**Economic Geographies of the Illegal: The Multiscalar Production of Cybercrime**

**Tim Hall**, Faculty of Humanities and Social Sciences, University of Winchester;

**Ben Sanders**, Department of Digital Futures, University of Winchester;

**Mamadou Bah**, Department of Accounting, Finance, Mathematics and Economics, University of Winchester;

**Owen King**, School of Geography, Earth and Environmental Sciences, University of Birmingham;

**Edward Wigley**, Department of Geography, Faculty of Arts and Social Sciences, The Open University.

Contact author: Tim Hall (tim.hall@winchester.ac.uk)

**Economic Geographies of the Illegal: The Multiscalar Production of Cybercrime**

**Abstract**

Economic geographers have traditionally been reluctant to extend their analysis to illicit and illegal markets despite their being significant in their global economic extent and displaying highly uneven geographies. By contrast, the geographies of licit, legal industries have produced multiple traditions of empirically rich, theoretically diverse accounts. Our understandings of the spatialities of illicit and illegal ‘industries’ derive from a different set of intellectual traditions for whom space is a less explicit, central concern. This paper aims to advance our understanding of the geographies of illegal economic activities by exploring the spatialities of one illegal industry, cybercrime (online for-profit fraud), through the lens of economic geography. It considers the spaces within which cybercrime is embedded, exploring it as the product of factors operating at multiple scales. It reviews cybercrime scholarship focused, variously, at the local, national and transnational scales and examines factors salient to the production of cybercrime through case studies at these scales. It examines national level drivers of cybercrime, local cybercrime agglomerations in Europe and transnational asymmetries, connections and opacities and the production of cybercrime. In each case, it reflects upon the potentials for the development of more spatially informed readings of cybercrime specifically, and illegal economic activities more generally, and considers how this might be mobilised to inform anti-cybercrime policy. The paper speaks to both theme I of this special edition ‘the interactions, the norms, the rituals, the behaviours of OCGs in physical spaces’ and theme III ‘the interactions between OCGs and institutions such as the political and economic field’.

**Compliance with ethical standards**

This work does not involve any conflicts of interest.

This work did not involve research with human participants or animals.

This work does not necessitate informed consent.

 “[I]f criminological research into cybercrime focuses on what is happening in the digital world to the detriment of the offline world, a significant part of the organized cybercrime scene will remain undetected” (Leukfeldt, 2014 p. 248).

"Cybersecurity should not just be about the analysis of fast changing technical threats and the challenges they pose. Alongside the online and technical, there is an offline, human and contextual element that matters" (Lusthaus and Varese 2017, p. 1).

**Introduction**

Economic geographers have traditionally been reluctant to extend their analysis to illegal markets (Hall 2013; Hudson 2014; 2019) despite their being significant in their global economic extent and displaying highly uneven geographies (Galeotti 2005; van Dijk, 2007; Hall 2018). By contrast, the geographies of licit, legal industries have produced traditions of empirically rich, theoretically diverse accounts across many industries and regional contexts. Our understandings of illegal ‘industries’ derive largely from a different set of intellectual traditions for whom space is a less explicit, central concern. This paper aims to advance our understanding of the geographies of illegal economic activities by exploring the clustering of one such industry, cybercrime, specifically, online for-profit fraud, through the lens of economic geography. However, this is not to reify the illegal as a discrete economic realm. Rather, we acknowledge a literature that traces the ways in which the legal and illegal, licit and illicit are intertwined within regions and through social, economic and political practices and mobilities (Nordstrom 2007; Wilson 2009; Chiodelli et al., 2017; Hudson 2019).

 The paper starts with the contention, axiomatic within the literatures of economic geography, that economic activities are the result of the interactions of processes operating at multiple scales, something that is as true for illegal economic activities as it is for legal ones (Hudson 2014, p. 780). However, such multi-scalar perspectives are not routinely applied to the scrutiny of illegal economic activities, something this paper seeks to address. It is framed by three questions: what factors contribute to the development of regional agglomerations of cybercrime? What scales do these factors operate at (and across)? And how might this knowledge be mobilised to help tackle cybercrime? It examines them through three case studies, of potentially criminogenic combinations of national attributes, micro-associations within cybercrime hubs in Europe, and transnational asymmetries, connections and opacities in the production of cybercrime in West Africa. Methodologically this paper is built upon an extensive, qualitative meta-synthesis of accounts of cybercrime that explore, in various ways, the regional contexts from which cybercrime emerges. This critically reviews what these accounts tell us, empirically and conceptually, about the spatialities of cybercrime. In addition, it employs a statistical analysis of data relating to national characteristics that have been identified, within the literature, as potentially criminogenic with regard to online for-profit fraud.

**Cybercrime**

Cybercrime is a collective term that covers a number of predatory or disruptive online activities including: economically motivated crimes including fraud (malware, ransomware, online auction fraud and phishing emails, for example), hacking, identity theft and the distribution of illegal pornography and counterfeit digital products, politically motivated cyberterrorism and psychologically motivated crimes such as revenge pornography (Neal 2010; Ibrahim 2016a; Yar 2019). Cybercrime is often a highly geographical phenomenon (Kigerl 2012, p. 471; 2016, p. 147). For example, online for-profit fraud is characterised by extensive regional agglomerations of perpetrators in Brazil (Glenny 2008, p. 314), Turkey (Glenny 2011, p. 192); West Africa (UNODC 2005; Adeniran 2011; Ariansola and Asindemade 2011; Tade and Ibrahim 2011; Agwu 2013; Ibrahim 2016a) and parts of East-Central Europe / former Soviet Union (ECE FSU) (McCombie et al. 2009; Vasylenko 2012; Ilievski and Bernik 2016; Raskovski et al. 2016; Lusthaus and Varese 2017). Some authors also acknowledge the growth and volume of cybercrimes originating in regions beyond its most well documented agglomerations including Western Europe and North America (Glenny 2012, p. 147; Soudijn and Zegers 2012; Broadhurst et al. 2014; Leukfeldt 2014; Wittes et al. 2016). These potentially alternative cybercrime economies have, however, drawn relatively little academic attention in comparison to ECE FSU, West Africa, and more recently China.

Regional cybercrime agglomerations are the origins of significant threats to personal, corporate and national security (Kshetri 2005 p. 542; UNODC 2005, p. 24). For example, the UK's National Crime Agency has recognised Russian-speaking nations as the prime cyber threat to the UK (Dearden 2017), whilst the global (24 countries) annual cost of cybercrime has been estimated at US$ 388 billion (Symantec 2011), although more sceptical assessments are available (Anderson, et al. 2012). The prevailing responses to these threats are technological and legal / regulatory / policing in nature. However, technology offers largely reactive responses (Neal 2010, p. 75), whilst the challenges facing the legislation, regulation and policing of cybercrime are well documented (Aas 2007, p. 164; Broadhurst and Chang 2013; Kshetri 2013; Yar 2019). The distinct spatialities of cybercrime though suggest that within its regional agglomerations these activities are regarded, to some extent at least, as socially licit (Kshetri 2010a, p. 1057). This points to extra-technical and extra-legal responses to the threats of cybercrime; to interventions in the offline regional economic, social, cultural and political contexts from which they emerge (Kigerl 2012, p. 471; Lusthaus and Varese 2017) and to the significance of sophisticated understandings of these contexts.

Despite its distinctive geographies, the spatialities of cybercrime have been, at best, secondary concerns within its own literatures. Cybercrime's literatures are diffuse and multidisciplinary in nature and emerge from three primary disciplinary perspectives: technical / security (Kraemer-Mbula et al. 2013; Berger et al. 2016), policy / legislative / regulatory / policing (Liang and Lu 2010; Broadhust and Chang 2013; Ebobi 2017); and anthropology / criminology / sociology. For all of these literatures, cybercrime's geographies are at best incidental concerns. Equally, cybercrime has failed to emerge as a substantive concern amongst geographers (though see Zook 2007), despite a nascent interest in other aspects of illicit and illegal economies (Hall 2013; 2018; Hudson, 2014; 2019; Chiodelli, et al. 2017) and a tradition of mapping the geographies of cyberspace (Dodge and Kitchin 2001).

The social science literatures of cybercrime have tended to be focused within particular scales of analysis, as opposed to the multi-scalar analytical lens which has increasingly characterised geographical research. Cybercrime literatures, then, have been framed around either local, national or transnational / continental scales. They are broadly characterised by a fissure between low-resolution, surveys of policy and legislation; statistical studies at the national level of distributions of economically-motivated cybercrimes and high-resolution ethnographic studies of cybercriminal subcultures conducted at the micro-scale and focused predominantly within West Africa and ECE FSU. What unites these literatures is their concern with understanding the contexts from which cybercrime emerges. However, their differences have precluded the emergence of any sustained dialogue between them. A further nascent, diffuse literature that considers cybercrime as potentially the product of transnational connections and flows is also apparent. This offers a counterpoint to cybercrime's more regionally grounded literatures although its deployment to date in the analysis of cybercrime is limited.

Cybercrime, since the turn of the century, has frequently been presented, within policy, media and some academic circles, through a narrative of ‘cyber-organized crime’, although this is a rendition that some critical academic studies have contested (Lavorgna, 2020; Lusthaus, 2013). Attempting to situate cybercrime within the wider terrain of organized crime begs two questions. First, to what extent is cybercrime organized? Second, what connections exist between cybercrime and more traditional forms of organized crime? Cybercrime groups demonstrate two forms of organization and governance: through virtual internet based forums in the cases of those groups who are territorially dispersed and through social ties for groups who are more territorially defined and embedded. Whilst non-state hacking tends to be organized and governed through virtual forums, for more territorially defined cyber-fraud gangs, social ties between group members are important (Leukfeldt, 2014; Leukfeldt, 2017a: 45). Whilst social ties and spatial co-presence amongst gang members offer the potential for forms of organization and governance akin to those of traditional organized crime groups, virtual governance through cybercrime forums is generally weaker. Lusthaus (2013: 56) is able to say of the latter “cybercriminal forums are like mafias but they are not mafias”. Further, there is some debate over the extent to which cybercrime is connected to other forms of organized crime (Glenny, 2012: 145). However, Kshetri (2013a: 42) can argue “a significant proportion of them [cybercrimes originating in ECE FSU] are linked with organized crimes, which is clearly demonstrated [by] many large-scale entrepreneurial initiatives”, whilst evidence discussed below, from analysis of police files relating to 40 European and American cybercrime groups, highlights the presence of members active in multiple offline organized criminal markets in gang initiation and management (Leukfeldt, 2014; Leukfeldt et al., 2017a; 2017b). Finally, these dimensions of cybercrime appear to be regionally contingent. The evidence would suggest, for example, that there are greater levels of organization with cybercrime from ECE FSU and more extensive connections to other forms of organized crime than is the case in West Africa (Glenny 2011, pp. 173-174; Kshetri 2013a, p. 42), although we have a dearth of robust data to support these observations (Lusthaus, 2013: 59).

**Questions of Economic Geography**

Whilst contemporary economic geographies offer diverse theoretical, methodological and empirical bodies of enquiry, they are generally unified by a number of concerns. Primarily, they are concerned with the unevenness of economic development, the agents and drivers that underpin this and its effects. A broadly political-economy orientation “recognises the complexity of the economy as constituted by labour processes, processes of material transformation, and processes of value creation and flow in specific space/time contexts” (Hudson, 2005, p. 13). This paper does not offer a summary of this rich tradition of enquiry, excellent examples are readily available elsewhere (see Aoyama et al. 2011). Further, it does not pluck an extant theoretical / analytical model 'off the shelf' and apply it to the analysis of cybercrime. Rather, it starts with the first two of the three questions outlined in the introduction that frame this paper. There are significant literatures, within economic geography and in cognate disciplines beyond, that have explored the processes that underpin the emergence of regional agglomerations of industrial activity. Little, if any of this work, however, has explored regional agglomerations of illegal economic activities (Hudson, 2019). Similarly work that has directly explored illegal economies from within disciplines including criminology, economics and economic sociology have been little concerned with their spatial dimensions (Beckert and Dewey, 2017). This paper aims to reconcile these disciplines’ concerns for illegal economies with the spatial concerns of economic geography.

The questions that frame this paper are derived from preoccupations of scholarship on the geographical unevenness of economic activities that require us to scrutinise processes unfolding at multiple scales and the relationships between them. Here, the local scale includes exploring micro-practices of association that occur within cybercrime gangs and within the neighbourhoods that they appear to cluster within. This includes a concern for the empirics of cybercrime agglomerations at the levels of the neighbourhood, city and city-region. Do then, grounded observations of cybercrime record evidence of agglomerations occurring at broadly these scales and what drives this? This is set within regional and national contexts that appear to offer environments that are potentially criminogenic in their particular mixes of economic, social, political and regulatory characteristics. In terms familiar to economic geographers, this asks what factor inputs, industry specific mixes of land, labour and capital, characterise cybercrime economies within the geographical contexts within which they develop. It considers sets of social, economic, political and environmental conditions and institutional arrangements characteristic of cybercrime agglomerations that shape their opportunities and goals and the constraints cybercriminals must negotiate (Porter 1990; 1998; Allen 2005, p. 17). Finally, the paper also considers the criminogenic potentials of transnational asymmetries, connections and flows associated with cybercrime economies. This mirrors questions within economic geography about the nature and extent of external linkages and extra-local flows of knowledge, and their impacts upon agglomerations of economic activity (Bathelt et al., 2004).

The unevenness of economic development at all scales is considered as both empirical outcome and active constituent within the operation of illegal markets. These are concerns that have, to date, been little applied to cybercrime, either within its own literatures or those of economic geography.

The paper now moves to consider three case studies of cybercrime, each focused at a different scale. In doing so, it seeks to critically evaluate and deploy the insights of cybercrime’s diverse literatures whilst probing further avenues of development.

**‘Rogue Nations’? Criminogenic Combinations of National Attributes**

The prevailing interpretation of macro-distributions of cybercrime has been through a thesis which examines the significance of combinations of key national attributes. Cybercrime here is seen as the result of the interactions between multiple characteristics of places, the combinations of which are uneven across global space. Lusthaus and Varese (2017, p. 1), for example, suggest Romanian cybercrime is the product of the interaction of three factors: the technical legacies of Communism, Romania’s poor economic development and high levels of corruption. Studies in this vein have identified factors that include both those that facilitate cybercrime, such as high levels of computer literacy, as well as 'push' factors such as a lack of legitimate economic opportunities (Aas 2007; Aning 2007; Kshetri 2010a; 2010b; Neal 2010; Warner 2011; Doyon-Martin 2015; Ibrahim 2016a; 2016b). The regional presence, for example, of difficult economic conditions, falling living standards and a lack of legitimate economic opportunities is not sufficient in itself to account for the presence of extensive cybercrime economies. There are plenty of places around the world characterised by harsh economic conditions that do not sustain cybercrime economies. Rather, it is the combination of these conditions and other factors, it is argued, that accounts for the regional agglomeration of profit-oriented cybercrime. This spatial co-presence thesis informs statistical studies (Kshetri 2005; McCombie et al. 2009; Kigerl 2012; Kigerl 2016a; Kigerl 2016b; Holt et al. 2018), some of the more sophisticated journalistic accounts of cybercrime (Glenny 2008; 2011) and is deployed within some of its ethnographic literatures (Lusthaus and Varese 2017). The majority of these studies span the meso- and macro-scales in that the unit of data collection is typically the nation whilst their scope is often global with data analysed for the majority of the world's nations. It argues, then, that cybercrime's macro-geographies reflect identified national differences. We do return in a later section to consider certain ‘pathologies’, such as high levels of corruption, that have become associated with high cybercrime nations, where we argue they may be relationally produced and are not necessarily solely reflective of endogenous failures within these nations.

 Theoretically this literature has drawn primarily upon criminological traditions, a number of studies referencing routine activity theory, for example (Grabosky 2007; Kigerl, 2012; Holt et al. 2018), although occasionally more eclectic theoretical palates are deployed. This is an application of a theory originally developed to interpret volume crimes at the local scale, such as burglary, where motivated offenders and targets are co-present in space and time in the absence of capable guardians (Cohen and Felson 1979). This has been employed here to interpret offender motivation (such as a lack of legitimate economic opportunities commensurate with their skill levels) and a lack of offline guardianship (through institutional weakness or normative influence of criminal actors in the cultural realm, for example). The application of routine activity theory to cybercrime though has drawn some criticism that suggests only limited usefulness, a consequence of “the distinctive spatio-temporal ontologies of virtual and non-virtual environments” (Yar 2005, p. 424).

 Broadly speaking this perspective echoes that of the location factors approach developed within economic geography, although it is deployed at a broader scale of analysis. Here agglomerations of economic activities are interpreted as reflective of the presence of combinations of different location factors within regions. Location factors are inputs into the production process of, in this case, malware or phishing emails, or conditions that facilitate these production processes. In the case of cybercrime, and in terms that economic geographers would recognise, its location factors revealed through this macro-statistical analysis include a motivated and appropriately skilled workforce, an appropriate technical infrastructure and a lax or corrupt institutional environment. However, questions about the limitations of the location factors approach have been aired within economic geography including focusing on only one element of the economic localisation process, issues in attributing causality to factor presence, and difficulties in articulating with potential factors at the extra-regional scale. Equally, these questions would seem to apply to the application of routine activity theory in this case.

The primary contribution of these macro-scale accounts of cybercrime has been to attempt to reveal what might be thought of as pre-conditions for the development of regional cybercrime economies. Namely, it is unlikely that extensive cybercrime economies would emerge within nations that do not display the mix of the types of characteristics outlined above. Collectively, these accounts have identified a range of institutional factors such as low rule of law, limited anti-cybercrime legislation and enforcement capacity (Kshetri 2005, p. 545; 2010a, p. 1057), numerous economic factors, and social / cultural factors, notably contexts within which cybercrime is tolerated or even celebrated, such as those of post-colonial Nigeria (Burrell 2008; Warner 2011; Agwu 2013; Ibrahim 2016a; 2016b), materialistic youth cultures in Turkey (Glenny 2011) and the nationalistic ideologies that have been recognised in externally directed Russian and Chinese cybercrime (Kshetri 2005; 2009; Yip 2010; Broadhust and Chang 2013; Hutchings 2014). Given the difficulties of operationalising social and cultural variables statistically at the national level, institutional and economic variables have been most widely deployed within macro-statistical analysis of cybercrime. Kigerl (2012), for example, used unemployment rate, internet users x unemployment interaction and participation in international anti-cybercrime legislation as predictor variables. Arguably, these studies have tended to utilise a somewhat restricted range of predictor variables. The more ethnographic studies of cybercrime discussed below, the majority of which involved the direct observation of cybercriminals active within their regional milieu, collectively hint at a wider range of potential factors underpinning the development of extensive agglomerations of cyber fraud. There appears to be scope, then, to bring macro-statistical and micro-ethnographic cybercrime literatures more closely into dialogue and to reconsider the range of factors tested within our explanations of the development of agglomerations of cybercrime.

This section offers some pointers on ways in which this approach might be further developed. It seeks to identify an expanded set of potential predictor variables through a qualitative meta-synthesis of 60 published accounts of regional cybercrime economies produced by social scientists, as well as some grey literature from the security analysis sector and some journalistic accounts that have been widely cited within the academic literature. It aims to identify those economic, social, cultural, technological, legal and regulatory, and political factors recorded in these studies as accounting for the development of these observed regional agglomerations of cybercrime. This involved a five stage procedure: systematic scan of the literature; selection of relevant studies; close review of selected studies; identification of regional factors influencing the development of cybercrime; and extraction and classification of factors identified. This follows an inductive approach, seeking to build general understanding of the predictors of cybercrime from specific observations. The aims of this analysis were to identify a potentially expanded range of factors and to specifically identify and operationalise those from beyond the economic and institutional factors that had tended to be employed in studies to date.

 The most developed evidence base within the literature concerns cyber fraud in ECE FSU and West Africa which collectively accounted for the majority of studies analysed here. Analysis of these accounts identified 18 economic; social / cultural; technological; political; legal, regulatory and policing location factors, explanatory characteristics of the milieu of cybercrime (Table 1) that were present in accounts of both main cybercrime regional agglomerations, with an additional four factors that were unique to West Africa.

Table 1: Location factors / factor conditions identified as contributing to the development of cybercrime in FSU ECE and West Africa (for sources see references, all references informing this analysis highlighted with \*).

The next stage of analysis was to attempt to operationalise the factors identified from this meta-synthesis of the literature. A number of criteria guided this effort. It was determined that the variables selected should clearly reflect the factors derived from the literature, be publicly available and universal or near universal in geographical coverage. The variables should also preferably be available for multiple years as it was felt established data sources were likely to be more robust than single year sources. Discussions of the data collection and survey methodology used within the sources drawn upon here can be obtained by accessing the original datasets and accompanying documentation.

From the above process, fifteen variables were identified from a variety of global datasets (see appendix). These related to sixteen variables from table 1 (traditions of illicitness and normative influence of the illicit within the cultural realm were collapsed together). No appropriate variables were identified for those factors that were not operationalised. Inherently studies such as this are open to objections to the operationalised relationships between variables and the concepts they represent. This was acknowledged in this instance by scrutiny of multiple potential data sources for each factor and selection of what was deemed the most appropriate. Variables included in this analysis contained both objective measures of phenomena such as unemployment or educational attainment as well as variables derived from perception studies such as levels of corruption. The inclusion of perception data in such studies has been criticised as potentially compromising objectivity although its use has been defended in the analysis of organised crime (Holmes 2016, p. 32) and it has been widely deployed (see for example, van Dijk 2007).

 The prevailing approach within the statistical analysis of national level distributions of cybercrime is to attempt to identify a credible measure of the volume of cybercrime originating from different countries that can be defined as a dependent variable, to hypothesize independent variables and using appropriate statistical tests, to establish the nature and strength of the relationship between them. This enables researchers to quantify the effects of X changes in the independent variable(s) on Y changes in the dependent one (cybercrime). However, a major challenge this literature faces is finding data on the locations of cyber criminals. Understandably it does not utilise direct observations of cyber criminals in action which are difficult to undertake in practice at the scales at which this literature operates, and to operationalise statistically. It has also largely eschewed data on arrests of cyber criminals as they are poor predictors of national levels of cybercrime activity, due to data collection limitations, restricted policing effectiveness and corruption in some high cybercrime nations (Kigerl 2012, p. 474; Kshetri 2013a). Rather, these studies draw upon publicly available data sources such as spam archives. Extracted spam messages are geocoded using indicators of their origin such as the language used to compile software or the originating internet protocol address (Kigerl 2012, p. 474). Here also though, it is acknowledged, there are significant limitations reflective of the lengths that cyber criminals go to in disguising their location. As Kigerl argues “any information contained in a spam email message that can be geolocated to a given country is not an accurate estimate of where spammers themselves live as spam is almost never sent from a spammer's own home” (2016b, p. 67, see also Kshetri 2005, p 542; Kigerl, 2012, p. 473).

An alternative approach, reflecting these concerns about the accuracy of cybercrime origin data sources, is utilized here. The systematic review of the literature discussed above identified six countries within which extensive cybercriminal activity has been observed for whom complete sets of data for the 15 operationalized factors were available. These are: Brazil, Ghana, Nigeria, Romania, Russia and Turkey. By not including a quantitative measure of cybercrime activity originating from within these countries this analysis does not seek to establish that X change in independent variable(s) produces Y change in cybercrime originating from these countries. Rather, it seeks to establish statistically the characteristics of observed high cybercrime countries across the realms identified in table 1. It asks the question; to what extent do high cybercrime countries share common characteristics that might explain the development of extensive cybercrime economies there?

 To answer the above question, we applied Principal Component Analysis (PCA) as a useful statistical method. PCA involves the normalization of the collected data and the computation of a covariance matrix of the dataset. As there is a large number of interrelated variables in the cybercrime dataset, the next step in PCA is to transform the data into a new set of uncorrelated variables, a set of so-called principal components (eigenvectors). The principal components are ordered sequentially with the first component revealing the highest contribution (eigenvalue) to the total variance in the data; the second principal component is calculated to have the second most variance, etc. Each principal component is a linear combination of the original variables in which the coefficients indicate the relative importance of the variable in the component (Bah et al., 2015). In summary, PCA is a way to redistribute the variance along their maximal direction. It creates a new coordinate system that takes into account these variances.

 In this work, a Matlab script is developed that looks for the most important principal components (eigenvectors), those contributing most (>95%) to the total variance. It looks at the covariance matrix and tries to find the highest covariance between all 15 variables (cybercrime measures). It then constructs a combination of all these variables to create a new candidate that varies the most. This is then kept as PC 1. Then it iterates and tries to find a new combination that is orthogonal to the previous one. That means that if variable 1 is very strong on PC 1, then the algorithm cannot pick it anymore and its weight will be weak on all the following components. The distribution of these coefficients are given in a matrix of eigenvectors **X**. The variance of each of these new components are given in a matrix **Λ** of eigenvalues. The analysis reveal that a total of 5 eigenmodes are needed to achieve 95% of the total variance.

 Using the same approach as in Bah et al. (2015), it was possible to use the PCA model and generate new virtual data for each considered cybercrime measure, using the mean data and a linear combination of the selected principal components. Therefore, a sample of 10000 new values was obtained for each cybercrime factor (table 1). To analyse the new data obtained using PCA, a new correlation matrix was computed (figure 1). The strength of the linear relationship between two cybercrime measures, i.e. the correlation coefficients *r* between pairs of cybercrime measures are presented. This strength increases as *r* moves away from 0 towards -1 or 1. The extreme values of -1 and 1 occur only in the case of a perfect linear relationship. As *r* vary between -1 and 1, the computed value can indicate a negative or positive association. Values of *r* near 0 indicate a very weak linear relationship. The rule of thumb for interpreting *r* is as follows: the relationship is none or very weak, moderate or strong, if │*r*│< 0.3, 0.3 <│*r*│< 0.7 or │*r*│> 0.7. Figure 1 also displays histograms of the variables along the matrix diagonal and scatter plots of variable pairs which appear off diagonal. The slopes of the least-squares reference lines in the scatter plots are equal to the displayed correlation coefficients.

Figure 1: Correlation matrix of the considered dataset. Var1, Var 2,,..,Var 15 refers to the 15 variables in the appendix.

We might draw a number of specific observations from this analysis. First, it shows that there are four variables that are not strongly correlated (│*r*│< 0.7) with any other variables within high cybercrime countries. These are Var 2, economic uncertainty / downturn; Var 3, poverty / lack of opportunities in legitimate economy (particularly affecting young people with IT skills); Var 5, unbalanced economy / revenues inaccessible to the majority; Var 8, normative influence of materialism. These results tell us that their presence within high cybercrime countries seems to vary wildly so we cannot say they are general determinants of cybercrime in combination with other factors, although they may contribute within individual countries. All of these variables could be regarded as characteristics of countries that policy would seek to tackle or reduce. There is some evidence of other variables of this type negatively correlating with some positive economic, social, technological and regulatory factors suggesting a general lack of co-presence of these factors within high cybercrime countries. This does not support the incongruous combination / spatial co-presence thesis that has been deployed within this literature, as a universal explanation for the development of cybercrime extensively within countries. For example, if we look at Var 9 high internet penetration, this negatively correlates with Var 4 blurring of licit and illicit practices (-0.68), suggesting this incongruous combination is only exceptionally co-present.

 Second, we see a number of variables that show some degrees of strong correlation (<│*r*│> 0.7). These are: Var 1, macro-economic stability (measuring recent history of economic transition / liberalisation); Var 4 blurring of licit and illicit economic practices; Var 6, high levels of education; Var 7, IT literacy / skills amongst young people; Var 9, high internet penetration; Var 10, appropriate technical infrastructure; Var 11, (lower levels of) corruption; Var 12, (lower levels of) state and institutional weakness; Var 13, cybersecurity index scores (measuring government indifference or otherwise towards cybercrime); Var 14 political and regulatory environment (measuring internal legal and regulatory shortcomings); Var 15, social capital (measuring low levels of normative influence of gangsterism). All of these, with the exception of Var 4, could be regarded as positive national attributes and it is perhaps not surprising to find them related in these ways. However, Var 4 blurring of licit and illicit economic practices, is strongly negatively correlated to Var 1 and Var 10, suggesting a lack of spatial co-presence with these two variables in high cybercrime countries. Although they demonstrate some strong correlation, there is a great deal of variance in the extents to which these positive national attributes are found within high cybercrime countries. So, we have high cybercrime countries that score relatively highly on these attributes (such as Romania and Russia on most counts) whilst some score poorly (such as Nigeria). This suggests, then, that cybercrime is not simply a product of countries’ sharing broadly similar development profiles, with regard to these attributes at least.

What this analysis seems to confirm is the diverse trajectories of cybercrime within the countries within which it has developed extensively. In not identifying a universally criminogenic set of national attributes, it undermines somewhat the notion that the geographies of cybercrime are reducible to universal explanations. It points, perhaps, to different drivers of cybercrime development within different countries and regions, to the emergence of nationally or regionally specific cybercrime cultures. For this, there is support within cybercrime’s ethnographic literatures. For example, the literature records differences in the nature of regional cybercrime agglomerations with greater corporatisation and professionalisation typical of groups in ECE FSU (Glenny 2011, pp. 173-174; Kshetri 2013a, p. 42) and looser associations centred on cyber cafes which display only limited specialisation, characteristic of West Africa (UNODC 2005, p. 24; Aning 2007, p. 196; Burrell 2008; Agwu 2013; Ibrahim 2016a; 2016b; Eboibi 2017). There is also evidence of variations between regional agglomerations in the intrinsic motivations of cybercrime. Whilst the obvious financial motivation dominates in ECE FSU (albeit arguably also fused with geopolitical motivations in some instances) and places such as the Netherlands and Australia (Glenny 2012; Hutchings 2014; Goncharov 2015; Ortner 2015; Soudijn and Zegers 2015), in West Africa intrinsic motivations for cybercrime seem to be a more complex mix of the financial, lifestyle, status, religious and political (Peel 2006; Burrell 2008; Armstrong 2011; Tade and Ibrahim 2011; Ojedokun and Eraye 2012; Hartwig 2016; Lazarus, 2019)**.**

In addition to this, analysis at the national level is, inherently, able to say nothing about the specific empirics and dynamics of the sub national geographies of cybercrime. Yet, it is at the sub-national level that some of its most strikingly uneven geographies emerge. Examples include concentrations of cyber criminals in the Romania's Râmnicu Vâlcea and in the Igboland region of south east Nigeria, which reflects a history of genocide, social marginalisation and poor policing (Peel 2006; Zook 2007, p. 79). Such patterns suggest that there are processes of localisation in cybercrime economies that are not being captured through a national level lens and points to insights offered by micro-studies of cybercrime that demand further scrutiny.

**‘Hackervilles’? Micro-Associations within Cybercrime Hubs**

Many anthropological and sociological studies offer direct ethnographic observation of the grounded interactions between active cybercriminals and their local milieu (McCombie et al. 2009; Yip 2010; Adeniran 2011; Aransiola and Asindemade 2011; Armstrong 2011; Tade and Ibrahim 2011; Warner 2011; Ojedokun and Eraye 2012; Leukfeldt 2014; Jafarkarimi et al. 2015; Leukfeldt et al. 2017; Lusthaus and Varese 2017). These studies are typically conducted at the micro-scales of the neighbourhood, the cyber cafe, or the university and their observations interpreted within the contexts of complex regional histories, including those of colonialism, geopolitical hostility, economic transformation, poverty, technology, corruption and institutional weakness. For example, specific subcultures of cybercriminal activity have emerged that are conceived as related to and reflecting the values and attitudes of the local or national society. Hacking in China, then, takes on a nationalistic element whilst the Chinese government prioritise crimes that offend cultural values (and by extension pose a threat to the State) such as online pornography and gambling, over cyber-espionage or sabotage (Liang and Lu 2010; Yip 2010; Broadhurst and Chang 2013), whilst distinct Ghanaian and Nigerian subcultures of cybercrime are apparent (for example, yahooboyism and café culture) and a fusing of cybercrime with regional spiritual beliefs in Voodoo and Sakawa (Armstrong 2011; Warner 2011; Tade 2013; Lazarus, 2019).

 Ethnographic accounts of cybercrime dispel any lingering mythologies of it as solely a placeless, dispersed set of activities that are organised only through the virtual spaces of the internet. Rather, there is ample empirical evidence that it is locally embedded and, in some places at least, characterised by distinct hubs or agglomerations. Estimates suggest, for example, that 1000-2000 of Râmnicu Vâlcea's 120 000 population are involved in cybercrime, earning it the nicknames 'Hackerville' and 'the most dangerous town on the internet' (Bhattacharjee 2011; Franceschi-Bicchierai 2015), leading Lusthaus and Varese to conclude that Râmnicu Vâlcea represents “a major hub of cybercrime” (2017, p. 4). This section, then, spans three questions: what causes cybercrime gangs to form? Why do agglomerations of cybercrime gangs emerge in particular places? And, what positive externalities might cybercrime gangs derive from this arrangement?

 Râmnicu Vâlcea specialises in online auction fraud. Here, high value goods such as cars are offered for sale and advance fees or shipping fees solicited, whilst no goods are subsequently delivered. Organised scams of this nature can be extensive and potentially very lucrative, involving hundreds of fake advertisements generating $3 million of profit in one case (Lusthaus and Varese 2017, p. 3). Râmnicu Vâlcea's auction fraud gangs demonstrate functional specialisation with some members employed in the frauds' public faces, generating fake advertisements and managing customer / victim interactions, whilst others move and liquidate the monies generated (Bhattacharjee 2011; Lusthaus and Varese 2017, pp. 4-5). Cybercrime is undoubtedly important to Râmnicu Vâlcea in the context of a declining traditional industrial base and lack of alternative legitimate economic opportunities, and it appears to make tangible contributions to the city's development: “According to authorities, these [cybercrime] schemes have brought tens of millions of dollars into the area over the past decade, fuelling the development of new apartment buildings, nightclubs, and shopping centers. Râmnicu Vâlcea is a town whose business is cybercrime, and business is booming” (Bhattacharjee 2011, np).

 Within the city, cybercrime demonstrates tight socio-spatial agglomeration. The majority of cybercriminals come from a single district, Ostroveni, and are connected through shared neighbourhood and school ties (Bran, 2011 in Lusthaus and Varese 2017, pp. 6-7). There are clearly characteristics of Ostroveni that have facilitated the concentration of cybercrime there and equally, we might speculate, characteristics of other neighbourhoods in the city that have precluded or undermined its development there. Ostroveni is variously described in media reports as run down, working class and characterised by social housing from the Communist era (Bran 2012; 2013). Unfortunately, the literature offers no further clues currently to what the micro characteristics and processes underpinning the cybercrime economy of Ostroveni might be, although the neighbourhood's High School No 10 is alleged to be the focus of much of the area's cybercrime (Lusthaus and Varese 2017, p. 6). Ostroveni, then, remains something of a black box and we have a literature of it that, whilst it identifies a major cybercrime hub, offers little yet by way of highlighting the drivers that underpin its, and potentially others', development.

 However, Leukfeldt’s (2014) analysis, utilising case files and interviews with investigating officers, offers a glimpse into the internal world of a cybercrime gang who were based in the Bijlmer neighbourhood of Amsterdam and potentially provides some insights into the local dimensions of cybercrime that are transferable beyond its immediate site. This analysis has also been complemented by more extensive but nonetheless high-resolution studies of 40 cybercrime networks in the Netherlands, Germany, the UK and USA (Leukfeldt et al. 2017a; 2017b). This highlights that the balance between social and virtual ties vary between different cybercrime networks. Leukfeldt et al. (2017a, p. 45) concluded though that “social ties play an important role in origin and growth processes” of cybercrime gangs. For example, Leukfeldt et al. (2017b. p. 712) found that 13 of the 18 Dutch networks they analysed grew exclusively through social contacts. In such cases, gangs tend to display tightly clustered neighbourhood-focused social geographies, where social ties are fostered through schools, sports clubs, acquaintance on the street, within prisons or through previous criminal activity. Scrutinising Leukfeldt’s analysis offers some insights into the neighbourhood ‘ingredients’ that contribute to the development of cybercrime economies. Two neighbourhood characteristics stand out. First, is the presence of ‘core members’ of cybercrime gangs, individuals who instigate gangs, perform several important roles such as moving money, and controlling non-core gang members (Leukfeldt 2014 pp. 235-236; Leukfeldt 2017b, p. 710). These core members are required for cybercrime gangs to emerge. There has previously been some debate within the literature over the relationships between cybercrime and traditional forms of organised crime (see Glenny 2008, p. 314; 2012, p. 145; McCombie et al. 2009; Kshetri 2013a; Ortner 2015). Here, however, the contours of wider urban organised crime economies appear to be significant to those of cybercrime. In 15 out of the 22 cases analysed by Leukfeldt et al. (2017a) and nine of the 18 analysed by Leukfeldt et al. (2017b), core members were also involved in other offline crimes such as “drug trafficking, arranging fake marriages, fraud, robbery and identity forgery” (Leukfeldt et al. 2017a, p. 47). The evidence here points to the key roles of these core members in initiating cybercrime gang formation. Second, this work reveals the importance of more detached, dispersed social networks through which gangs recruit non-core members. Non-core members enable criminal activity, for example, through roles as bank or postal workers or as ‘money mules’ through whom cash from scams is liquidated (Leukfeldt, 2014, pp. 236-241). The literature speaks, in such cases, of recruitment through “the grapevine”, “vague acquaintances”, “friends of friends” (Leukfeldt 2014, pp. 238-240), “in schools, at sports or night clubs, or just on the street” (Leukfeldt et al. 2017b, p. 714).

 A further question concerns what causes the shift from a cybercrime economy based on the operations of a single gang, as appears to be the case in Bijlmer, to an extensive, multi-gang cybercrime economy, as appears to be the case in Ostroveni? It would seem most likely that neighbourhoods such as Ostroveni are characterised by an unusually high concentration of suitable cybercrime gang core members whose presence has the capacity to initiate the development of multiple networks, though this is something that the literature has yet to explicitly address.

These observations beg a final question. Namely, is the clustering of cybercriminals of the kind observed in Ostroveni merely an empirical outcome of certain local processes or is it an active component of the operation of these cybercrime economies? Does it offer gangs a comparative advantage of the kinds observed in other, legal, markets studied by economic geographers? Economic geographers have long recognised that the agglomeration of industrial activity can offer firms within particular industrial sectors advantages that can be realised economically. Commentators working within this tradition have argued that these advantages include: the sharing of factor inputs, such as pools of specialist labour; degrees of co-ordinated and co-operative, as well as competitive, behaviour between firms; the presence of related and supportive industries; accommodating local institutional arrangements and policy contexts; regional cultures that foster innovation; networks of trust and ‘local buzz’ that develop amongst entrepreneurs through face-to-face contacts; and the inputs from networks of external linkages and knowledge flows (Porter, 1990: 80; Bathelt et al. 2004; Aoyama et al. 2011). In sum, it has been argued that industrial agglomerations are “places that induce technological innovation and productivity growth, ultimately making them internationally competitive and economically resilient” (Aoyama et al. 2011, p. 86).

We might tentatively suggest that, despite there being no tradition of economic geography analysis of cybercrime agglomerations, the cybercrime literature offers some clues that suggest the advantages accruing to the multiple gangs operating within cybercrime hubs might mirror, or potentially exceed, those observed within legal information technology agglomerations (Huber, 2012). These advantages to cybercrime gangs include: the sharing of practice amongst cybercriminals within common social and work spaces such as the cybercafé (Agwu, 2013); the normative influence of cybercriminals within their regional cultural realm (Armstrong 2011; Olayinka Akanle, et al. 2016); cybercriminals seeking protection through corrupt connections with the local institutional environment which undermine law enforcement efforts (Yazdanifard and Oyegoke 2011; Lusthaus and Varese 2017, p. 6); the presence of related and supportive industries, Lazarus (2018), for example, discusses the synergies between Nigerian cybercriminals and hip hop artists / record labels, which facilitate the laundering of cybercrime profits and the positive representation of cybercriminals in Nigerian hip-hop music; as well as the sharing of specialist knowledge and software both face-to-face and through virtual forums (Glenny, 2011; Yazdanifard et al. 2011; Soudijn and Zegers, 2012; Leukfeldt et al. 2017a). Understanding agglomeration processes and their effects then offers the potential for opening up new fronts in the fight against cybercrime directed towards undermining the clustering of gangs, which, if their economies mirror those of legal industrial sectors, are potentially important components of their success and endurance.

**Transnational Asymmetries, Connections, Opacities and the Production of Cybercrime**

At the national and transnational scales, then, cybercrime is viewed as, in part, the product of asymmetries in the realms of legislation, regulation, policy and enforcement. Kshetri (2005, p. 543) argues, that “organized cybercrimes are initiated from countries that have few or no laws directed against cybercrimes and little capacity to enforce existing laws” (see also Kshetri, 2010b; Cassim 2011; Broadhurst and Chang 2013). Such asymmetries are apparent, for example, in the results of the statistical studies of cybercrime discussed above. The potential of such transnational asymmetries “structural disjunctures, mismatches and inequalities in the spheres of politics, culture, the economy and the law” (Passas 2001, p. 35) to be criminogenic has long been recognised in the context of organised crime (Midgley et al. 2014, p. 35). What is not disputed here is the criminogenic potentials of these asymmetries. Rather, we are concerned with rethinking their causes. The prevailing interpretation of the causes of these regulatory asymmetries are a series of endogenous failures of cybercrime origin nations in West Africa (Olayemi, 2014; Eboibi 2017) or ECE FSU (Vasylenko, 2012; Ortner, 2015; Ilievski and Bernik 2016) to meet Northern normativities of good governance generally, and of anti-cybercrime state actions specifically. However, there is a danger here that what eludes such a perspective are the multiple ways in which these apparently endogenously produced conditions might in fact be, in part at least, relationally produced.

 The literature on the relational production of cybercrime is, currently, patchy. Whilst it does not constitute a mainstream perspective within cybercrime research, it does record a number of examples from where a more substantive perspective might emerge and which highlights some of the limitations of extant perspectives who, perhaps implicitly, perpetuate a somewhat endogenous, othering gaze. For example, cybercrime in West Africa is typically attributed to a diverse palate of pathologies including political corruption, poor and indifferent governance, institutional weakness, weak rule of law, cultures of materialism, unbalanced economic development, chaotic economic change, poverty and inequality (see table 1 and Adeniran 2011; Ariansola and Asindemade 2011; Tade and Ibrahim 2011; Agwu 2013; Ibrahim 2016a). Whilst some authors recognise the roles of external agents within the production of such conditions, Ibrahim (2016a), for example, cites the role of the International Monetary Fund in the significant debt problems that affected the region following market reforms, there is a danger that check-lists such as this obfuscate the potentially external origins of these pathologies. Whilst we do not wish to suggest that West Africa was formerly a wholly pristine environment which has become corrupted by external forces, we would suggest that the complicity of external agents and their relations needs to be more prominently acknowledged within accounts of all regional cybercrime economies. We would then propose a perspective within which the relational was more routinely acknowledged.

 The UNODC (2005), for example, cite Williams (2004, p. 21) who argues that the origins of Nigerian advance fee '419' scams lie in the collaborative abuse of import administrative requirements during the Nigerian oil boom of the 1970s and 1980s. Here, Nigerian public officials colluded with foreign business partners who would massively over-invoice goods imported into Nigeria, resulting in the transfer of large sums of money out of the country. This tradition of fraudulent, collaborative transfer of money out of the region later underpinned the development and growth of Nigerian 419 bulk email scams. These were based on scripts directed towards potential Western victims, apparently sent by well-connected but persecuted Nigerians who urgently needed to transfer multi-million dollar sums out of the region in return for a Western collaborator receiving a cut of the money. These communications were in fact the means to obtain bank account details from anyone gullible enough to respond. To external eyes that saw West Africa predominantly through pathologies of chaos, exploitation and as the source of easily obtained illicit wealth, such requests appeared plausible. Individual cases reflected the scale of illicit wealth transfer out of Nigeria during its earlier oil boom. One gang, for example, persuaded the head of International Finance at Brazil's Banco Nordeste to transfer monies equivalent to US$240 million linked to the construction of a (non-existent) airport (UNODC 2005, p. 26).

 Central to the success of these scams are email representations of the West African region as one riven by chaos, corruption, exploitation and danger. Whilst these representations are scripted by scammers themselves, they too can be thought of as relationally produced. These are not simply free-floating products of scammers' fertile imaginations. Rather, they are simulacra that reflect back to external audiences their own tendency to view West Africa in these deeply stereotypical terms (Zook 2007, p. 78-79). In this subversion of post-colonial exploitation, Burrell (2008) draws on de Certeau’s notion of ‘tactics’ to illustrate how cybercriminals can take advantage of the Western ‘gaze’ of Africa as war-torn, impoverished and chaotic whilst Africans are viewed as not clever enough to conduct a sophisticated scam. The evolution of Nigeria's 419 scams is often painted as one of long histories of Nigerian letter, fax and telephone based scams directed towards Western victims (Gleeny 2008; Agwu 2013; Ibrahim 2016a) that has simply migrated online. However, to submerge or fail to appreciate the relational aspects of their evolution offers only partial and arguably orientalist interpretations.

 High levels of corruption have also been painted as a factor facilitating the growth of cybercrime in West Africa. Again these are typically attributed to endogenous failures within the countries concerned, often through the apparent moral failings of public officials or in more structural corruption inherent in the region's institutions. By contrast one account locates this, in the case of Nigeria, not solely within such endogenous failures but also in a series of political-economic relations with the West, specifically the UK. These include extensive corrupt practices of British companies in Africa and the British government's failure to address such practices, despite previous commitments to do so, and the complicity of British financial institutions in laundering illicit funds originating from Nigerian public officials (Peel 2006). This analysis mirrors wider critical geographical perspectives on the relational production of corruption in the global South (Brown and Cloke 2004). It points to sites of intervention in addressing cybercrime lying in Westminster and the City of London as well as in Lagos and Igboland.

Further evidence of the transnational, relational production of cybercrime is apparent in the case of e-waste flows to West Africa and the personal data harvesting industry there that this has spawned. Global e-waste movements are notoriously opaque. Of the 44.7 million metric tonnes of e-waste generated globally in 2016, only 10-20 per cent was documented to be properly collected and recycled (Baldé et al., 2017, p. 39; Iwenwanne 2019). West Africa is a global hub for transnational flows of e-waste for recycling. 60 percent of the UK's e-waste, for example, is recycled in Nigeria, which received 288 000 tonnes in 2017, while Ghana receives 215,000 tonnes of e-waste per year (Doyon-Martin 2015; Hartwig 2016; Iwenwanne 2019). These imports allow the harvesting of personal data from e-waste that has been inadequately secured and wiped prior to disposal. The result of regulatory arbitrage by Western e-waste entrepreneurs after the enactment of environmental regulations in South East Asia largely curtailed e-waste flows there (Doyon-Martin 2015: Hartwig 2016), these transnational e-waste networks have facilitated personal data harvesting through a lack of awareness and responsibility for secure e-waste disposal amongst Western consumers; complex, opaque supply chains that allow the anonymous acquisition of e-waste by West African criminal groups; poor enforcement of OECD e-waste regulations; and inadequate e-waste recycling and disposal infrastructure in West Africa (Warner 2011; Doyon-Martin 2015; Hartwig 2016; Ibrahim 2016a). The exportation of European and North American consumers’ e-waste to Ghana and Nigeria could be interpreted as the latest form of exploitation of African countries by (post-) colonial wealthier countries. As Hartwig (2016) notes, the Agbogbloshie district in Accra, Ghana was a pristine and ecologically diverse wetland as recently as the 1990s but is now a dump site for e-waste. The transportation of e-waste across multiple borders and the lack of enforcement of regulations regarding its disposal leaves plenty of opportunity for it to enter hidden flows towards black markets. Once inside such flows it becomes easier for devices to be sold into cybercriminal hands than responsibly disposed or recycled. By using the personal data harvested from (often illegally) imported e-waste, cybercriminals are again able to find a perceived form of justice from wealthier nations that use parts of West Africa as land-fill.

**Mobilising Geographical Perspectives on Cybercrime**

Overwhelmingly, to date, anti-cybercrime measures have sought to construct hostile legislative, regulatory and institutional environments through effective data collection, surveillance of illegal activities, appropriate technological defences and investment in expert and lay knowledge to identify and defend against attacks. In turn, effective processes for reporting, law enforcement and retaliating against cybercriminal behaviour are instituted. By contrast, few anti-cybercrime initiatives have sought to mobilise insights into the socio-spatial contexts from which cybercrime emerges. However, this paper suggests a number of scales across which such knowledges might be applied.

 At the national scale, the analysis presented here found little evidence that cybercrime’s geographies are subject to universal explanations. Rather, it points to policies that are nationally or regionally sensitive. Further, it suggests that development-oriented policies per se, do not necessarily offer routes out of cybercrime unless they are also able to engage with its specific drivers, practices and cultures at these scales.

At the local scale, Leukfeldt (2014) recognises the contributions of situational crime prevention in disrupting individual, neighbourhood-based cybercrime networks. We have seen that concentrations of network core members, many active in offline crimes, is potentially key in the emergence of cybercrime hubs. This suggests that tightly focused place-based police strategies aimed at disrupting underworld activity may have a disruptive effect on cybercrime network formation and, where it can target core members of multiple networks, on the emergence of cybercrime hubs. More needs to be known, however, about agglomeration processes within cybercrime economies before such strategies can be deployed with confidence. Further, studies have highlighted the roles that sites such as schools, sports clubs, workplaces and universities play in recruitment of non-core members to cybercrime networks and the formation of the looser associations characteristic of West Africa (Ojedokun and Eraye 2012; Ibrahim, 2016b; Lusthaus and Varese, 2017; Leukfeldt et al. 2017b). Here site-based, non-police strategies might be enacted that explore these ‘micro-publics’, sites of potential inter-cultural dialogue around shared interests, presences and common goals (Amin 2002; Sandercock 2006), to challenge the normative holds of gangsterism within local cultural realms.

 At the transnational scale we might recognise two potential interventions. The first concerns the elimination of certain transnational legal and regulatory asymmetries recognised as facilitating cybercrime (Broadhurst and Chang 2013). This echoes a wider policy discourse that identifies tackling such asymmetries as a key means of harming organised crime groups of all kinds (Passas 2001; Hudson 2014; Midgley et al. 2014). The second involves infusing policy with a more relational sensibility. Lusthaus and Varese (2017, p. 8) are right to argue that “cybercrime [also] needs to be tackled in the places where it originates”. To this we would emphasise, drawing on a tradition of geographical scholarship that views places not as bounded entities (Sheppard, 2002), that it is important not to draw boundaries around the places where cybercrime originates and solely direct interventions internally. A number of studies highlight the need, at times, to direct interventions to regions spatiality distant to the places from which cybercrime emerges but which are nonetheless closely networked with them. These include, for example, in the case of e-waste flows to West Africa, better enforcement of OECD e-waste regulations, measures to improve awareness of secure e-waste disposal practices amongst Western consumers and greater transparency within transnational e-waste supply chains (Warner 2011; Doyon-Martin 2015; Ibrahim 2016a; Hartwig 2016). These dispersed policies, though, should be connected through models that echo the networked nature of the cybercrime problem. Individual initiatives enacted in discrete places are likely to have only limited impacts. There is a nascent understanding from the policy literatures of other illegal markets of the potentially enhanced effectiveness of enacting multiple policies in combination, rather than individual policies in isolation (Babor, et al. 2010; Kilmer et al. 2015; Kilmer 2016), although the evidence base here is currently thin. In sum, this paper suggests the potentials of multiscalar, relational pluri-policy models be further explored in the case of cybercrime.

**Conclusions**

Three broad conclusions emerge from the analysis within this paper. First, it suggests that the geographies of cybercrime are not reducible to universal explanations. Whilst it did not identify any universally criminogenic combination of national attributes, different sets of incongruous combinations of such attributes might apply at the level of national or regional agglomerations of cybercrime. Here it points to the potential significance of regional cultures and practices of cybercrime and the framing of policy responses accordingly. Second, it discerns some tentative evidence of agglomeration effects within cybercrime economies that are deserving of further attention. Finally, it highlights the need to acknowledge more the potential relational production of cybercrime agglomerations.

Whilst the previous section has highlighted some policy directions, the recognition of the multi-scalar, regional and relational production of cybercrime, emphasised through the geographical reading offered within this paper is also significant in research terms. This paper acknowledges the pioneering, high-resolution insights advanced by cybercrime’s ethnographic literatures from anthropological and sociological traditions. However, in coming from disciplines where questions of spatiality are not routinely central they have yet to explicitly or fully scrutinise those processes underpinning cybercrime’s distinctive geographies and their effects. Specifically, this paper recognises the need for research that explores the processes that have produced tight spatial agglomeration of cybercriminals in some places, the economically realisable advantages that they derive from this and their local economic development impacts. Whilst this paper has highlighted that agglomerations are characteristics of those forms of cybercrime for whom social ties are important forms of governance and organization, it is less clear to what extent, if at all, they also emerge in forms of cybercrime that are predominantly governed and organized through virtual forums or in hybrid ways. This is an issue that would repay further investigation. At a national scale this paper has suggested the potentials of analysis that accommodates a wider range of predictor variables than has previously been the case within research from this tradition. Here we might look to an expanded dialogue with micro-scale ethnographic literatures in the identification of these variables that draws upon their shared interest in understanding the regional contexts from which cybercrime emerges. This has only been achieved in an exploratory sense within this analysis and there remains much to be done here. This paper has also discussed that limited body of research that has suggested a relational, transnational contribution to the production of the conditions within which cybercrime might thrive, suggesting that such perspectives might emerge as more central within future cybercrime analysis.

 Currently, the various cybercrime literatures discussed above exist largely in mutual isolation. The introduction to this paper referenced the observation of the economic geographer Ray Hudson that “the contemporary illegal economy is grounded in the *subtle* *interplay between* (our emphasis) activities at different scales” (2014: 780). That an economic geography perspective is yet to emerge within cybercrime research not only suggests the further developments within its specific literatures discussed above, but that future research should be characterised much more by these literatures being brought more closely into dialogue.

**References**

Aas KF, (2007) Globalization and Crime. Sage, London

\*Adeniran A, (2011) Cafe culture and heresy in Yahooboyism in Nigeria. in Jaishankar K, (ed) Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour. CRC Press, Boca Raton, FL, pp. 3-12

\*Agwu E, (2013) Cybercriminals on the internet superhighways: a technical investigation of different shades and colours within the Nigerian cyberspace. International Journal of Online Marketing 3 (2): 56-74

Allen CM, (2005) An Industrial Geography of Cocaine. Routledge, New York

Amin A, (2002) Ethnicity and the Multicultural City: Living with Diversity. Report for Department of Transport, Local Government and the Regions. University of Durham, Durham

Anderson R, Barton C, Bohme R, Clayton R, van Eeten, MJG, Levi M, Moore T, and Savage S, (2012) Measuring the Cost of Cybercrime <https://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf> (Accessed 9th April 2020)

Aning K, (2007) Are there emerging West African criminal networks? The case of Ghana. Global Crime 8 (3):193-212

Aoyama Y, Murphy JT, and Hanson S, (2011) Key Concepts in Economic Geography. Sage, London

\*Aransiola JO, and Asindemade SO, (2011) Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychology, Behaviour and Social Networking 14 (2): 759-763

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

\*Asal V, Mauslein J, Murdie A, Young J, Cousins K, and Bronk C, (2016) Repression, education and politically motivated cyberattacks. Journal of Global Security Studies 1 (3): 235-247

\*Atta-Asamoah A, (2010) Understanding the West African cyber crime process. African Security Review 18 (4): 105-114

Babor T, Caulkins J, Edwards G, Fischer B, Foxcroft D, Humphreys K, Obot I, Rehm J, Reuter P, Room R, Rossow I, and Strang J, (2010) Drug Policy and the Public Good. Oxford University Press, Oxford

Bah M T, Shi J, Browne M, Suchier Y, Lefebvre F, Young P, King L, Dunlop DG, and Heller MO, (2015) Exploring inter-subject anatomic variability using a population of patient-specific femurs and a statistical shape and intensity model. Medical Engineering & Physics 37 (10): 995–1007

Baldé CP, Forti V, Gray V, Kuehr R, and Stegmann P, (2017) Global E-waste Monitor 2017: Quantities, Flows and Resources, United Nations University (UNU), International Telecommunication Union (ITU) & International Solid Waste Association (ISWA), Bonn/Geneva/Vienna

Bathelt H, Malmberg A, and Maskell P. (2004) Clusters and knowledge: local buzz, global pipelines and the process of knowledge creation. Progress in Human Geography 28 (1): 31-56

Beckert J, and Dewey M, (eds) (2017) The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy. Oxford University Press, Oxford

\*Beek J, (2016) Cybercrime, police work and storytelling in West Africa. Africa 86 (2): 305-323

Belam M, (2016) We're living through the first world cyberwar – but just haven't called it that. *The Guardian*, <https://www.theguardian.com/commentisfree/2016/dec/30/first-world-cyberwar-historians> (Accessed 9th April 2020)

Berger A, D’Alconzo A, Gansterer WN, and Pescapé A, (2016) Mining agile DNS traffic using graph analysis for cybercrime detection.Computer Networks 100: 28–44

\*Bernik I, (2014) Cybercrime and Cyberwarfare. ISTE Ltd / John Wiley and Sons, London and Hoboken, NJ

Bhattacharjee Y, (2011) Welcome to Hackerville: The Romanian cybercriminal hotspot. Wired 7th February, <https://www.wired.co.uk/article/welcome-to-hackerville> (Accessed 9th April 2020)

Bran M, (2011) Les pirates roumains d’ “Hackerville” tiennent te ˆte aux polices du monde entire’. Le Monde 28th December

Bran M, (2012) Romania: ‘Hackerville’, capital of global cyber-crime. France24 7th December: <https://www.france24.com/en/20121207-reporters-romania-hackerville-ramnicu-valcea-cyber-crime-fraud-scams-hackers-internet-police-fbi-cia-bitdefender> (Accessed 9th April 2020)

Bran M, (2013) In Romania, a quiet city has become the global hub for hackers and online crooks. Worldcrunch 7th January: <https://worldcrunch.com/tech-science/in-romania-a-quiet-city-has-become-the-global-hub-for-hackers-and-online-crooks> (Accessed 9th April 2020)

\*Broadhurst R, and Chang YC, (2013) Cybercrime in Asia: trends and challenges. In Liu J, Hebenton, B and Jou S, (Eds.) Asian Handbook of Criminology. Springer, New York, pp. 49-63

\*Broadhurst R, Grabosky P, Alazab M, and Chon S, (2014) Organisations and cybercrime: an analysis of the nature of groups engaged in cybercrime. International Journal of Cyber Criminology 8 (1): 1-20

Brown E, and Cloke J, (2004) Neoliberal reform, governance and corruption in the South: assessing the international anti-corruption crusade. Antipode 36 (2): 272-294

\*Burrell J, (2008) Problematic empowerment: West African internet scams as strategic misrepresentation. Information Technologies and International Development 4 (4): 15-30

\*Cassim F, (2011) Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. Comparative and International Law Journal of Southern Africa5, (1): 123-138

Chiodelli F, Hall T, and Hudson R, (eds.) (2017) The Illicit and Illegal in Regional and Urban Governance and Development: Corrupt Places. Routledge, Abingdon

Cohen LE, and Felson M, (1979) Social change and crime rate trends: a routine activity approach. American Sociological Review 44, (4): 588-608

Dearden L, (2017) Russian-speaking countries pose ‘number-one cyber threat to UK’, officials warn. Independent 17th November. <https://www.independent.co.uk/news/uk/crime/russia-hacking-threat-uk-number-one-warning-cyber-attacks-wannacry-north-korea-iran-investigations-a8061521.html> (Accessed 9th April, 2020)

Dodge M, and Kitchin R, (2001) Mapping Cyberspace. Routledge, London

\*Donner CM, Marcum CD, Jennings WG, Higgins GE. and Banfield J, (2014) Low self-control in cybercrime: exploring the utility of the general theory of crime beyond digital piracy. Computers in Human Behavior, 34: 165-172

\*Doyon-Martin J, (2015) Cybercrime in West Africa as a result of transboundary e-waste. Journal of Applied Security Research. 10 (2): 207-220

\*Eboibi FE, (2017) A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. Computer Law and Security Review 33 (5): 700-717

Franceschi-Bicchierai L, (2015) Inside ‘Hackerville’, Romania’s infamous cybercrime hub. Vice, 17th June, <https://www.vice.com/en_us/article/4x3jnd/inside-hackerville-romanias-infamous-cyber-crime-hub> (Accessed 9th April 2020)

Galeotti M, (ed.) (2005) Global Crime Today: The Changing Face of Organised Crime, Routledge, London

\*Ghandi R, Sharma A, Mahoney W, Sousan W, Zhu Q, and Laplante P, (2011) Dimensions of cyber-attacks: cultural, economic, social and political. IEEE Technology and Society Magazine 30 (1): 28-38

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

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

\*Glenny M, (2012) Organised crime in a network society. Journal of International Affairs 66 (1): 145-149

\*Goncharov M, (2015) Russian underground 2.0. Trends Lab Working Paper, Trends Micro, Tokyo

\*Grabosky P, (2007) The internet, technology and organized crime. Asian Journal of Criminology 2 (2): 145-161

Hall T, (2013) Geographies of the illicit: globalisation and organised crime. Progress in Human Geography 37 (3): 366 – 385

Hall T, (2018) The Economic Geographies of Organized Crime. Guilford, New York

\*Hartwig K, (2016) Digital Waste and Cybercrime: Understanding the Relationship. Working paper, Harvard University (available from: <http://www.academia.edu/31385539/DIGITAL_WASTE_and_CYBER_CRIME_EXAMINING_THE_RELATIONSHIP> accessed 22nd October 2018)

\*Hassan AB, Lass FD, and Makinde J, (2012) Cybercrime in Nigeria: causes, effects and the way out. ARPN Journal of Science and Technology 2 (7): 626-631

Holmes L, (2016) Advanced Introduction to Organised Crime. Edward Elgar, Cheltenham

Holt TJ, Burruss GW, and Bossler AM, (2018) Assessing the macro-level correlates of malware infections using a routine activities framework. International Journal of Offender Therapy and Comparative Criminology 62, (6): 1720-1741

Huber F, (2012) Do clusters really matter for innovation practices in Information Technology? Questioning the significance of technological knowledge spillovers. Journal of Economic Geography 12 (1): 107-126

Hudson R, (2014) Thinking through the relationships between legal and illegal activities and economies: spaces, flows and pathways. Journal of Economic Geography 14 (4): 775-795

Hudson R, (2019) Economic geographies of the (il)legal and the (il)licit. in Hall, T. and Scalia, V. (eds) A Research Agenda for Global Crime. Edward Elgar, Cheltenham, pp. 11-27

\*Hutchings A, (2014) Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission. Crime, Law and Social Change 62 (1): 1-20

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

\*Ibrahim S, (2016b) Causes of socioeconomic cybercrime in Nigeria. Proceedings of 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF) <https://ieeexplore.ieee.org/document/7740439> (Accessed 19th October 2018)

\*Ilievski A, and Bernik I, (2016) Social-Economic aspects of cybercrime. Innovative Issues and Approaches in Social Sciences 9 (3): 8-22

Iwenwanne V, (2019) Nigeria's e-waste mountain. Resource <https://resource.co/article/nigerias-e-waste-mountain> (accessed 30th September 2019)

\*Jafarkarimi H, Tze Hiang Sim A, Saadatdoost R, and Mei Hee J, (2015) Individual characteristics and hacking, piracy, online gambling and pornography use among students: a study in Malaysia. International Journal of Cyber Behaviour, Psychology and Learning 5 (2): 30-43

\*Kigerl A, (2012) Routine activity theory and determinants of high cybercrime countries. Social Science Computer Review 30 (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 10, (2): 147-169

Kigerl A, (2016b) Email spam origins: does the CAN SPAM act shift spam beyond United States jurisdiction? Trends in Organized Crime 21, (1): 62-78

Kilmer B, (2016) Uncle Sam's cocaine nosedive: a brief exploration of a dozen hypotheses. in LSE Expert Group on the Economics of Drug Policy, (eds) After the Drug Wars. Report of the LSE Expert Group on the Economics of Drug Policy. London School of Economics, London, pp. 67-78

Kilmer B, Midgette G, and Saloga C, (2015) Back in the National Spotlight: An Assessment of Recent Changes in Drug Use and Drug Policies in the United States. Brookings Institute, Washington DC

Kraemer-Mbula E, Tang P, and Rush H, (2013) The cybercrime ecosystem: online innovation in the shadows? Technological Forecasting & Social Change 80: 541–555

\*Kshetri N, (2005) Pattern of global cyber war and crime: a conceptual framework. Journal of International Management 11 (4): 541-562

\*Kshetri N, (2009) Positive externality, increasing returns, and the rise in cybercrimes. Communications of the ACM 52 (12): 141-144

\*Kshetri N, (2010a) Diffusion and effects of cyber-crime in developing economies. Third World Quarterly 31 (7): 1057-1079

\*Kshetri N, (2010b) The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Springer, New York

\*Kshetri N, (2013a) Cybercrimes in the Former Soviet Union and Central and Eastern Europe: current status and key drivers. Crime, Law and Social Change 60 (1): 39-65

\*Kshetri N, (2013b) Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. Electronic Commerce Research 13 (1): 41-69

Lavorgna A. (2020) Organized crime and cybercrime in Holt T J, and Bossler A M, (eds) The Palgrave Handbook of International Cybercrime and Cyberdeviance. Cham, Switzerland: Palgrave Macmillan

Lazarus S. (2018) Birds of a feather flock together: the Nigerian cyber fraudsters (Yahoo Boys) and hip hop artists. Criminology, Criminal Justice, Law and Society, 19 (2): 63-81

Lazarus S. (2019) Where is the money? The intersectionality of the spirit world and the acquisition of wealth. Religions, 10 (3): <https://doi.org/10.3390/rel10030146>

\*Leukfeldt ER, (2014) Cybercrime and social ties: phising in Amsterdam. Trends in Organized Crime 17 (4): 231-249

\*Leukfeldt ER, Kleemans ER, and Stol WP, (2017a) Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis. Crime, Law and Social Change 67 (1): 39-53

Leukfeldt ER, Kleemans ER, and Stol WP, (2017b) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. British Journal of Criminology 57, (3): 704-722

\*Li X, (2017) A review of motivations of illegal cyber activities. Criminology and Social Integration Journal 25 (1): 110-126

\*Liang B, and Lu H, (2010) Internet development, censorship and cyber crimes in China. Journal of Contemporary Criminal Justice 26 (1): 103-120

\*Lusthaus J, (2013) How organised is organised cybercrime? Global Crime 14 (1): 52-60

\*Lusthaus J, and Varese F, (2017) Offline and local: the hidden face of cybercrime. Policing: A Journal of Policy and Practice doi.org/10.1093/police/pax042

\*Malin CH, Gudaitis T, Holt TJ, and Kilger M, (2015) Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communications. Academic Press, London

\*Marcum CD, Higgins GE, Ricketts ML, and Wolfe SE, (2014) Hacking in high school: cybercrime perpetration by juveniles. Deviant Behavior 35 (7): 581-591

\*McCombie S, Pieprzky J, and Watters P, (2009) Cybercrime attribution: an Eastern European case study. Proceedings of the 7th Australian Digital Forensics Conference Edith Cowan University, Perth Western Australia, December 3rd 2009, pp. 41-50

Midgley T, Briscoe I, and Bertoli D, (2014) Identifying Approaches and Measuring Impacts of Programmes Focused on Transnational Organised Crime. Department for International Development, London

Neal S, (2010) Cybercrime, transgression and virtual environments. In Muncie J, Talbot D, and Walters R, (eds) Crime: Local and Global. Cullompton: Devon

Nordstrom C, (2007) Global Outlaws: Crime, Money, and Power in the Contemporary World. University of California Press, Berkley

\*Odumesi JO, (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology 6 (3): 116-125

\*Okeshola FB, and Adeta AK, (2013) The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research 3 (9): 98-114

\*Ojedokun UA, and Eraye MC, (2012) Socioeconomic lifestyles of the Yahoo Boys: a study of perceptions of university students in Nigera. International Journal of Cyber Criminology 6 (2): 1001-1013

\*Olayemi OJ, (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology 6, (3): 116-125

\*Olayinka Akanle JO, Adesina and Akarah EP, (2016) Towards human dignity and the internet: the cybercrime (*yahoo yahoo*) phenomenon in Nigeria. African Journal of Science, Technology, Innovation and Development, 8 (2): 213-220

\*Ortner D, (2015) Cybercrime and punishment: The Russian Mafia and Russian responsibility to exercise due diligence to prevent trans-boundary cybercrime. Brigham Young University Law Review 1: 177-218

Passas N, (2001) Globalization and transnational crime: effects of criminogenic asymmetries. In Williams P, and Vlassis D, (eds) Combating Transnational Crime: Concepts, Activities and Responses. Frank Cass, London

\*Peel M, (2006) Nigeria Related Financial Crime and its Links with Britain. Chatham House, London

Porter ME, (1990) The competitive advantage of nations. Harvard Business Review March-April: 73-91

Porter, ME, (1998) Clusters and the new economics of competition. Harvard Business Review 76 (6): 77-90

\*Rashkovski D, Naumovski V, and Naumovski G, (2016) Cybercrime tendencies and legislation in the Republic of Macedonia. European Journal on Criminal Policy and Research 22 (1): 127-151

Sandercock L, (2006) Cosmopolitan urbanism: a love song to our mongrel cities. in Binnie J, Holloway J, Millington S, and Young C, (eds) Cosmopolitan Urbanism. Routledge, Abingdon

\*Shabnam N, Faruk O Md, Kamruzzaman Md, (2016) Underlying causes of cyber-criminality and victimization: an empirical study on students. Social Sciences 5 (1): 1-6

Sheppard E, (2002), The spaces and times of globalization: place, scale, networks and positionality. Economic Geography 78 (3): 307-330

\*Soudijn MR, and Zegers BCHT, (2012) Cybercrime and virtual offender convergence settings. Trends in Organized Crime 15 (2-3): 111-129

Symantec, (2011) Symantec Internet Security Threat Report, <https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf> (Accessed 18th October 2019)

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

\*Tade O, and Ibrahim A, (2011) Social organization of internet fraud among university undergraduates in Nigeria. International Journal of Cyber Criminology 5 (2): 860-875

UNODC, (2005) Transnational Organized Crime in the West African Region. United Nations Office on Drugs and Crime, Vienna

van Dijk J, (2007) Mafia markers: assessing organized crime and its impact upon societies. Trends in Organized Crime. 10, (4): 39-56

\*Vasylenko O, (2012) Problem of cybercrime in Ukraine: spread of, specific nature and methods of fighting. Internal Security 4 (1): no page

\*Warner J, (2011) Understanding cyber-crime in Ghana: a view from below. International Journal of Cyber Criminology 5 (1): 736-749

Williams P, (2004) The global implications of West African organized crime. Input paper: West African Assessment Project

Wilson E, (2009) Deconstructing the shadows. In Wilson E, (ed.) Government of the Shadows: Parapolitics and Criminal Sovereignty. Pluto Press, London

*\**Wittes B, Poplin C, Jurecic Q, and Spera C, (2016) Sextortion: Cybersecurity, Teenagers and Remote Sexual Assault. The Brookings Institution, Washington DC

*\**Wright S, (2017) Mythology of cyber-crime—insecurity & governance in cyberspace: some critical perspectives. In Ramírez J, and García-Segura L, (eds) Cyberspace: Risks and Benefits for Society, Security and Development. Springer, New York, pp. 211-227

Yar M (2005) The novelty of ‘cybercrime’: An assessment in light of routine activity theory. European Journal of Criminology 2: 407-427

Yar M (2019) Transnational governance and cybercrime control: dilemmas, developments and emerging research agendas. In Hall T, and Scalia V, (eds) A Research Agenda for Global Crime. Edward Elgar, Cheltenham, pp. 91-106

\*Yazdanifard R, Oyegoke T, and Seyedi AP, (2011) Cyber-crimes: challenges of the Millennium age. In Zheng, D. (ed) Advances in Electrical Engineering and Electrical Machines. Springer, New York, pp. 527-534

\*Yip M, (2010) An investigation into Chinese cybercrime and the underground economy in comparison with the West. Presentation to Netcraft, 7th Decemer https://eprints.soton.ac.uk/271759/ (Accessed 22nd October 2018)

\*Zanini M, and Edwards SJA, (2001) The networking of terror in the information age. In Arquilla J, and Ronfeldt D, (eds) Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND, Santa Monica Ca., pp. 29-60

*\**Zook MA, (2007) Your urgent assistance is requested: the intersection of 419 spam and new networks of imagination. Ethics, Place & Environment 10 (1): 65-88

1. Recent history of economic transition / liberalisation: Macroeconomic stability at pillar level. World Economic Forum, (WEF) Global Competitiveness Report (GCR), 2018.

2. Economic uncertainty / downturn: World Uncertainty Index, year average for 2018.

3. Poverty / lack of opportunities in legitimate economy (particularly affecting young people with IT skills): World Bank Unemployment with Advanced Education (% of total labour force with advanced education. 2017 (Nigeria 2016, Ghana 2015).

4. Blurring of licit and illicit economic practices: International Labour Organization Women and Men in the Informal Economy: A Statistical Picture, Share of informal employment in non-agricultural employment by urban location (2018).

5. Unbalanced economy / revenues inaccessible to the majority: Legatum Prosperity Index, 2018. (% of the population living below the national poverty lines).

6. High levels of education: Quality of math and science education from WEF Global Information Technology Report (GITR), 2016.

7. IT literacy / skills amongst young people: Digital skills amongst among population. WEF GCR, 2018.

8. Normative influence of consumerism / materialism: Post-materialist Index (4 item), World Values Survey, 2010-2014.

9. High internet penetration: WEF GITR, 2018. Internet users as a % of population.

10. Appropriate technical infrastructure: WEF GITR, 2018 3rd pillar infrastructure score.

11. High levels of corruption: Transparency International Corruption Perception Index, 2018.

12. State and institutional weakness: World Bank World Governance Indicators - Rule of law 2018.

13. Government indifference towards cybercrime / not a government priority: ITU Global Cybersecurity Index, 2017.

14. Internal legal and regulatory shortcomings: WEF GITR, 2016 – 1st pillar ‘Political and regulatory environment’.

15. Traditions of illicitness / normative influence of gangsterism: Legatum Prosperity Index, 2018 (Social capital pillar)

**Appendix**: National predictors of cybercrime – statistical sources.

ECONOMIC FACTORS

 Recent history of economic transition / liberalisation;

 Economic uncertainty / downturn;

 Poverty / lack of opportunities in legitimate economy (particularly affecting young people with IT skills);

 Blurring of licit and illicit economic practices.

 Additional factor (West Africa): Unbalanced economy / revenues inaccessible to the majority.

SOCIAL / CULTURAL FACTORS

 High levels of education;

 IT literacy / skills amongst young people;

 Traditions of illicitness;

 Normative influence of the illicit within the cultural realm;

 Normative influence of consumerism / materialism.

 Additional factor (West Africa): neglect of youth issues by governments.

TECHNOLOGICAL FACTORS

 High internet penetration;

 Appropriate technical infrastructure.

 Additional factor (West Africa): extensive physical movement of e-waste to West Africa.

POLITICAL FACTORS

 High levels of corruption;

 State and institutional weakness;

 Government indifference towards cybercrime / not a government priority;

 Justification for external victimisation.

 Additional factor (West Africa): long permeable borders allowing the transfer of people and ideas.

LEGAL, REGULATORY AND POLICING FACTORS

 Internal legal and regulatory shortcomings;

 Inadequate capacity to investigate and prosecute cybercrime;

 Challenges of transnational policing within these regions.

Table 1: Location factors / factor conditions identified as contributing to the development of cybercrime in FSU ECE and West Africa (for sources see references, all references informing this analysis highlighted with \*).



Figure 1: Correlation matrix of the considered dataset. Var1, Var 2,..Var 15 refers to the 15 cybercrime measures in Table 1 / variables in appendix.