Cybercrime in Commonwealth West Africa and the Regional Cyber-Criminogenic Framework

Prof. Tim Hall, Department of Policing, Criminology and Forensics, University of Winchester

Dr Ulrike Ziemer, Department of Social Sciences, University of Winchester.

Abstract

Cybercrime can, in theory, be carried out from anywhere in the world connected to the internet. Despite this, cybercrime displays markedly uneven patterns of perpetration across space. There is a nascent, multidisciplinary literature that has begun to engage with the questions of cybercrime's spatialities. This literature, at its heart, sees cybercrime as the product of the spatial co-presence of certain cyber-criminogenic combinations of conditions that occur unevenly across space. It advances versions of what we might call, 'a regional cyber-criminogenic thesis'. However, this literature remains relatively sparse, and its diversity has precluded any sustained cross-disciplinary dialogue from emerging. There is, for example, some discord within this literature around which combinations of conditions it identifies as potentially cyber-criminogenic, but, to date, no substantive cross-disciplinary scrutiny of these differences has emerged. This paper attempts to address this by articulating a regional cyber-criminogenic framework, accommodating perspectives from across this literature, which identifies eight potentially cyber-criminogenic conditions. The paper specifically considers the relevance of the regional cyber-criminogenic framework to Commonwealth nations. It includes an overview of cybercrime and the Commonwealth and then applies the framework to Ghana and Nigeria specifically, to examine the conditions that facilitate the development of cybercrime there. The paper also briefly considers the application of this framework to Commonwealth anti-cybercrime policy.

Keywords: cybercrime, regional, socio-economic, cyber-criminogenic, conditions, framework

Introduction

Cybercrimes, of all kinds, are in theory placeless. They can be carried out from anywhere in the world with a connection to the internet. However, despite this, they display distinctive spatialities, characterised by markedly uneven patterns of perpetration across space. The literature, for example, identifies Eastern European and West African nations from which extensive economically motivated cyber frauds – such as advance-fee fraud and phishing – disproportionately originate, including the Commonwealth nations of Ghana and Nigeria (Ibrahim 2016a; 2016b; Kshetri 2013a; Lusthaus and Varese 2021). Elsewhere, the literature has associated extensive geopolitically motivated hacking with nations such as Russia and China, among others (Kshetri 2013a: 56; 2013b). It has also begun to recognise neighbourhood-level clusters of active cybercriminals in districts such as Ostroveni in the Romanian city of Râmnicu Vâlcea (Lusthaus and Varese 2021: 9) and Bijlmer in Amsterdam (Leukfeldt 2014; Loggen and Leukfeldt 2022). There are, of course, other spatialities of cybercrime, including those of victimisation (Halder 2021; Holt et al. 2018; Martellozzo and Jane 2017), policing, legislation and regulation (Gillespie 2019; Wall and Williams 2014), of the technical infrastructures that both sustain and defend against illegal online activities, and of awareness, education, and fear of cybercrime (Austin 2021; Cook et al. 2022). While these are equally deserving of critical scrutiny, this paper focuses specifically on the spatialities of cybercrime perpetration.

Acknowledging the spatialities of cybercrime perpetration (hereafter referred to simply as 'cybercrime') opens up the physical spaces within which cybercriminals are located, as well as the virtual spaces through which they operate, as legitimate sites of analysis (Lusthaus and Varese 2021). It raises empirical, theoretical and applied questions, namely:

- What are the specific spatialities of cybercrime?
- What regional, contextual conditions influence patterns of cybercrime offending?
- How might we mobilise these knowledges within anti-cybercrime policy and practice?

There is a nascent, multidisciplinary literature, spanning anthropology, criminology, sociology and investigative journalism; international relations and political economy; and statistics that has begun to engage with these questions. Despite their different disciplinary positions, these literatures, at their heart, all see cybercrime as the product of the spatial co-presence of certain cyber-criminogenic combinations of conditions that occur unevenly across space. They advance versions, then, of what we might call, 'a regional cyber-criminogenic thesis'. While this work has significantly advanced our understanding of the regional contexts from which cybercrime originates, we can recognise some limitations. Despite its recent growth, this literature remains relatively sparse (Perkins et al. 2022: 197), and its diversity has precluded any sustained cross-disciplinary dialogue

from emerging. There is, for example, some discord between these literatures around which combinations of conditions they identify as potentially cyber-criminogenic, but to date no substantive cross-disciplinary scrutiny of, or reflection upon, these inter-disciplinary differences has emerged. There has only been one attempt to transcend these disciplinary positions and identify all potentially cyber-criminogenic conditions collectively articulated across this multidisciplinary literature (Hall et al. 2021) and we feel these findings demand some refinement. Therefore, despite only a limited history, this literature appears to be at something of an impasse with few spaces of cross-disciplinary contact evident.

This paper aims to exceed the rigidly disciplinary positions that have largely characterised work in this area to date, by articulating a regional cyber-criminogenic framework that accommodates perspectives from across the disciplinary span of this literature and which captures the full range of potentially cyber-criminogenic conditions it identifies. In doing so, it will critically examine the empirical foundations upon which the conditions included within this regional cyber-criminogenic framework rest, identifying areas where further research is needed. It will use this to articulate a space from which more cross-disciplinary, dialogic research agendas might emerge.

The paper specifically considers the relevance of this framework to Commonwealth nations and particularly those of West Africa. It includes an overview of cybercrime and the Commonwealth, exploring the implication of Commonwealth nations within the geographies of cybercrime perpetration and victimisation. It also explores the conditions that facilitate cybercrime originating in the West African Commonwealth nations of Ghana and Nigeria. The paper further considers the application of this framework in anti-cybercrime policy. Here, the paper draws upon lessons from successful information technology (IT) development in Rwanda, to suggest a policy direction that might contribute to mitigating the interaction of potentially cyber-criminogenic factors in Commonwealth countries such as Nigeria and Ghana with high incidents of cybercriminal activities.

Cybercrime

Cybercrime is a term that has been applied to a wide range of online crimes as diverse as fraud, blackmail, child pornography, revenge pornography, digital counterfeiting, cyber espionage and cyber terrorism. This empirical diversity ensures the term has little analytical currency and it is typical for research to focus on specific forms of cybercrime, rather than cybercrime generally. The literature is replete with attempts to define and classify cybercrime in various ways. These will not be rehearsed here but discussions of them are readily available (Neal 2010; Wall 2007; Yar 2019; Yar and Steinmetz 2019). In this paper, we draw on Ibrahim's (2016a) proposal for a tripartite taxonomy

based on cybercriminals' motivations. This recognises socio-economic, psychosocial and geopolitical motivations (Table 1).

Table 1. Tripartite cybercrime framework

Socio-economic cybercrime	Psychosocial cybercrime	Geopolitical cybercrime
*Hackers and crackers	*Hackers and crackers	*Hackers – 'Hacktivist'
Cyber fraud	Child pornography	Cyber spies
Cyber embezzlement	Cyberstalking	Cyber espionage
Cyber piracy	Cyberbullying	**Cyber terrorism
Cyber blackmail	Revenge porn	Cyber vandalism
Romance scam	Cyber rape	Cyber assault
Online drug trafficking	*Cyber hate speech	*Cyber hate speech
*Cyber prostitution	*Cyber extortion	Cyber riot
*Cyber extortion	Obscenity	Cyber sabotage
Illegal online gambling	*Cyber prostitution	Cyber colonialism
*Cyber trespass	*Cyber trespass	Cyber rebellion
**Cyber terrorism	Cyber homicide	
	**Cyber terrorism	

Source: From Ibrahim 2016a, 45

Notes: *where the type of cybercrime appears in more than one column; **where the type of cybercrime appears in more than two columns.

This taxonomy is not without its limitations. Its categories remain broad in the offences each includes and, as Table 1 demonstrates, some cybercrimes may have multiple motivations. However, it provides a useful heuristic device to frame discussions of the spatialities of cybercrime.

Cybercrime's spatial literatures

We can recognise three distinct research literatures that have explored the spatialities of cybercrime. These are now critically reviewed in turn.

Statistics

Statistical cybercrime literatures typically utilise national-level data, often analysing data for large groups of nations, and attempt to map the geographies of cybercrime at transnational/global scales (Kigerl 2012; 2016a; Lusthaus et al. 2020). They also encompass other aims, however, such as attempts to categorise cybercrime nation types (Kigerl 2016a) and to assess the impacts of

legislation (Kigerl 2016b). These studies typically aim to first identify a dependent variable, a credible measure of the volume of cybercriminals active within nations or of cybercrime originating from different nations. This is not an unproblematic endeavour. Academic researchers are generally sceptical of cybersecurity industry reports (Kigerl 2012: 471; Lusthaus et al. 2020: 451–452) and are equally wary of cybercrime prosecution statistics, as these tend to be more reflective of differences in enforcement capacity and priority than levels of cybercriminal activity (Kigerl 2012: 474; Kshetri 2013a). Rather, data derived from spam archives are commonly used. Here, spam messages are extracted at volume and are geocoded through indicators of their origin, such as language or the originating internet protocol address (Kigerl 2012: 474). However, there are significant limitations inherent in these data sources that reflect the extent to which cybercriminals try to disguise their true locations (Kigerl 2016b: 67). At best, such data offer imperfect proxies of the locations of active cybercriminals and this remains a significant challenge for this literature.

Second, independent variables that may plausibly influence the volume of cybercrime originating from different nations are hypothesised and operationalised. Technological, economic and institutional variables, derived from publicly available global datasets produced by organisations such as the World Economic Forum and the World Bank, are the most widely deployed. This reflects the sparsity of robust national social and cultural datasets at the global scale. Examples of variables utilised include unemployment rate, internet users and participation in international anti-cybercrime legislation (Kigerl 2012) and computing resources, corruption, cybersecurity research and policy, and international relations (Mezzour et al. 2014). Finally, statistical procedures measure the effects of changes in the independent variable(s) on the dependent variable (cybercrime).

Theoretically, this literature draws primarily upon criminological traditions. The most widely deployed theory within this literature is routine activity theory (RAT). Originally developed to interpret volume crimes such as burglary, RAT interprets crime events as the product of the co-presence of motivated offenders and suitable targets, in the absence of capable guardians (Cohen and Felson 1979). It has interpreted cybercrime through motivated offenders (for example, due to a lack of legitimate economic opportunities for young people with IT skills) who operate within regional contexts who lack suitable guardianship (through legislative or institutional weakness or corruption), coming together with suitable targets (such as new or naïve internet uses) in online settings where technical defences are insufficient or can be easily circumvented (Holt et al. 2018; Kigerl 2012; Maimon et al. 2015; see also Leukfeldt and Yar 2016 for a wider review of the application of RAT to cybercrime).

This literature suggests that the most significant predictors of cybercrime activity within nations are gross domestic product (GDP) and internet users per capita. High-cybercrime nations, according to this literature, tend to be characterised by IT-literate populations, as suggested by higher rates of internet users per capita, in regional contexts where they are faced with limited opportunities to deploy their skills within the legitimate economy, as suggested by lower levels of GDP or high rates of unemployment (Kigerl 2012: 482). They tend to be associated with lower GDP only up to a point, however. Nations with very low levels of GDP tend to also be low-cybercrime nations, a reflection of their relative lack of technical infrastructure and IT literacy (Kigerl 2016a: 162). The significance of the interaction between poverty/a lack of economic opportunity and IT literacy has also been observed across other cybercrime literatures (Doyon-Martin 2015; Glenny 2008, 2011; Ibrahim 2016a, 2016b; Kshetri 2010; Lusthaus and Varese 2021). Other factors, such as high levels of corruption, have also been cited as additional predictors of cybercrime in some contexts (Mezzour et al. 2014).

International relations/political economy

A nascent international relations/political economy literature, of which Kshetri is the key author, offers broad surveys of cybercrime at the national and transnational scales, typically for nations widely perceived as major cybercrime threat nations such as China, Russia and Ukraine (Kshetri 2013a; 2013b) or for large groups of nations, such as the developing world (Kshetri 2010). It explores issues such as the nature of cybercrime within different nations and regions, comparative discussions of cybercrime, the ways in which cybercrime and cybersecurity increasingly shape the relations between nations, and national and regional responses to cybercrime (Kshetri 2010; 2013a; 2013b). It also commonly discusses the contextual conditions that underpin the development of cybercrime within different regions.

Table 2 summarises cyber-criminogenic conditions identified across Kshetri's analyses of cybercrime in China, the developing world, and the Former Soviet Union and Central and Eastern Europe (2009; 2010; 2013a; 2013b). These have been categorised using headings derived from RAT with the addition of one further category, 'facilitating context', to describe those conditions that contribute to cybercrime activities but do not fit into previously identified RAT categories. Although RAT is not a theory present within the international relations/political economy cybercrime literature, it provides a useful categorising device here. It is worth noting that some of the conditions below could, arguably, be allocated to more than one category or to alternative categories. 'High levels of corruption', for example, have been noted as a motivating factor within West African cybercrime (Adeniran 2011; Burrell 2008; Ibrahim 2016b; Tade 2013; Tade and Ibrahim 2011; Warner 2011).

Table 2. Cyber-criminogenic conditions identified within the international relations/political economy literature

Offender motivations

- Cybercriminals' confidence, a reflection of the low likelihood of being caught.
- Lack of legitimate economic opportunities, which generate economic motivations for cybercrime, especially for young people with IT skills.
- Wider social legitimacy and a lack of stigma associated with cybercrimes; 'hacking cultures'.
- Strongly nationalist political and cultural environments that encourage external victimisation and cyber wars.

Absence of capable guardians

- Permissive regulatory regimes.
- Limited capacity to fight cybercrime.
- Institutional weakness.
- High levels of corruption.
- Varying degrees of integration with the West in the realm of cybersecurity.
- Path-dependent externalities associated with cybercrime.
- Limited defences against cybercrime.

Suitable targets

- Widespread use of cheap, crime-prone hardware and software.
- Naïve, novice internet users with little awareness of cybersecurity products and practices.
- Presence of some highly digitised industries, such as China's online gaming industry, providing lucrative targets for cybercriminals.

Facilitating context

- Growing broadband connectivity.
- Presence of organised criminal groups involved in online, as well as offline, crime.

Source: Based on Kshetri 2009; 2010; 2013a; 2013b; Cohen and Felson 1979

A major contribution of this literature is that it recognises potentially cyber-criminogenic cultural and political conditions, beyond those predominantly technological, economic and institutional conditions identified within the statistical literature above. Specifically, it talks about the social legitimacy that cybercrime apparently enjoys in some regional contexts, including Eastern Europe, China and the global South, and the potential influence of strongly nationalist political contexts on cybercrime activity (Kshetri 2009: 143–144; 2013b: 52–53, 59). Of the former, with reference to China, Kshetri (2013b: 59) argues:

> *Recent studies and surveys have highlighted differences in culture associated with hacking in China and the West. For instance, many types of 'hackers' are considered to be socially undesirable in the West. The terms such as 'hacker' and 'hacking', on the other hand, seem to have somewhat more positive and less negative attitudes than they have acquired in the West.*

This literature also highlights the presence of stocks of suitable, domestic, targets in high-cybercrime nations, something that the statistical literature does not address.

Anthropology/criminology/sociology /investigative journalism

Anthropological, criminological and sociological studies of cybercrime, and accounts produced by the investigative journalist Glenny (2008; 2011), explore the grounded interactions between active cybercriminals within their regional contexts. These studies originate predominantly from two regions, Eastern Europe and the former Soviet Union, and West Africa, although there are some examples from beyond, including studies of cybercrime in Australia (Hutchings 2014), the Netherlands (Leukfeldt 2014), Germany, the UK and the USA (Leukfeldt et al. 2017), Turkey and Brazil (Glenny 2008; 2011). These studies are typically conducted at the micro scale, and employ ethnographic, interview, survey-based and archival methods. We can recognise a broad distinction between those studies that engage largely with official sources, through interviews and ethnographic encounters with law enforcement and criminal justice personnel, or analysis of court documents and police files (Beek 2016; Hutchings 2014; Leukfeldt 2014; Leukfeldt et al. 2017; Warner 2011), and those that engage largely with cybercriminals and/or members of their regional community through survey, interview and occasionally ethnographic methods (Adeniran 2011; Aransiola and Asindemade 2011; Armstrong 2011; Burrell 2008; Ibrahim 2016b; Lusthaus and Varese 2021; Ojedokun and Eraye 2012; Soudijn and Zegers 2012; Tade 2013; Tade and Ibrahim 2011; Voiskounsky et al. 2001). Studies that obtain direct interview testimony from active cybercriminals are relatively rare and are more common within a West African context (Aransiola and Asindemade 2011; Burrell 2008; Tade 2013; Tade and Ibrahim 2011). This reflects the greater accessibility of cybercriminals active within higher education student populations there. It is not uncommon to find studies of Nigerian cybercriminals conducted within universities, for example.

There is overlap with the cyber-criminogenic conditions identified within the statistical and international relations/political economy literatures discussed above and those articulated within these anthropological, criminological and sociological studies. For example, this literature, like the others discussed above, speaks of the presence of high levels of poverty among young people, interacting with technical literacy; political corruption; poor law enforcement capacity; and social

contexts in which cybercrime is legitimised compared to other forms of criminal activity. However, by situating cybercrime within its complex regional cultural and geopolitical histories, this literature further extends recognition of the range of potentially cyber-criminogenic conditions. Specially, it talks of materialistic cultures that value wealth accumulation regardless of its origins (Adeniran 2011; Armstrong 2011; Ayodele et al. 2022; Glenny 2011; Ibrahim 2016a; Tade 2013; Tade and Ibrahim 2011) and regional histories of colonial or corporate exploitation that are deployed within justifications of Western victimisation (Armstrong 2011; Burrell 2008; Tade 2013; Warner 2011).

A regional cyber-criminogenic framework

This section applies the insights from the literature reviewed above into combinations of social, economic, political, technological and institutional conditions that might be regionally cyber-criminogenic. There has been one previous attempt to identify potentially cyber-criminogenic conditions collectively articulated across the multidisciplinary literatures discussed above (Hall et al. 2021). Here, 18 conditions ('factors') (plus four additional factors that were specific to West Africa) were identified. These spanned economic, social/cultural, technological, political, and legal/regulatory and policing factors. While valuable, we can recognise some limitations with this endeavour. First, a framework of 18–22 individual factors provides an unwieldy basis upon which to, for example, operationalise and conduct statistical analysis. Equally, it would be challenging for anthropological, criminological and sociological studies to respond to and accommodate the range of specific factors included within Hall et al.'s (2021) framework. A more refined framework, which retains the range that Hall et al. (2021) capture, while containing fewer categories, would offer a more user-friendly template. There is also some overlap between the factors identified in Hall et al. (2021). The authors, in identifying specific data sources to represent the 18 potentially cyber-criminogenic factors, collapse together two ('traditions of illicitness' and 'normative influence of the illicit within the cultural realm'), as they were too alike to meaningfully distinguish through statistical operationalisation (Hall et al. 2021: 289). There is additional potential overlap between other factors in this framework, such as 'high levels of corruption' and 'state and institutional weakness', for example. A framework consisting of broader categories would help to minimise or eliminate such overlap. In addition, Hall et al. (2021) do not recognise stocks of suitable domestic targets as a potentially cyber-criminogenic factor, despite this featuring in Kshetri's international relations/political economy analysis of cybercrime (2009; 2010; 2013a; 2013b). Recognising the application of RAT to cybercrime, noted earlier, we categorise the factors here through RAT categories, plus one additional category ('facilitating context') (see also Table 2 above).

Table 3. A regional cyber-criminogenic framework

Offender motivations

- An impoverished **legitimate economic context,** where opportunities in this economy do not match the skills levels of young people.
- A materialist **social/cultural context,** in which some forms of illicit wealth accumulation are legitimised.
- A corrupted **political context,** in which illicit wealth accumulation is legitimised.
- An antagonistic **geopolitical context,** in which external victimisation is legitimised.

Absence of capable guardians

- An inadequate **legal/regulatory and policing context,** in which cybercriminals have little chance of being prosecuted and convicted.

Suitable targets

- A vulnerable **socio-technological context** characterised by stocks of suitable domestic targets.

Facilitating context

- A developed **socio-technological context,** in which digital technologies are widely available and extensively used by the population.
- A developed **illicit economic context** characterised by extensive illicit and illegal economic markets and activities.

Source: Based on Hall et al. (2021)

The analysis underpinning this regional cyber-criminogenic framework is an attempt to transcend the rigidly disciplinary positions that have characterised research into the spatialities of cybercrime to date. It identifies a set of potentially cyber-criminogenic factors, based predominantly on analysis of socio-economic cybercrime, which have been collectively articulated across its multidisciplinary literatures. The regional cyber-criminogenic framework does not constitute a universal blueprint from which to read off the regional presence of cybercrime. Rather, it highlights factors that seem to have the potential to be cyber-criminogenic under certain circumstances. We should not, for example, assume that all the factors within the framework need to be present within a nation or region for cybercrime to develop extensively there. Future research, therefore, might focus on which combinations of factors within our framework are cyber-criminogenic, under what circumstances and in what regions. This would build upon suggestions in previous research (Hall et al. 2021: 293) that cyber-criminogenic combinations show some regional contingency.

Studies can confirm the presence of factors from the regional cyber-criminogenic framework within regions with recourse to a variety of forms of evidence. For some factors, for example, those relating to the legitimate economic and the political contexts, robust forms of objective and perception data are available, such as World Bank data on unemployment with advanced education[1] and Transparency International's annual Corruption Perception Index,[2] which are widely used in academic research. Some factors, however, which seem to lend legitimacy to the actions of cybercriminals in some contexts, derive from the sociocultural and geopolitical realms of regions. For these factors, data are more elusive. While we have some international survey data that include measures of the materialist orientations of different nations, for example, including the World Values Survey,[3] this is neither universal in its coverage nor particularly attuned to the question of the social legitimacy of illicit wealth accumulation. For this, we need to seek testimony from members of the regional community of high-cybercrime nations, explicitly exploring the question of the social legitimacy of cybercrime as a form of wealth accumulation within these settings. Further, in attributing causality to potentially cyber-criminogenic factors, the testimony of active or former cybercriminals, for example, in affirming their motivations, is a particularly valuable form of evidence.

Despite the value of the testimony of cybercriminals and members of their regional communities, their presence within cybercrime's literatures is somewhat patchy and uneven. Across all studies reviewed in this paper from all regions, the sum total of active or former cybercriminals who were interviewed, either directly by the authors of these studies or through secondary sources such as published interviews conducted by journalists, was 98. The majority of these were university students in West Africa, predominantly Nigeria, involved in cybercrime. In addition, approximately 1,200–1,400 members of the regional communities of high-cybercrime nations were surveyed within these studies. The empirical foundations of some factors identified within the regional cyber-criminogenic thesis, then, are somewhat restricted, show geographical bias and, in some cases, are now dated. Clearly, there is much that future research could do to generate more extensive testimony from active or former cybercriminals in these regions, and members of their regional communities.

The weight of literature informing this framework is uneven across different types of cybercrime. It primarily draws on literature exploring socio-economic and, to a smaller extent, geopolitical cybercrime. We might suppose that it will speak most directly to the geographies of these types of

[1] https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS
[2] https://www.transparency.org/en/cpi/2021
[3] https://www.worldvaluessurvey.org/wvs.jsp

cybercrime, although this remains, for the moment, subject to empirical validation. No literature exploring psychosocial cybercrime informed the design of this framework; indeed, as noted at the head of this paper, very little literature exists that explores the spatialities of this type of cybercrime. Exploring and interpreting the geographies of psychosocial cybercrime and building an equivalent framework relevant to crimes such as cyberbullying, cyberstalking and revenge porn, therefore, remains an endeavour for the future.

Cybercrime and the Commonwealth

Commonwealth nations are implicated in different ways into the global geographies of socio-economic cybercrime. While some are squarely identified as cybercrime threat nations, from which disproportionate amounts of cybercrime originate, others have been identified as, primarily, target nations, and/or those whose citizens display heightened levels of fear of cybercrime (Cook et al. 2022).

The evidence base currently available with which to sketch out the contours of cybercrime victimisation at the macro scale is somewhat restricted. Academic studies of socio-economic cybercrime victimisation at this scale are rare (Smirnova and Holt 2017). While cybersecurity industry analysis offers a variety of sources that speak to this issue, as noted above, researchers have urged caution in the use of such data (Kigerl 2012: 47; Lusthaus et al. 2020: 451–452). This limited evidence base reflects the challenges of obtaining accurate measures of cybercrime victimisation and the differences in patterns of victimisation associated with different types of socio-economic cybercrime.

Looking at cybersecurity industry sources, there is some consensus around which nations suffer the highest levels of cybercrime victimisation, whether this is measured by the number of victims, risk of encounter or by economic losses attributable to cybercrime (Federal Bureau of Investigation 2021; Lewis 2018; Statista no date). Notwithstanding the limitations of the evidence available, the primary driver of cybercrime victimisation at the macro scale, then, appears to be target suitability. There is some overlap between the nations identified in industry reports and those identified in the limited academic literature of socio-economic cybercrime victimisation at the macro scale. For example, Perkins et al.'s (2022) study of malicious spam distribution confirms the significance of target suitability, here measured in terms of being an Asian nation, GDP, political freedom and corruption. Smirnova and Holt's (2017: 1408) study of national victimisation patterns in stolen financial data markets also highlights the importance of risk minimisation.

While the USA is consistently identified as among the most victimised nations globally, the Commonwealth countries of Australia, Canada, India, New Zealand, South Africa and the UK are regularly identified as high-cybercrime victim nations within cybersecurity industry analysis. These countries all offer perpetrators extensive, digitally connected target populations, who, with the exceptions of India and South Africa, have relatively high GDPs per capita. As Lewis (2018: 7) argues: 'Unsurprisingly, the richer the country, the greater its loss to cybercrime is likely to be'. In addition to the USA, various academic studies identify Australia, Canada and the UK as Commonwealth cybercrime victim nations (Franklin et al. 2007; Holt et al. 2016; Holt and Lampke 2010, in Smirnova and Holt 2017: 1407).

Regarding cybercrime perpetration, Kigerl (2016a) conducted a statistical analysis that attempted to classify nations according to both the volume and type of their socio-economic cybercrime specialisation. Table 4 extracts all Commonwealth nations from this analysis.

Table 4. Commonwealth countries by K-means cluster assignment

Low-cybercrime countries	Advance-fee fraud specialists	Non-serious cybercrime countries	Phishing specialists
Bangladesh	Barbados	Brunei	Antigua and Barbuda
Belize	Ghana	Canada	Australia
Botswana	Jamaica		Bahamas, The
Cameroon	Malaysia		Cyprus
Eswatini	Nigeria		Dominica
Fiji	Samoa		Grenada
Gabon	Vanuatu		Guyana
Gambia, The			Malta
India			New Zealand
Kenya			St Kitts and Nevis
Kiribati			Saint Lucia
Lesotho			St Vincent and the Grenadines
Malawi			Seychelles
Maldives			Singapore
Mauritius			Trinidad and Tobago
Mozambique			United Kingdom
Namibia			
Pakistan			
Papua New Guinea			
Rwanda			
Sierra Leone			
Solomon Islands			
South Africa			
Sri Lanka			
Tanzania			
Togo			
Tonga			

Tuvalu
Uganda
Zambia
Source: From Kigerl 2016a

This analysis suggests that many Commonwealth nations are either low-cybercrime or non-serious cybercrime countries. However, a number are classified as either advance-fee fraud or phishing specialists. Few of the nations identified in either of these two classifications (columns 2 and 4 in Table 4) has generated much attention within the literature of socio-economic cybercrime perpetration. Ghana and Nigeria are notable exceptions, with both the subject of extensive research literatures that have explored many dimensions of the cybercrime originating there. Ghana and Nigeria seem to represent the two apex cybercrime perpetration nations within the Commonwealth. Indeed, one of the most pervasive images of Nigeria within the international imagination is that of its notorious 419 email scams (Zook 2007). Multiple studies cited in the anthropological, criminological and sociological literatures reviewed above have confirmed West Africa as a high-cybercrime region. This association between Commonwealth West Africa and cybercrime undoubtedly causes significant reputational damage, with likely associated material consequences for this region. However, Kigerl's (2016a) analysis suggests that there are other Commonwealth nations that may be enrolled within the geographies of socio-economic cybercrime perpetration and are, therefore, worthy of scrutiny from a more geographically liberated research literature.

Cyber-criminogenic factors in Commonwealth West Africa

The extensive literature examining cybercrime in West Africa confirms the presence of factors from the regional cyber-criminogenic framework within this region. For example, it is common for studies conducted in both Ghana and Nigeria to highlight young people's frustration with their lack of opportunities due to West Africa's impoverished legitimate economic context, alongside a developed socio-technological context, evident through their relatively high levels of education and IT literacy, as motivations for their involvement in illegal online activities (Adeniran 2011; Aransiola and Asindemade 2011; Armstrong 2011; Ayodele et al. 2022; Burrell 2008; Ibrahim 2016a; Tade and Ibrahim 2011; Warner 2011). This issue is particularly acute in Nigeria, where in 2019, World Bank data identified the unemployment rate for Nigerians with advanced education as 17.15 per cent (World Bank 2023), the sixth highest globally. These widely held frustrations were also highlighted in, for example, Burrell's (2008) study of internet café culture in Ghana, which draws on multiple sources, including interview and ethnographic data:

> *It is not accurate to categorize these activities as arising out of a desire to 'gain something for nothing'. Instead, they appear to be informal attempts to realise personal gain by*

> *individuals who perceive legitimate channels of opportunity as being closed to them. This perspective was expressed among young people (not only Internet scammers) such as Stephen, an unemployed 21-year-old, who asserted that in Ghana, 'You can only get a job when you have a relative in that job. He will just link you to the money jobs. But if you don't know anybody there, just forget it, you're not getting any jobs'.* (Burrell, 2008: 20)

Young people's frustrations appear to be compounded by a materialist social/cultural regional context (Adeniran 2011; Armstrong 2011; Ibrahim 2016a; 2016b; Tade 2013; Tade and Ibrahim 2011). Although measuring materialism in the social and cultural realm is challenging, as are cross-cultural comparisons, empirical studies of cybercrime in West Africa frequently identify materialist orientations among young people as a contributory factor in the proliferation of West African cybercrime. Tade (2013: 697), for example, argues: 'The unbridled quest for materialism in Nigerian society has been argued as one of the factors influencing youth to innovate sinister ways of achieving success, without following the laid-down societal approved means'.

Numerous studies also identify a corrupted political context, which is seen to legitimise illicit wealth accumulation among cybercriminals and/or which directly facilitates it (Adeniran 2011; Burrell 2008; Ibrahim 2016b; Tade 2013; Tade and Ibrahim 2011; Warner 2011). These studies tend to identify the perception of illicit wealth generation among officials being deployed as a form of self-justification by those engaged in cybercrime. As one respondent, active in cybercrime, confirmed in Tade's (2013: 698) study, 'The issue of embezzlement is also germane. Monies given out to officials to create infrastructural facilities and even jobs to people are diverted into personal purse. This serves as negative influence on people, particularly the youths'. This view of West Africa as a region characterised by high levels of corruption is reflected in external data. Transparency International's Corruption Perception Index (2021)[4] ranks Ghana and Nigeria as the 73rd and 154th cleanest (least corrupt) nations in the world (out of a global total of 180).

Numerous studies of cybercrime in the region also identify an antagonistic geopolitical context that derives from the region's histories of colonial and corporate exploitation as a causal factor in the high rates of cybercrime originating from there (Armstrong 2011; Burrell 2008; Tade 2013; Warner 2011). This, like the perceptions of official corruption noted above, takes the form of cybercriminals deploying what they perceive as historical injustices as justification of their external victimisation. For example, Warner (2011: 747), argues:

[4] https://www.transparency.org/en/cpi/2021

> *Internationally,* Sakawa[5] *boys justify their duping of Westerners by claiming that it is pointed retribution for centuries of historical injustices perpetrated by the West against Africans. Indeed, the histories of the Trans-Atlantic slave trade, combined with the none too-distant experience of colonialism and a surface-level adherence to the Pan-Africanist ideal of international social justice has combined to form a triumvirate of rationales to excuse the robbery of Westerners via the Internet.*

Or, as a practicing cybercriminal more succinctly put it on an internet forum: '*Sakawa* in Ghana is pay back to the white men and woman…Have we all forget about what they done to as (us)' (Warner 2011: 747).

Several studies have highlighted an inadequate legal, regulatory and policing context to the problem of cybercrime in West Africa (Ayodele et al. 2022; Beek 2016). Beek's (2016: 309–310) study of cybercrime and policing in Ghana, for example, highlighted numerous challenges facing the policing response to cybercrime there. These included the inherent jurisdictional complexity of transnational cybercrime; a lack of specialist policing units, technical expertise and internet access; limited investigation of low-value cyber scams; a reliance on personal networks between the Ghanaian and international police forces for cases to be transferred to Ghana; and an expectation that foreign victims of cybercrime would travel to Ghana to seek justice. All of these suggest that cybercriminals, of the kinds noted in the West African literature, have only limited chances of getting caught and prosecuted for their activities.

The argument that cybercrime enjoys some degree of social legitimacy is also prominent within interpretations of West African cybercrime. Here, for example, it has been argued, based on qualitative interviews with 15 active cybercriminals in Nigeria, that cybercriminals here are viewed as less 'criminally minded' than those engaged in other forms of deviance (Ayodele et al. 2022: 32). Others cite the popularity of West African hip-hop music and films that justify the predatory actions of cybercriminals or paint them in a heroic light, as evidence of the wider legitimacy afforded to cybercrime in West African society (Lazarus 2018; Whitty 2018: 102–103). Studies that cite West African hip-hop music and films as evidence of the wider social legitimacy of cybercrime, however, offer no empirical evidence from members of the regional community to substantiate this claim, either directly within the studies themselves or indirectly through the sources they cite. For example, Whitty (2018) cites a textual analysis of popular *Sakawa* movies by a media studies scholar (Oduro-Frimpong, 2014), rather than any audience research or testimony from West Africans to

[5] *Sakawa* are spiritual practices sometimes used by cyberfraudsters in the belief that they will bring them success.

confirm their consumption of these movies is consistent with a wider world view that regards cybercrime as socially legitimate. Interestingly, rather than offering uncritical portrayals of cybercriminals, the Ghanaian movies that Oduro-Frimpong analyses offer more nuanced portrayals that blend condemnation with acknowledgement of the motivations of cybercriminals. Oduro-Frimpong argues, 'the films, while often acknowledging the role of greed in practitioners of *sakawa*, also foreground social problems such as joblessness and poverty' (2014: 143). Therefore, the social legitimacy of cybercrime is assumed from the popularity of these cultural products, rather than directly demonstrated.

It is worth considering the empirical evidence present in those anthropological, criminological and sociological studies of cybercrime that do survey or include testimony from members of the wider communities of Commonwealth West African high-cybercrime nations regarding the social legitimacy afforded to cybercrime in these contexts. Here, the evidence is somewhat patchy and indirect, as exploring this question is rarely a central aim of these studies. There is actually little evidence of this kind to directly endorse the social legitimacy argument present in studies of cybercrime conducted in West Africa. One respondent to a survey seeking parents' perspectives on Nigerian cybercrime did argue:

> *If a 419 boy [cybercriminal] is arrested, people would be sympathetic to him. They would ask, 'What type of crime has he committed? Is it just because he defrauded someone? Is it bigger than the ones people in government are committing? Why are they treating the small boy [cybercriminal] as if he has done something terrible?'* (Ibrahim 2016b: 6).

However, beyond this, evidence from the studies reviewed here, if anything, questions the validity of the social legitimacy thesis of cybercrime within a West African context. For example, Armstrong's (2011: 7) anthropological study of public discussions of *sakawa* in Ghana suggests that it, and associated cyber scams, are widely perceived in negative terms as un-Ghanaian and un-Christian. It is seen as 'Nigerian', and as a corrupting practice that has entered the country over Ghana's porous border with Nigeria. Further, Burrell's (2008) discussion of the practices and perceptions of internet scamming in Ghana reports examples of social condemnation of scammers by legitimate internet users there. Evidence is presented of concerns for the reputational damage internet scamming causes to Ghana's international image, as well as judgements of scammers as 'greedy or lazy' (2008: 24). She also notes concerns expressed by internet users in Ghana that they might fall victims to scams themselves and reports instances where Ghanaian interviewees had lost money to local (and international) scammers (see also Beek 2016: 317). Finally, Ojedokun and Eraye's (2012) study of the

perceptions of Nigerian cybercriminals suggested they were regarded negatively by fellow students, who saw undergraduates engaged in cybercrime as extravagant and poorly performing academically.

This section, then, has demonstrated that while many of the factors within the regional cyber-criminogenic framework are undoubtedly present in Commonwealth West Africa, some questions remain regarding the claim that cybercrime enjoys widespread social legitimacy within this, and other, high-cybercrime regions. This points to one important avenue of further research.

Applying the regional cyber-criminogenic framework: tackling cybercrime in Commonwealth West Africa

This section considers how the regional cyber-criminogenic framework might inform policy designed to tackle cybercrime. Evidence would suggest that rather than simply the spatial co-presence of the factors identified in the framework, it is the *interactions* between them that are cyber-criminogenic. The interaction of IT literacy and regional poverty, for example, has emerged as particularly significant within statistical analysis of high-cybercrime nations (Kigerl 2012), and has been demonstrated in some settings within more ethnographic studies (Lusthaus and Varese 2021: 4). However, our own analysis suggests that the co-presence of these two factors is not universally cyber-criminogenic (Hall and Ziemer, forthcoming). Our research in the South Caucasus nation of Armenia reveals a country where many of the factors identified in the regional cyber-criminogenic framework are present, but where rates of socio-economic cybercrime perpetration remain low compared to nations with comparable profiles. Our interviews with a range of regional experts revealed that in Armenia, the interaction between IT literacy and regional poverty was mitigated to a large degree by a rapidly growing legitimate IT sector, partly driven by government policy over many years, partly by diaspora, and partly by international investment and relocations. Here, growth in this sector had been sufficient to absorb the pool of young people with IT skills in the country and wages were sufficiently high to deter illegality. This analysis highlights the potential geographical contingency of causality and suggests that cybercrime cannot simply be assumed from the spatial co-presence of certain factors within nations. It also indicates potential avenues of policy development. Therefore, what lessons might this case suggest for policies designed to tackle cybercrime in Commonwealth West Africa?

The Commonwealth East African nation of Rwanda, like Armenia, shares some characteristics identified within the cyber-criminogenic framework. For example, the proportion of the labour force with advanced education who were unemployed in Rwanda stood at 19 per cent in 2020. This was

higher than the figures for both Ghana (4 per cent) and Nigeria (17 per cent).[6] Rwanda also scored and was ranked higher (score 2.8, rank 106) than Ghana (score 2.2, rank 125) and Nigeria (score 2.6, rank 113) on the infrastructure pillar of the World Economic Forum's *The Global Information Technology Report* (2016). This pillar compares electricity production, mobile network coverage, internet bandwidth and secure internet servers per million of the population for all nations. These data suggest potentially powerful cyber-criminogenic interactions in Rwanda.[7] However, despite this, at no point is Rwanda identified within the literature as a high-cybercrime nation. Indeed, Kigerl's (2016a) analysis (see Table 4) identifies Rwanda as a low-cybercrime nation. However, like Armenia, Rwanda has pursued a successful policy of IT development in recent years (World Economic Forum 2022). Also in common with Armenia, this has taken place in the context of potentially cyber-criminogenic interactions in Rwanda. While these IT development policies have not been explicitly designed and promoted as anti-cybercrime measures, they offer another apparent example of IT development in the context of regional poverty and other cyber-criminogenic factors, without any obvious growth in indigenous cybercriminal activity. They also highlight an area that is worthy of further of attention in the context of cybercrime policy innovation, as well as in the context of economic development policy, within which it has primarily been discussed to date. There remains yet little literature on indigenous cybercrime in Rwanda and none that directly explores the relationships between IT development and cybercrime there. Addressing these lacunae in the literature would enhance our knowledge and understanding of cybercrime and the factors that drive its development – both within and beyond Rwanda. The case of IT development in Rwanda, then, offers a model that deserves greater scrutiny, not least for its potential transferability to other regional contexts and possibilities to mitigate cyber-criminogenic interactions.

Conclusions

This paper has shown that our understandings of the macro patterns of cybercrime perpetration and victimisation remain emergent, partial and in some cases, restricted. This is the case both globally and with specific regard to Commonwealth nations. Kigerl's (2016a) analysis (Table 4), for example, revealed several Commonwealth nations that potentially contain extensive cybercrime activity, about which its literatures have said almost nothing to date. There is a clear geographical bias towards the former Soviet Union, Eastern Europe, West Africa and, to an extent, China, in the existing cybercrime research. We would recommend future research range beyond these 'usual

[6] https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS

[7] It should be noted, however, that Transparency International's (2021) *Corruption Perception Index*, records lower levels of corruption in Rwanda (ranked the 52nd 'cleanest' nation included in the index) compared to Ghana (ranked 73rd 'cleanest' nation) and Nigeria (ranked 154th 'cleanest' nation).

suspects' to other regions highlighted as potentially cyber-criminogenic by this, and other, analysis. A more comprehensive analysis of cybercrime within all Commonwealth nations would contribute significantly to our knowledge here. We would also advocate that future research be more interdisciplinary and dialogic. For example, our regional cyber-criminogenic framework might inform the factors included in future statistical analysis of cybercrime. This analysis is valuable in producing maps of potentially high-cybercrime nations through factor correlations. However, determining causation requires more grounded, field-based research. Statistical analysis, therefore, might profitably guide these more grounded, ethnographically informed research endeavours.

There is also scope for future research to engage more critically with the theoretical frameworks that have been deployed within the literatures reviewed here. RAT, for example, has now been quite extensively used to interpret the regional presence of cybercrime. At the same time, the literatures reviewed above have identified the interactions between regional poverty and IT literacy to be particularly cyber-criminogenic. However, in RAT terms this combination alone does not include a factor related to the absence of capable guardians, one of the triad of conditions that RAT argues is necessary for a crime event to occur. This suggests that either this analysis has failed to identify factors related to the regional absence of capable guardians, or, alternatively, that RAT, in being applied to cybercrime, requires some modification. Our analysis also suggests the addition of another factor, 'facilitating context', beyond the original RAT triad. Future research might ask, then, whether factors from all RAT categories are required to be present within cyber-criminogenic regions.

Our analysis has also revealed that the literature has collected only limited direct testimony from active or former cybercriminals, valuable in determining offender motivations, and relatively little testimony from members of their regional communities, valuable in addressing the question of whether cybercrime enjoys social legitimacy within some regional contexts. Although an issue not restricted to the literature of West Africa, more robustly addressing such lacunae in a Commonwealth West African context would offer significant empirical contributions to the cybercrime literature.

The most pressing issue facing Commonwealth nations, revealed by this review of the literatures of cybercrime, is addressing the high rates of socio-economic cybercrime originating in Ghana and Nigeria. As the case of Armenia above shows, potentially cyber-criminogenic combinations of factors may be present within nations, but rates of cybercrime may remain low where there are other factors present, such as Armenia's rapidly growing IT sector, that mitigate their interaction. This suggests that exploring such mitigating factors in different regional contexts might offer new paths

of anti-cybercrime policy innovation. Therefore, a cybercrime policy priority for the Commonwealth to pursue, might be to consider the transferability of policies of IT development, such as those pursued in Rwanda, to a West African context, and to explore their potential to mitigate cyber-criminogenic interactions, particularly between economic poverty and socio-technological literacy, which have been identified in Ghana and Nigeria.

References

Adeniran, A (2011), 'Cafe culture and heresy in Yahooboyism in Nigeria', in K Jaishankar (Ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*, CRC Press, Abingdon, 3–12.

Armstrong, A, (2011), '"Sakawa" Rumours: Occult Internet Fraud and Ghanaian Identity', UCL Anthropology Working Papers Series, Working Paper No. 08/2011, University College London.

Aransiola, JO, and SO Asindemade (2011), 'Understanding cybercrime perpetrators and the strategies they employ in Nigeria', *Cyberpsychology Behavior and Social Networking*, Vol. 14 No. 2, 759–763.

Austin, G (Ed.) (2021), *Cyber Security Education: Principles and Policies*, Routledge, Abingdon.

Ayodele, A, J Kehinde Oyedeji and H Olamide Badmos (2022) 'Social construction of internet fraud as innovation amongst youths in Nigeria', *International Journal of Cybersecurity Intelligence and Cybercrime*, Vol. 5 No. 1, 23–42.

Beek, J (2016), 'Cybercrime, police work and storytelling in West Africa', *Africa*, Vol. 86 No. 2, 305–323.

Burrell, J (2008), 'Problematic empowerment: West African internet scams as strategic misrepresentation', *Information Technology and International Development*, Vol. 4 No. 4, 15–30.

Cohen, LE, and M Felson (1979), 'Social change and crime rate trends: a routine activity approach', *American Sociological Review*, Vol. 44 No. 4, 588–608.

Cook, S, L Giommoni, N Trajtenberg Pareja, M Levi and ML Williams (2022), 'Fear of economic cybercrime across Europe: a multilevel application of routine activity theory', *British Journal of Criminology*, available at: 10.1093/bjc/azac021.

Doyon-Martin, J (2015), 'Cybercrime in West Africa as a result of transboundary e-waste', *Journal of Applied Security Research*, Vol. 10 No. 2, 207–220.

Federal Bureau of Investigation (2021) *Internet Crime Report 2021*, Internet Crime Complaint Centre, Washington, DC.

Franklin, J, V Paxson, A Perrig and S Savage (2007), 'An inquiry into the nature and causes of the wealth of Internet miscreants', in ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, 275–288.

Gillespie, AA (2019), *Cybercrime: Key Issues and Debates*, second edition, Routledge, Abingdon.

Glenny, M (2008), *McMafia: Crime Without Frontiers*, Bodley Head, London.

Glenny, M (2011), *Dark Market: Cyberthieves, Cybercops and You*, Bodley Head, London.

Halder, D (2021), *Cyber Victimology: Decoding Cyber-Crime Victimisation*, Routledge, Abingdon.

Hall, T, B Sanders, M Bah, O King and E Wigley (2021), 'Economic geographies of the illegal: the multiscalar production of cybercrime', *Trends in Organized Crime*, Vol. 24 No. 2, 282–307.

Hall, T and U Ziemer (forthcoming), Exploring the Relationship Between IT Development, Poverty and Cybercrime: An Armenia Case Study, in submission.

Holt, TJ, GW Burruss and AM Bossler (2018), 'Assessing the macro-level correlates of malware infections using a routine activities framework', *International Journal of Offender Therapy and Comparative Criminology*, Vol. 62 No. 6, 1720–1741.

Holt, TJ, and E Lampke (2010), 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies*, Vol. 23 No. 1, 33–50.

Holt, TJ, O Smirnova and YT Chua (2016), 'Exploring and estimating the revenues and profits of participants in stolen data markets', *Deviant Behavior*, Vol. 37 No. 4, 353–367.

Hutchings, A (2014), 'Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission', *Crime Law and Social Change*, Vol. 62 No. 1, 1–20.

Ibrahim, S (2016a), 'Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals', *International Journal of Law, Crime and Justice*, Vol. 47, 44–57.

Ibrahim, S (2016b), 'Causes of socioeconomic cybercrime in Nigeria', *Proceedings of 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, available at: https://ieeexplore.ieee.org/document/7740439

Kigerl, A (2012), 'Routine activity theory and the determinants of high cybercrime countries', *Social Science Computer Review*, Vol. 30 No. 4, 470–486.

Kigerl, A (2016a), 'Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates', *International Journal of Cyber Criminology*, Vol. 10 No. 2, 147–169.

Kigerl, A (2016b), 'Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction?', *Trends in Organized Crime*, Vol. 21 No. 1, 62–78.

Kshetri, N (2009), 'Positive externality, increasing returns and the rise in cybercrimes', *Communications of the ACM*, Vol. 52 No. 12, 141–144.

Kshetri, N (2010), 'Diffusion and effects of cyber-crime in developing economies', *Third World Quarterly*, Vol. 31 No. 7, 1057–1079.

Kshetri, N (2013a), 'Cybercrimes in the former Soviet Union and central and Eastern Europe: current status and key drivers', *Crime, Law and Social Change*, Vol. 60 No. 1, 39–65.

Kshetri, N (2013b), 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research*, Vol. 13 No. 1, 41–69.

Lazarus, S (2018), 'Birds of a feather flock together: the Nigerian cyber fraudsters (yahoo boys) and hip hop artists', *Criminology Crime Justice Law and Society*, Vol. 19 No. 2, 63–81.

Leukfeldt, ER (2014), 'Cybercrime and social ties: phishing in Amsterdam', *Trends in Organized Crime*, Vol. 17 No. 4, 231–249.

Leukfeldt, ER and M Yar (2016), 'Applying routine activity theory to cybercrime: a theoretical and empirical analysis', *Deviant Behaviour*, Vol. 37 No. 3, 263–280.

Leukfeldt, ER, Kleemans, ER and WP Stol (2017), 'Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis', *Crime, Law and Social Change*, Vol. 67 No 1, 39-53.

Lewis, J (2018) *Economic Impact of Cybercrime – No Slowing Down*, CSIS, Santa Clara, CA.

Loggen, J and R Leukfeldt (2022), 'Unravelling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands', *Trends in Organized Crime*, Vol. 25 No. 2, 205–225.

Lusthaus, J, M Bruce and N Phair (2020), 'Mapping the geography of cybercrime: a review of indices of digital offending by country', *IEEE European Symposium on Security and Privacy Workshops (Euro SandPW)*, 448–453.

Lusthaus, J and F Varese (2021), 'Offline and local: the hidden face of cybercrime', *Policing: A Journal of Policy and Practice*, Vol. 15 No. 1, 4–14.

Maimon, D, T Wilson, W Ren and B Berenblum, B (2015), 'On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents', *British Journal of Criminology*, Vol. 55 No. 3, 615–634.

Martellozzo, E and EA Jane (Eds.) (2017), *Cybercrime and Its Victims*, Routledge, Abingdon.

Mezzour, GL, R Carley and KM Carley (2014), *Global Mapping of Cyber Attacks*, Carnegie Mellon University.

Neal, S (2010), 'Cybercrime, transgression and virtual environments', in J Muncie, D Talbot and R Walters (Eds.) *Crime: Local and Global*, Willan, Devon.

Oduro-Frimpong, J (2014), '*Sakawa* rituals and cyberfraud in Ghanaian popular video movies', *African Studies Review*, Vol. 57 No. 2, 131–14.

Ojedokun, UA and MC Eraye (2012), 'Socioeconomic lifestyles of the yahoo boys: a study of perceptions of university students in Nigeria', *International Journal of Cyber Criminology*, Vol. 6 No. 2, 1001–1013.

Perkins, RC, J Howell, CE Dodge, GW Burruss and D Maimon (2022), 'Malicious spam distribution: a routine activities approach', *Deviant Behavior*, Vol. 43 No. 2, 196–212.

Smirnova, O and TJ Holt (2017), 'Examining the geographic distribution of victim nations in stolen data markets', *American Behavioral Scientist*, Vol. 61, No. 11, 1403–1426.

Soudijn, MR and BCHT Zegers (2012), 'Cybercrime and virtual offender convergence settings', *Trends in Organised Crime*, Vol. 15 No. 2–3, 111–129.

Statista (no date) 'Percentage of internet users in selected countries who have ever experienced any cyber crime from November to December 2021', Cyber threat encounter rate by country 2021, Statista, available at: https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/ (accessed 27 September 2022).

Tade, O (2013), 'A spiritual dimension to cybercrime in Nigeria: the "yahoo plus" phenomenon', *Human Affairs*, Vol. 23 No. 4, 689–705.

Tade, O and A Ibrahim (2011), 'Social organization of internet fraud among university undergraduates in Nigeria', *International Journal of Cyber Criminology*, Vol. 5 No. 2, 860–875.

Transparency International (2021) *Corruption Perception Index 2021*, Transparency International, Berlin, available at: https://www.transparency.org/en/cpi/2021 (accessed 24 January 2023).

Voiskounsky, AE, JD Babaeva and OV Smyslova (2000), 'Attitudes towards computer hacking in Russia', in BD Loader and D Thomas (Eds.) *Cybercrime: Security and Surveillance in the Information Age*, Routledge, Abingdon, 56–84.

Wall, D (2007), *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Bristol.

Wall, D and M Williams (Eds.) (2014), *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, Routledge, Abingdon.

Warner, J (2011), 'Understanding cyber-crime in Ghana: a view from below', *International Journal of Cyber Criminology*, Vol. 5 No. 1, 736–749.

Whitty, MT (2018), '419 – it's just a game: pathways to cyber-fraud criminality emanating from West Africa', *International Journal of Cyber Criminology*, Vol. 12 No. 1, 97–114.

World Bank (2023), 'Unemployment with advance education (% of total labour force with advanced education)', World Bank, available at: https://data.worldbank.org/indicator/SL.UEM.ADVN.ZS (accessed 24 January 2023).

World Economic Forum (2016), *The Global Information Technology Report 2016*, World Economic Forum, Geneva.

World Economic Forum (2022), 'Rwanda is tackling digital development challenges – and succeeding', World Economic Forum, available at: https://www.weforum.org/agenda/2022/07/rwanda-is-tackling-digital-development-challenges-and-succeeding/ (accessed 14 September 2022).

Yar, M (2019), 'Transnational governance and cybercrime control: dilemmas, developments and emerging research agendas', in T Hall and V Scalia (Eds.) *A Research Agenda for Global Crime*, Edward Elgar, Cheltenham, 91–106.

Yar, M and KF Steinmetz (2019), *Cybercrime and Society*, third edition, Sage, London.

Zook, MA (2007), 'Your urgent assistance is requested: the intersection of 419 spam and new networks of imagination', *Ethics, Place and Environment,* Vol. 10 No. 1, 65–88.