not a feature of the binary models alone: it limits the precision and clarity of ICCC’s (2008–2010) reports as well. The crux is that the ICCC’s umbrella term: ‘cybercrime’ or ‘cybercrime perpetrators’ is ambiguous and misleading at best.

It is not only misleading: it has consequences on the emerging academic discourse in Nigeria over the years. Specifically, it has influenced the framing of most scholarly endeavours in Nigeria (e.g. Adomi and Igun, 2008), which echo a sense of ‘moral panic’ on ‘419’ phenomenon. Relatedly, the ICCC’s reports could be implicated in supplying ‘ammunitions’ to ‘Western propaganda machinery, which often blows the Nigerian 419 fraud-news out of proportion’ (Adogame, 2007, p.7). Given that repeating discourses normalise their claim, the problem is deep. Whilst there is a total absence of social/contextual taxonomies in cybercrime scholarship, it is not difficult to notice the presence of ‘league tables’ as well as the binary models discussed above. This mismatch could be implicated in the uncritical representation of ‘Nigeria as the third worst nation’ in cybercrime literature (Aransiola and Asindemade, 2011; Adomi and Igun, 2008). Based on the premise that conceptualising cybercrime is challenging, this article therefore aims to stimulate contemporary scholarly endeavours from Nigeria and elsewhere to look beyond the ‘league tables’ and the binary models and consider contextual/social nuances at play. This is one of the usefulness of the TCF as it has the capacity to enable a clearer conceptualisation of cybercrime in Nigeria and beyond.

Unlike geopolitical and psychosocial categories, socioeconomic cybercrime is prevalent in Nigeria. Bearing in mind that the recognition of the socio-cultural fabric elements of a given situation is at the core of this paper, reinforces its value. The over-reliance on the populist ‘league table’ and the binary models in cybercrime scholarship has led some authors (e.g. Adomi and Igun, 2008; Chawki et al., 2015b) to overlook jurisdictional cultures and nuances. It has possibly misled some people in policy arenas. As Lagazio et al. (2014) observed, the orchestration of the fear of cybercrime in itself stimulates over-spending and psychosocial cybercrime is not a feature of the binary models alone: it limits the precision and clarity of ICCC’s (2006–2010) claim, it is worth considering the background to the Nigerian 419 fraud. ‘Scam’ is an age-old game in all human societies and the Nigerian 419 fraud, like its historical antecedents such as the Spanish Prisoner Swindle (Ogwezzy, 2012; Whitaker, 2013), has emerged from a particular history. Therefore, to dismiss long-term historical perspectives is vulnerable to omit critical factors necessary to understand the social and contextual platforms on which ‘419 fraud’ has emerged. The underlying idea is to further develop the socioeconomic theory of Nigerian cybercriminals — answer to the question, what is cybercrime in Nigeria? Historically, socioeconomic cybercrime in contemporary Nigerian society metamorphised as Igone (2007) narrated, from various types of deceptive ‘games’ played in pre-colonial Nigeria. Like all human societies, the contemporary Nigerian society that has sprouted from the ruins of three ancient West African
kingdoms: Benin kingdom, Bornu empire, and Songhai empire, (Shuter, 2008) has not done away with the relics of scam. Such scam-games of pre-colonial Nigeria are called the ancient relics of scam, as illustrated in Fig. 3 below. These relics of scam may be conceptualised as ancient assemblages of beliefs and practices that have evolved over time and entangled with the contemporary Nigerian democracy and politics, to become a common ‘toolbox’ for money success. Drawing from Robinson and McAdams (2015), in order to communicate this theoretical position beyond abstraction, the relics of scam hypothesis is simplified down to a set of verbal postulates, a box-and-arrow diagram – as illustrated in Fig. 3 below. One of the primary rationales being to enhance our understanding with the least cognitive effort. During the colonial period in Nigeria, whilst some commentators observed that ‘crime’ made little appeal to young Nigerians (e.g. Paterson, 1944), others noticed that Nigerian schoolboys were very gifted in the psychology of manipulations (e.g. US Consulate 1949). It could be that the former were referring to the general population of Nigerian youth, whereas the latter were referring to a specific group of young Nigerians — those who had the opportunity to embrace Western education in the 1940s. Besides, a majority of these reports on schoolboys were generated directly from their head teachers. The key point is that ‘schoolboys’ rather than ‘illiterates’ were principally implicated in authoring various kinds of letters, claiming as Ellis (2016) commented, to be sellers of diamonds, ivory, gold, and other exotic items from ‘Africa’, whereas they were the ‘Wayo trickers’ – fraudsters. However, the ‘destiny’ of ‘Wayo trickers’ changed drastically when petroleum was found in Nigeria (Adogame, 2007).

Petroleum was discovered in Nigeria four years prior to the official end of colonial rule in 1960. Consequently, petroleum became the dominant pillar of the Nigerian economy (Adogame, 2007). In turn, as Saro-wiwa (1989, p.21) commented, most political elites saw the oil-money as ‘a national cake, already baked, ready to be shared’. For them, ruling the nation has nothing to do with nation-building but has everything to do with the funneling of federal money into personal bank accounts. While corruption is a global phenomenon, there is a long-standing view that Nigeria is not one of the ‘cleanest’ nations in the world (Transparency International, 2014). Although the petroleum boom has boosted the magnitude of corrupt practices in Nigeria, it also has some benefits.

As Smith (2008) described, the Nigerian petroleum boom was responsible for boosting the fertility rate as well as increasing the inflow of foreign scholars and workers in the 1970s. Consequently, numbers of educated people in Nigeria increased massively. However, nothing lasts indefinitely, and in the 1980s the price of oil fell drastically, rapidly deflating the Nigerian economy, but not corrupt practices. As oil boom became oil doom, the International Monetary Fund (IMF) entered the equation. To paraphrase Adogame (2007, p.8) ‘IMF by prescribing deregulation exercises, austerity measures as the only panacea to economic reconstruction, ensnared Nigeria into a vicious circle of perpetual money borrowing and interest paying’. The misappropriation of these loans further deteriorated the economy. This was how the IMF, corrupt practices of some politicians and political impunity became hopelessly interwoven with 419 fraud.

Fig. 3. Cultural relics of scam.

---

9 For example, General Sanni Abacha, Nigerian president from 1993 to 1998 corruptly amassed a personal wealth of up to 4 billion USD (Igwe, 2007).
Specifically, Apfer (1999), in his analysis of ‘IBB = 419’, elaborated that, under General Ibrahim Badamasi Babangida (a.k.a. IBB), the longest-serving Nigerian Military regime (1985–1993) supported 419 kingpins and benefited directly from them. IBB’s alleged elevated bribery-corruption scheme, political impunity and a range of kickbacks between other politicians and some foreign companies created real-life ‘scripts’, which added layers of authenticity to early 419 criminals’ schemes. These layers of authenticity made the Nigerian 419 fraud templates invaluable/attractive to swindlers — Nigerians and non-Nigerians. It is easier for swindlers to modify/use the ‘authentic’ templates with track record of success, than to reinvent the wheel of the game. In other words, many of the fraud templates originated from plausible, or even genuine, crime scenarios. Evidently, as Adogame (2007) and Bretton (1962) observed, whilst numerous foreign companies found bribery and falsifying of paper work as keys to benefit from Nigeria, the politicians saw foreigners as a means of acquiring abundant wealth. The marriage between them over the years has produced voluminous ‘419 fraud templates’ and reinforces the idea that cybercrime in Nigeria is rooted in socioeconomics. As a result therefore of a sequence of events that interpenetrate one another to worsen the state of the economy, unemployed graduates, predominantly male, became a part of the equation.

Given the condition of the Nigerian economy in the 1980s, it was not difficult for most unemployed graduates to become vulnerable to 419 scamming (e.g. Adogame, 2007; Smith, 2008). It could be that the petroleum boom in the 1970s provided an elevated aspirational-level for university students. In consequence, higher expectations made the acceptance of unemployment-induced destitution ‘harder’ for recent graduates than for control groups, that is, average unemployed individuals. This echoes the discrepancy theory of satisfaction (Michalos, 1985) in positive psychology, which postulates that upward social comparisons create a discrepancy between expectations and actual life events — upward social comparisons are most likely to stimulate lesser rather than greater satisfaction (see also Cooper and Artz, 1995; Perales and Tomaszewski, 2015).

The ‘gap’ or discrepancy between expectations and actual rewards chiefly determines whether people have low or high levels of satisfaction (Michalos, 1985; Cooper and Artz, 1995). However, this is not to concede that there is a causal relationship between unemployment and offending rates. The links between them despite showing some fairly clear patterns, are far from straightforward (e.g. Newburn, 2016). The most consistent view is that online crimes (as well as terrestrial crimes) in Nigeria are male dominated (e.g. Ojedokun and Eraye, 2012; Aransiola and Asindemade, 2011). This is important because male domination of cyber-fraud in Nigeria is linked to the socioeconomic cybercrime theory of Nigerian cyber-criminals, which, in turn, suggests fundamental problems with the prevailing binary category of cybercrime.

9. Socio-fabric elements and cultural landscapes

The explanations as to why adult males in Nigeria have been implicated in the bulk of socioeconomic cybercrime demands the application of cultural insights. The rationale being that there is an intersectionality of issues of interpersonal relationships in physical spaces and cyberspace. Cultural constellations of people in social contexts affect people’s activities in cyberspace. The centrality of socioeconomic cybercrime in Nigeria is linked to the centrality of the patriarchal system. As Ibrahim (2015) pointed out, the strong patriarchal system and customary ‘common-sense’ in Nigeria among other factors, encourage men culturally, unlike women, to be the breadwinners. Due to men’s cultural positionality in society in relation to women, men are generally more ‘desperate’ to achieve financial success. Indeed, contemporary scholars articulate that some cyber-criminals in the Sub-Saharan region go as far as deploying mystical/spiritual powers to enhance their exploits online (e.g. Tade, 2013 in Nigeria; Armstrong, 2011 in Ghana). The key point here is that regarding cybercrime, the primary aims of most Nigerian cyber-criminals converge on defrauding as many victims as possible (Smith, 2008; Akpome, 2015), which is illustrative of socioeconomic cybercrime, rather than for example, psychosocial cybercrime (please see Table 2 for victim-perpetrator primary and secondary loss/benefits).

One of the considerations that shape this trend is the local philosophy and demonstrable reality that, if a man is financially successful, he has ‘unlimited’ privileges in multiple facets of life-domains, unlike in Western society. For example, a man who has the means, regardless of his age, under customary and Islamic marriages can marry multiple wives. He can even marry wives as young as fourteen or thirteen years old, in some cases, depending on his ‘tastes’ (Nigerian Marriage Act, 1990; Ogunde, 2016; Monk et al. in press). Apart from the Nigerian common-sense custom allowing polygamy, a man’s adultery is socio-culturally perceived as ‘a heroic feat’ (Chiwuba, 2015, p.305). These types of relationships shapes the manner in which a given society perceives its adult females at a particular historical point in time and how women are expected to relate to adult males (Ajayi and Owumi, 2013; Ibrahim, 2015; Chiwuba, 2015; Ogunde, 2016). It also extends to future generations and impacts on the children – the image-of-childhood in the Sub-Saharan region (Rwezaura, 1998; Ibrahim and Komulainen, 2016). A strong patriarchal system helps to perpetuate these types of cultural landscapes, which in turn shape the socioeconomic crime in Nigeria. Unlike in some Western nations, the cultural landscapes inherent in Nigeria invoke relatively positive societal reactions, towards any man who has financial success (irrespective of the source of such a success – e.g. cyber-fraud) (see also Becker, 1967 on social reactions). Such background evidence reinforces that the Nigerian cyber-criminals are primarily monetary-driven as illustrated in Table 2. Therefore, the Nigerian cybercriminals (popularly ranked third)
are under one nuanced umbrella of cybercrime — cyber-fraud (socioeconomic cybercrime), which is not made clear through the lens of the binary model as well as ICCC’s (2008–2010) observations.

The above social and contextual factors informed the core of present day cybercrime in Nigeria. Arguably, these forms of cultural landscapes are possibly the explanations for the centrality of socioeconomic cybercrime in Nigeria, which suggests problems with the existing binary model of cybercrime as aforementioned. The implication is that what is cybercrime in Britain or in the USA - ranked second and first respectively, (ICCC, 2010) does not fit squarely within the contextual meaning of cybercrime in Nigeria. For instance, unlike the Sub-Saharan region, as Sheridan et al. (2014) pointed out, in most Western nations, cyber stalking is a social problem. Another implication is that these social and contextual factors also challenge the simplistic rendering of cyberspace and physical space as two different entities with easily defined boundaries as they are intertwined, as shown in Fig. 3. Evidently, the particularities of cybercrime in Nigeria support the incorporation of social and contextual factors into cybercrime classifications and consequently, render problematic the existing taxonomies.

10. Conclusion

This article has aimed to establish the particularities of cybercrime in Nigeria and whether these suggest problems with prevailing taxonomies of cybercrime. It has examined the explanatory capacity of the existing taxonomies in making sense of what is true of all societies, and what is true of one society at one point in time and space. Thus, these analyses have helped to propose that whilst in Nigeria, cybercrime is fundamentally rooted in socioeconomics, the lenses of the existing cybercrime taxonomies are not well equipped to project the pattern of this phenomenon clearly. Therefore, in line with motivational theories framed within the basic psychological framework of categorisation, this paper has not only complemented the existing taxonomies, but has also offered a more conceptually robust alternative for grouping cybercrime: the TCF. It has argued that cybercrime can be motivated three possible ways: socioeconomic, psychosocial and geopolitical. Whilst what constitutes cybercrime in most Western nations such the UK and the USA may involve these three groups, cybercrime in Nigeria is fundamentally rooted in socioeconomics. Therefore, the conceptual ‘pipelines’ of the cybercrime framework in the Global North may not hold water in Nigeria — representing the Sub-Saharan region. Drawing together and extending categories of cybercrime, this article has provided a more holistic taxonomy incorporating socioeconomic, psychosocial and geopolitical motivations. This contribution offers new ways of making sense of numerous variances of cybercrime listed in Table 1. It also provides a clearer way of conceptualising cybercrime in Nigeria and elsewhere because jurisdictional cultures and nuances apply online as they do offline.

Acknowledgment

I am grateful to Professor Robert Reiner and Dr Jessica Morgan for their comments on my draft, and I also thank the anonymous reviewers for their insightful and thoughtful comments. I thank my friends, Nicola Baldwin, Shervin Venccatchellum, Andreas Haggman and Stephen Wyatt, for proofreading different parts of my draft and Dr Laura Christie for proofreading the final version of this article as a whole. I am grateful to the journal’s production manager (Sheha Mohan) for her patience. I also thank the organisers and participants of the 4th International Conference on Cybercrime & Computer Forensics – Vancouver, where I presented this paper in June 2016 (at Simon Fraser University). My sincere gratitude goes to my mentor, Professor Ravinder Barn, for her comments when I was working under her (The CyberRoad Map Project from 2014 to 2015); a fragment of this paper was my unpublished contribution to the Project. I also thank the EPSRC and the UK government as part of the Center for Doctoral Training in Cyber Security at Royal Holloway, University of London.

References

FBI, 2016. Internet Crime Schemes. available at:https://www.ic3.gov/crimeschemes.aspx#item-13 (accessed 27.05.16.).
FBI, 2016. Internet Crime Schemes. available at: https://www.ic3.gov/crimeschemes.aspx#item-13 (accessed 27.05.16.).