Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country

Jonathan Lusthaus
Department of Sociology
University of Oxford
Oxford, UK
jonathan.lusthaus@sociology.ox.ac.uk

Miranda Bruce
UNSW Canberra Cyber
University of New South Wales
Canberra, Australia
miranda.bruce@unsw.edu.au

Nigel Phair
UNSW Canberra Cyber
University of New South Wales
Canberra, Australia
nigel.phair@unsw.edu.au

***Abstract*—The acknowledgement that cybercrime offenders are embedded within local contexts presents a broad vector for further study. But research in this area is still in its early days and many topics need to be developed further. Foremost among these is the geography of cybercrime. This endeavour has an important policy contribution to make. For example, if we can determine which countries are producing cybercrime at more significant levels, preventative measures can be specifically targeted to those countries. The first step within such a research agenda must be the development of an index of cybercriminality by country, as this is foundational to identifying hubs of digital offending and the factors driving the emergence of these hubs. This paper is methodological in its contribution, and does not offer its own empirical findings. Instead, it aims to provide some broad foundational thinking for a very challenging research exercise, and it is intended to support later, more refined, efforts to develop indices. It consists of two components. First, it reviews existing attempts to identify and rank cybercrime hotspots. Second, it draws important lessons from these works towards developing a successful index. Some methodological points are made on what the way forward may be for this emerging field, and how a reliable and valid index on cybercriminality could be crafted.**

***Index Terms*—cybercrime, offenders, geography, measurement, rankings, hubs**

I. Introduction

The acknowledgement that cybercrime offenders are embedded within local contexts presents a broad vector for further study [2], [13], [15]. But research in this area is still in its early days and many topics need to be developed further. Foremost among these is the geography of cybercrime. If we don't address this subject, scholars will fail to "see the particular factors playing into the structure of cybercrime operations within countries, the nature of local participants, and the specific ways they contribute to the overall industry" [1](p. 69). This endeavour has an important policy contribution to make. If we can determine which countries are producing cybercrime at more significant levels, preventative measures can be specifically targeted to those countries. This effort may also lead to a greater understanding of why cybercrime emerges more seriously in these places, which could allow the tailoring of specific policy responses. Finally, better comprehending the nature of cybercrime development may help identify future cybercrime hubs which are yet to fully emerge, so that early interventions could be made into at-risk countries before a serious cybercrime problem develops [5].

The first step within such a research agenda must be the development of an index of cybercriminality by country, as this is foundational to identifying hubs of digital offending and the factors driving the emergence of these hubs. This paper is methodological in its contribution, and does not offer its own empirical findings. Instead, it aims to provide some broad foundational thinking for a very challenging research exercise, which should support later, more refined, efforts to develop indices. It consists of two components. First, it reviews existing attempts to identify and rank cybercrime hotspots. Second, it draws important lessons from these works towards developing a successful index. Some specific methodological points are made on what the way forward may be for this emerging field, and how a reliable and valid index on cybercriminality could be crafted.

II. Literature on Cybercrime Rankings

The media regularly produces articles that identify cybercrime hotspots. For instance, in 2014, Time Magazine highlighted five of the "worst" countries involved in this "global business". These were Russia, which uses "some of the most technologically advanced tools in the trade", China, Brazil, Nigeria and Vietnam [6]. A number of blogs and articles have made similar claims, although there is some variation between them [7]. While some of these articles are summarising findings from industry reports [8], [9], the methodological approach behind the identification of cybercrime hotspots is not always clear. The rest of this section engages with the two core categories of research that aim to produce the fundamental knowledge on cybercrime rankings: 1) scholarly research; 2) reports from industry and law enforcement.

A. Scholarly Research

Unfortunately, the academic work on this subject is extremely sparse. It is rare to be able to discuss every (known) scholarly work that touches on a subject, but in this review we have that opportunity. If we have overlooked any examples, it is not due to volume. Perhaps the earliest academic attempt to grapple with this subject is carried out by McCombie and colleagues. McCombie, Pieprzyk and Watters [10] investigate whether Eastern European countries are particularly tied to "phishing and related cybercrime rather than elsewhere, and

why" (p. 41). While the article engages with a number of topics beyond the scope of this review, towards its end it attempts to isolate a series of variables that may explain why countries like Russia and Ukraine are particularly associated with cybercrime. The core variables it identifies are: corruption, Internet penetration, and levels of tertiary education, drawing on data from Transparency International, the International Telecommunications Union and the World Bank.

The paper implies a simple regression without carrying one out, and the result is an initial look at what factors may play a role in cybercrime hub formation. It would be interesting to expand this approach, both in terms of the dependent variable and the independent variables. The dependent variable is largely assumed and informal: that Russia and Ukraine are the leading proponents of cybercrime. This is an oversimplified dependent variable. Instead, this variable should be stated as "the presence of strong cybercriminality" or a similar configuration. By taking this limited two-state approach, the authors are largely discounting the idea of an index, which would include a range of cybercriminality across all (or a large number of) countries. While they discuss at least one other known cybercrime hub—Nigeria—they do not include it in their comparative analysis due to its low Internet penetration. This removes a country that might challenge the paper's model, especially as to how effective these factors are in explaining Russia and Ukraine's position as major cybercrime hubs. It might also have been interesting to compare Russia and Ukraine to other countries in the former Soviet Union that might have similar conditions. But this is not discussed.

McCombie et al also curate a set of independent variables that plausibly explain Russia and Ukraine's position as cybercrime hubs. But they have left out other variables that might be an asset for the model. There are a number of standard variables that could be suited to comparison across countries, including general economic indicators. There are also some more specific variables that could warrant inclusion, like (cyber) law enforcement capacity across countries.

In short, the authors have identified a fruitful approach, but there is a need to formalise it by carrying out a regression. Two elements are required to do this. First, an index of cybercriminality by country needs to be developed in order to allow for a genuine dependent variable to be deployed. Second, a more comprehensive set of independent variables need to be drawn together. Once this is done, the data can speak for itself.

Following McCombie, Nir Kshetri was the next scholar to engage with the concept of cybercrime hubs. Kshetri [11] is also focused on a range of topics, and the idea of ranking cybercrime hotspots is but one of many concerns (see also [12]). A contribution provided by his book *The Global Cybercrime Industry* is an attempt to rank the top sources of cybercrime between 2002-2004 and then also 2007. Rather than beginning with the supposition that certain countries are the leading proponents of cybercrime (e.g. Russia and Ukraine), Kshetri provides rankings of states based on a number of points of interest, including: locations where most fraud originates; percentage of fraudulent orders on US sites; attack metrics; malware creation and hosting; spam; phishing websites; and victim complaints.

On its face, there is value in Kshetri's approach. First, he seeks to rank countries to some degree, rather than only seeking one or more exceptional cases. While he does later seek some broad understanding of the "characteristics of the source nation" (p. 142), a baseline metric of cybercriminality must be established initially, which he has done to a degree. Second, Kshetri's rankings are drawn from publicly available data. This is important in establishing an empirical foundation for any future analysis. Finally, this data appears to indicate that developing rankings on the broad category of cybercriminality itself is challenging. Data is more likely to be found on specific types of cybercrime, rather than cybercriminality in general. There are also likely to be different measures that could be used, so some thought must be given to this before any future ranking system is established.

There are also areas where this preliminary analysis has significant limitations. The tables provide only 10 or so countries per category, rather than an extensive list of states, which would aid further quantitative analysis. The tables that Kshetri produces are reproductions, with some inconsistencies, of publicly available data that appears largely drawn from government (e.g. Internet Crime Complaint Center – IC3) and industry (e.g. Symantec and Sophos) reports, sometimes as cited in media articles. There is little assessment made of the reliability and/or validity of these data for academic purposes. Some relevant issues herein are that the IC3 is the US government organisation for cybercrime reporting. It should be noted as particularly US-centric and tied to victim reports. As such, it should not be surprising that the US easily ranks at the top of this list. Threat reports from cybersecurity companies should also be regarded with some scepticism, considering that little is known of the 'science' of how they determine the country source of an attack. There may also be commercial benefit in inflating certain cybercrime statistics. While Kshetri makes some attempt to rank countries by cybercrime measures, the attribution methodology of the data he relies on should be interrogated.

To this point, the scholar who has most seriously investigated the ranking of cybercrime hubs and what factors are likely driving these rankings is Alex Kigerl. Kigerl [13] provides some relevant remarks on the means of measuring which countries are "high in cybercrime", and the challenges therein:

One [approach] is to measure where most cybercriminals live in physical space. Surely, some countries are home to more cybercriminals than others. The second means of measuring high cybercrime countries is to determine from which nations cyberattacks are coming from. For instance, which countries host the most phishing servers, which are the source of most spam messages, and which countries contain the most botnet zombies. Where the cybercriminals live is not necessarily

where the cyberattacks are coming from. An offender from Romania can control zombies in a botnet, mostly located in the United States, from which to send spam to countries all over the world, with links contained in them to phishing sites located in China. The cybercriminal's reach is not limited by national borders (p. 473).

Kigerl goes on to note that while the location of cybercriminals themselves is probably the most significant element, this is also very difficult to determine, particularly in a quantifiable way. One possible measure is language used when compiling malware, whether English, Russian, Chinese or otherwise (p. 474). But this will not narrow down to a specific country. This would also only speak to malware production, and not other aspects of cybercrime. Rather than proceeding down this more challenging path, Kigerl outlines the simpler tasks of tracking cyber attacks rather than cybercriminals:

While it is important to know where cybercriminals reside, it is much easier to measure from where cyberattacks originate across the globe. Many cyberattacks travel across the Internet, and in order to get anywhere on the Internet, routers and servers must know the transmission's address in cyberspace at one point during a message's transit through a network. Cyberattacks are digital in nature, consisting of data that reside, at least temporarily, on computers. Determining where cyberattacks come from is simply a matter of acquiring these data. Fortunately many firms, especially cybersecurity companies, have tremendous amounts of these data. Cybersecurity firms that sell spam filters can track spam; firms that distribute antivirus software can track malware; and companies that offer website security can track attacks on those websites. These cyberattacks can be geolocated to specific countries (p. 474).

Unfortunately, in the subsequent analysis he carries out, Kigerl adopts this second simpler method. He attempts to bring a theoretical and predictive rigor to this approach, beyond what cybersecurity companies are already offering in this space. But while he notes that it's "possible that there exists a relationship between cyberattack source and cybercriminal source" (p. 475), this appears to be largely in contradiction to his earlier statements.

Despite this central challenge, Kigerl should be commended for engaging with this subject in a serious way, and for grappling with the complexities of quantitative analysis on a topic that has few detailed and reliable datasets suited to such an effort. By moving past a conceptual level discussion, Kigerl illustrates the challenges of building a cybercrime metric, and then carrying out analyses that engage with this metric. This requires a serious effort, as part of a systematic work program.

Kigerl incorporates a range of variables into his model, but for theoretical reasons he is chiefly interested in three: Internet users per capita, unemployment rates, and international cybercrime law enforcement and cooperation. He develops some broad findings of potential interest including that the percentage of Internet users in a country has a positive association with spam (p. 481), and that the interaction between unemployment rate and Internet users per capita has a significant association with spam (p. 482).

But if our foundational interest is in the measure of cybercrime, this model fails. Kigerl doesn't have a measure of cybercrime itself, but rather for sub-categories of spam and phishing. These are drawn from NGO datasets (pp. 476-477). These measures are built into the model, but not illustrated as a distinct metric. Yet even if we were interested in spam and phishing as proxies of cybercrime, as noted, Kigerl is a victim of the trap that he laid for himself. As he makes clear during the paper:

Both [spam and phishing] are not measures that can confidently be assumed to represent cybercriminal country of origin. Ideally, these measures would represent the cybercriminal's location, but the next best thing would be the cyberattack location. There is a chance that much of the spam data represent cyberattack location or where spambots, botnets, or servers used to send spam are located. However, the IP addresses assumed to be the location from which spam is sent can be spoofed, but it is not certain how much is falsified in this way (p. 482).

Kigerl is particularly suspicious of the data on Phishing top-level domain (TLD) rate: "While spam is thought to originate from botnets and other spam sending servers, it is less clear how phishing TLDs relate to location. Some countries do not require citizenship to register a TLD associated with them, so the fact that a TLD represents a location (a country) is purely artificial" (p. 478). This is an important point. Nearly all jurisdictions have opened up their domains to international purchasers, which means they can be exploited by cybercriminals (for instance, the use of .co for Columbia looks very similar to .com).

In a later paper, Kigerl [14] moves slightly closer to dealing with the metrics of cybercriminality in more detail, although this is again not the direct focus. The central aim of this second paper is to classify countries within cybercrime categories, using multivariate quantitative analysis. This article takes a similar approach to Kigerl's past work in that he uses the same source of spam messages from the archives of Untroubled Software, though for a later period. In this case, he categorises these messages by phishing scams, advance fee fraud, malware distribution, and non-serious spam. Kigerl similarly returns to the use of phishing domains as another proxy for fraud, despite his prior statements questioning the validity of such data. For this later paper, he also incorporates BitTorrent tracker data as a measure of countries where piracy is common, along with a similar variable of file sharing client downloads per capita (for further details see pp. 151-156).

Kigerl develops some interesting findings, which reinforce the point that cybercrime is not monolithic. There are different types of cybercrime and different countries may specialise in some of these types but not others: "Nations were assigned to one of four clusters, including low cyber crime countries with low GDP and internet connectivity, advance fee fraud

specialist nations, with modestly low connectivity; non-serious cyber crime nations, high in piracy and email spam and that were the wealthiest with the most internet users, and phishing specialist countries, also with high internet connectivity but average wealth" (p. 162). Kigerl may not go far enough, as there are likely even more categories of cybercrime, including credit card fraud, extortion, various "cashing out" operations and a range of hacking/intrusion offences that would not appear in the datasets he gathered. In future studies, significant thought should be given to all the types of cybercrime and whether/how these could be grouped together and operationalized.

But while this 2016 paper contributes to the broader discourse, it suffers from the same weaknesses that Kigerl identified in his earlier work. It does not have a true measure for cybercrime, or more specifically various sub-categories of cybercrime. The underlying technical data most likely do not provide the degree of attribution required to capture the true location of the offenders behind the attacks. For all the methodological labors, in the first instance we need a baseline measure of cybercrime that has greater internal validity.

Work by Lusthaus may be the most recent research in this broad space. But it also goes nowhere near developing a metric or ranking of countries according to cybercriminal activity. Based on hundreds of interviews with law enforcement agents, security professionals and former cybercriminals, Lusthaus [1] proposes a number of known cybercrime hotspots. But this list is limited: the former Soviet Union states; Romania; Nigeria; China; Brazil; and countries of the West, such as the USA, which are known for the monetary aspects of cybercrime (pp. 68-78). This is a longer list than the two countries provided by McCombie and colleagues (see also [15](pp. 6-7)), but it suffers from the same deficiencies in not providing a extensive country ranking that could be used in quantitative analysis. There are also similarities with Kigerl's findings, in that it is noted that there are specific cybercrime specialties found in particular countries, which are tied to local socio-economic conditions. In short, cybercrime is not a universally uniform phenomenon. Expanding this type of approach, Lusthaus [5] develops the beginnings of a model of cybercrime development to qualitatively isolate which elements may predict a heavy cybercrime presence within certain countries. But there remains considerable quantitative work to be done if a true metric on cybercrime is to be constructed.

B. Law Enforcement and Industry Reports

Moving past the extremely sparse academic literature, one has to be open to the possibility that public and private sector reports may provide a more detailed and effective response to the research question. Unfortunately, this also is not the case. In law enforcement reports, this topic is rarely addressed. Probably the most relevant work on this comes from Europol's annual Internet Organised Crime Threat Assessment Reports. Each year up to 2018, the report featured a section on the "Geographic Distribution of Cybercrime". But the countries are not formally ranked, and the focus is largely on regions as a whole with occasional country examples discussed. For instance, the 2018 report stated: "The Americas, particularly the USA, continue to be both a key originator of global cyber-attacks and a target for cyber-attacks originating both domestically and from overseas"; "Similar to the USA, Brazil is also a top host of phishing sites, with some reporting putting Brazil as one of the world's top ten originators of all cyber-attacks" [16](p. 66). Meanwhile, the 2017 report notes a somewhat non-hotspot: "As in previous years' reports, while Oceania still suffers from cybercrime internally, it does not often feature in EU investigations" [17](p. 69). The 2016 report [18] identifies Nigeria (p. 59), China (p. 60) and Russia (p. 61) as key drivers of particular types of cybercrime in their regions.

Such reports clearly do not provide detailed answers on cybercrime rankings. But, interestingly, they also rely primarily on open source data and/or data from industry rather than being exclusive presentations of law enforcement information. This draws us back to a discussion of the industry reports that were addressed in Kigerl's work. These reports are plentiful and do engage with cybercrime rankings in the most direct and detailed way. In fact, there are so many of these reports that, unlike the academic literature, they need to be discussed only in overview (see, for example [19]). These reports are produced by a range of major companies – for example Akamai and Symantec – on an annual or even quarterly basis. They often draw on data collected internally, though neither the data nor methods are commonly discussed in much detail. It is rare that they provide a comprehensive ranking of all countries, often limiting themselves to, for instance, top 10 or top 20 lists. It is also rare to provide an overall cybercrime metric. Reports commonly focus on specific types of cybercrime and provide rankings accordingly. These vary widely: bots; credential stuffing; malicious activity; phishing; spam; web-based attacks and so on.

While these reports most directly address the task of ranking countries by cybercriminality, they are perhaps the least reliable of all the available categories of research. As noted, they rarely discuss data and methods in necessary detail. There are also general questions about the function of these reports, which appear to fall within the marketing matrices of these companies and may be tied to the commercial offerings they provide. But their biggest failing is the one identified by Kigerl: what these companies primarily capture is technical data on various types of cybercrime that likely does not reflect the true location of the attackers themselves [14](p.147). As cybercriminals often carry out attacks across national boundaries, may collaborate with partners around the world, and can draw on infrastructure based in different countries, superficial measures do not capture the true geographical distribution of cybercrime.

To be credible, any data that is used must contain a level of attribution. Attribution is very challenging, often labor intensive, and may require different techniques in particular cases [20]. Investigators carry out this function as part of their roles in law enforcement and private companies. But, unless the cases are linked to court proceedings or high profile matters,

attribution is rarely made public due to various sensitivities. The large troves of data that are used to compile rankings in these reports necessarily cannot include this high level of attribution. While these data stockpiles are convenient to use, they are not a valid measure of cybercriminal geography. If they are a measure of anything, they are a measure of cyber-attack geography. The utility of this type of measure is less clear.

C. Coda: Aggregation of Rankings

We have attempted to aggregate some of the findings from the above categories of research. We gathered together as many public sources as we could find that provide some kind of ranking of cybercrime hubs. In total, we collected 65 publications of relevance, and then counted each instance where a country appeared in a numerical list that ranked countries by cybercrime offending. This could be cybercrime as a whole, or particular subcategories like spam, phishing or malware. These lists often appear in reports and other publications as "Top 10 Countries where Cybercrime Originates", "Worst Countries for Spam", and so on. Table 1 aggregates the top 25 countries, based on the frequency in which they appeared in these published lists.

Given our above analyses, we believe there is a range of questions concerning the validity of published data on this subject. As a result, this table should not be read as a meaningful measure of cybercrime. It instead better reflects some of the biases built into existing attempts to rank countries by cybercriminality. Most notably, it appears that the highest ranked countries are also known for having the most significant Internet infrastructure. While it is possible that Internet infrastructure and cybercrime are correlated, it seems more likely that this table has captured the core obstacle to successfully measuring cybercrime by country: the technical data used are much more likely to capture aspects of the attacks themselves, and the components of the Internet that they pass through at various points. They are much less likely to capture the true location of where the attacks originated, and where the cybercriminals themselves are located.

TABLE I

Frequency of Countries Appearing in Cybercrime Ranking Lists		
Rank	***Country***	***Frequency***
1	USA	65
2	China	57
3	Germany	55
4	France	47
5	UK	43
6	Russia	38
7	Canada	35
8	Japan	31
9	Italy	30
10	Netherlands	27
11	South Korea	25
12	Brazil India	21
13	Taiwan	18
14	Spain	17
15	Ukraine	14
16	Vietnam	13
17	Poland	12
18	Turkey	9
19	Indonesia	8
20	Singapore Sweden	7
21	Mexico Argentina	6
22	Ireland Israel	5
23	Australia Egypt Hong Kong Malaysia	4
24	Colombia Hungary Kuwait Thailand	3
25	Australia Ecuador Finland Iran Philippines Romania UAE	2

III. Lessons Learned and Ways Forward

The core finding coming out of this review is that developing a country-level index on cybercriminality is a challenging task. The tiny literature on this subject is somewhat indicative of this. But even those few studies that touch on the concept of a cybercrime ranking largely skirt the issue. Some like McCombie and Lusthaus focus on identifying a small number of hotspots. Others, like Kshetri and Kigerl, rely on existing datasets that should serve as proxies for different aspects of cybercrime. But, as authors like Kigerl note, these types of technical data should be treated with skepticism as they do not reflect the true origin of various cybercrime enterprises, and the people behind them. This is the core failing of industry reports, which offer the most direct attempts to rank countries by cybercrime measures. Law enforcement reports also provide scant details.

A fully-fledged work program is required to progress this study appropriately. There is tremendous value in developing a reliable and valid cybercrime metric. By accurately identifying which countries are cybercrime hotspots, the public and private sectors could concentrate their resources, and avoid spending time and money on cybercrime countermeasures in countries where the problem is minimal. As Lusthaus and Varese [4] note: "While the victims can be thousands of kilometres away and surely need to be vigilant, cybercrime also needs to be tackled in the places where it originates" (p. 8).

There are potentially three ways forward in developing an effective measure of cybercrime by country. The first is to persist with the use of technical data. This could involve the continued use of existing datasets from NGOs and the private sector, but with an extremely clear-eyed focus on selecting the best proxies and perhaps developing clever workarounds to clean the data and give it a greater fit for purpose. Such an effort would probably involve the close collaboration between

social scientists and computer scientists. A related option would be that academics collect their own technical data on cybercrime. This might be done through the use of honeypots or otherwise. These efforts would have to be similarly focused on ensuring that such data speaks to the true origin of the cybercriminals, and not some intermediary aspect of their technical architecture.

The second data source that may be relevant to developing a cybercrime index is legal data. In this case, court records, indictments and other investigatory materials speak more directly to attribution. Where investigations and prosecutions lead to the identification of offenders, something more can be said about their location. The detail is far more granular. But the challenge with this type of data is scaling up. It is well suited to micro-level analysis and case studies. At a macro-level, the key weakness is how representative these specific cases can be.

Finally, based on the issues raised in this paper, one promising way forward in attempting to rank cybercriminality by country is survey data. No appropriate survey currently exists, so one would need to be specifically developed. Interviews with investigators and offenders have been very valuable in providing broad insights on cybercrime, particularly when other forms of (technical) data have not been available on a certain point (e.g. offline cybercriminal interactions) or where that data is very noisy and difficult to operationalize (for examples see [1], [3]). But while interviews provide micro-level detail or general overviews, they are not suited to systematically building a cybercrime ranking. What is needed is a means to similarly tap into expert knowledge, but in a way that is suited to constructing an index.

Conducting an expert survey would have a number of advantages. First, unlike interviews, survey data can be extrapolated and operationalized. Second, attribution can remain a key part of the survey, as long as the participants in the sample have an extensive knowledge of cybercriminals and their operations. Third, a survey can sketch a more complete picture of the geographical distribution of cybercrime because it draws on broader investigation and intelligence knowledge, rather than only prosecuted cases.

REFERENCES

[1] J. Lusthaus, Industry of Anonymity: Inside the Business of Cybercrime, Cambridge: Harvard University Press, 2018.

[2] R. Leukfeldt, E. Kleemans, and W. Stol, "Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks", British Journal of Criminology, vol. 57, no. 3, pp. 704–722, 2017.

[3] A. Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission", Crime, Law and Social Change, vol. 62, no. 1, pp. 1–20, 2014.

[4] J. Lusthaus, and F. Varese, "Offline and local: the hidden face of cybercrime", Policing, vol. Online First, pp. 1–11, 2017.

[5] J. Lusthaus, "Modelling cybercrime development: the case of vietnam", The Human Factor of Cybercrime, R. Leukfeldt and T. J. Holt, eds., Abingdon and New York: Routledge, 2020.

[6] N. Rayman. "The world's top 5 cybercrime hotspots", May 8, 2020; https://time.com/3087768/the-worlds-5-cybercrime-hotspots/.

[7] Bloomberg. "Top ten hacking countries", May 7 2019, 2019; https://www.bloomberg.com/slideshow/2013-04-23/top-ten-hacking-countries.html.

[8] J. Cook. "The world's 10 biggest cybercrime hotspots in 2016, ranked", May 8 2020; https://www.businessinsider.com.au/worlds-10-cybercrime-hotspots-in-2016-ranked-symantec-2017-5?r=US&IR=T

[9] C. H. News. "Top 10 countries with most hackers in the world", May 8 2020; https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e.

[10] S. McCombie, J. Pieprzyk, and P. Watters, "Cybercrime attribution: an eastern european case study", in Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia, 2009.

[11] N. Kshetri, The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives, Berlin: Springer, 2010.

[12] N. Kshetri, "Cybercrimes in the former soviet union and central and eastern europe: current status and key drivers", Crime, Law and Social Change, vol. 60, no. 1, pp. 39–65, 2013.

[13] A. Kigerl, "Routine activity theory and the determinants of high cybercrime countries", Social Science Computer Review, vol. 30, no. 4, pp. 470–486, 2012.

[14] A. Kigerl, "Cyber crime nation typologies: K-Means Clustering of Countries Based on Cyber Crime Rates", International Journal of Cyber Criminology, vol. 10, no. 2, pp. 147–169, 2016.

[15] N. Phair, Cybercrime: the reality of the threat, Kambah, ACT: Esecurity Pub, 2007.

[16] EC3, Internet Organised Crime Threat Assessment, Europol, The Hague, 2018.

[17] EC3, Internet Organised Crime Threat Assessment, Europol, The Hague, 2017.

[18] EC3, Internet Organised Crime Threat Assessment, Europol, The Hague, 2016.

[19] N. Phair. "State of the nation: a snapshot of the online threat environment", May 12 2020; http://www.centreforinternetsafety.com/storage/ThreatReportmarkupversion_6b_C8.pdf.

[20] J. A. Shamsi, S. Zeadally, F. Sheikh, and A. Flowers, "Attribution in cyberspace: techniques and legal implications", Security and Communication Networks, vol. 9, no. 15, pp. 2886–2900, 2016.