Beneath the Dark Web: Excavating the Layers of Cybercrime's Underground Economy

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

***Abstract*—The Dark Web or DarkNet has attracted both considerable media and scholarly attention. This forms part of a broader tradition of analyzing relatively open cybercriminal marketplaces and forums. With the aid of data collected over a 7-year period, the focus of this paper is to help demarcate - beyond the Dark Web alone - all the layers within the world of profit-driven cybercrime. These include: 1) the top layer, which is the most open forums and marketplaces, whether Dark Web or otherwise; 2) the middle layer of more closely vetted forums; 3) the bottom layer of even smaller and more closed groupings; 4) the molten core, which is centered on the offline organization of cybercrime. The purpose of this analysis is to identify key aspects of the underground economy which warrant further scholarly attention, and to suggest possible approaches to engage with these subjects going forward.**

***Index Terms*—cybercrime, Dark Web, forums, marketplaces, underground economy, offline dimension, social science**

I. Introduction

The Dark Web or DarkNet has attracted both considerable media and scholarly attention. While some use either term as a catchall for online malfeasance in general, others take a narrower view. If the Clear Web is the Internet of the average user, the Dark Web is hidden from view by way of anonymity platforms like Tor or I2P. While IP addresses are hidden, these sites are not difficult to access in practice, as long as users employ, for instance, Tor themselves [1]. The Dark Web is also best distinguished from the Deep Web, which is not indexed by standard search engines [2].

But even by limiting the scope of what is considered part of the Dark Web, it occupies increasingly large amounts of academic investigation [3-5]. This forms part of a broader tradition of analyzing relatively open cybercriminal marketplaces and forums [6-8]. As the most visible element of cybercrime, along with data that can be easily collected through scraping, this seems like a logical place to focus attention. But while the iceberg tip is certainly worthy of study, we shouldn't ignore what lies below the surface. For a more comprehensive understanding of cybercrime, researchers also need to focus attention on the other layers of this underground economy.

With the aid of data collected over a 7-year period, the focus of this paper is to help demarcate these layers within the world of profit-driven cybercrime. It begins with an overview of the top layer, which is the most open forums and marketplaces, whether Dark Web or otherwise. The second layer is those forums and marketplaces that are more closely vetted, and that not anyone can view or join. Below that is the third layer of even smaller and more closed groupings. Finally, there is the molten core, which is centered on the offline organization of cybercrime and is not always present in digital data at all. The purpose of this analysis is to identify key aspects of the underground economy which warrant further scholarly attention, and to suggest possible approaches to engage with these subjects going forward.

II. Data and Methods

Before proceeding to the focus of this paper, a brief discussion of data and methods is required. This paper forms part of a much larger research project, carried out over a 7-year period [9]. The project was focused on the organization of profit-driven cybercrime and was primarily qualitative and fieldwork based. It involved semi-structured interviews with 238 participants in 20 countries. Visited countries included key suspected cybercrime hotspots, such as Russia, Ukraine, Romania, China, Nigeria, Brazil, and the United States. Across these fieldwork locations, interviews were carried out with current and former law enforcement agents, security professionals from the private sector and former cybercriminals. This cybercriminal sample was geographically diverse and included a spectrum from low-level offenders to those involved in the highest echelons of the business. Where possible, interviews were conducted in person, though some had to be done remotely through calls, writing and messaging.

The broader research project, along with this present paper, is exploratory in nature and its findings should be viewed as suggestive. The scope is considerable, as the study attempts to "map" the global cybercrime underground, rather than engage with much more specific research questions or case studies. While the interview sample is large for a qualitative study, it is too small for meaningful quantitative analysis and is not random. Participants were accessed through purposive or snowball sampling. It is also important to note that, while the semi-structured interviews touched on key themes each time, the specific focus and points of discussion varied depending on the expertise of each participant, rather than being built around a detailed standardized questionnaire. Interviewees came from many different backgrounds, countries and professions. Some

could offer information on, for instance, the structure of Russian-speaking malware groups, whereas others had limited knowledge of these topics as they might be an expert on Nigerian advance fee fraud or American cash out operations instead. As such, the interviews are best suited to citation in an illustrative way, which is the tradition that is followed throughout this paper.

While fieldwork has not been widely applied to cybercrime, there is a long tradition of it within the social sciences. A number of successful studies have applied similar methodologies to conventional criminal groups [10-12]. An interview-based approach is also slowly emerging within the cybercrime literature [13, 14]. Such approaches appear well suited to investigating cybercrime and can offer both macro and micro level insights that might not always be available through other data.

All interviews are reported anonymously, in order to protect participant identities. Real names have been replaced with pseudonyms, unconnected to the participants' true identities. Along with pseudonyms, a distinct code has been assigned to each subject, to allow for in-text citation. To explain how the codes can be understood, an example would be US-LE-4. This would mean this person is based in the US and is a law enforcement agent. The number implies they were the fourth person of this kind interviewed in the study. There are a couple of further complexities if a participant is formerly of a listed profession (F), or is an expatriate in the listed country (E). For subjects of a cybercriminal background, regional rather than country signifiers are used. For instance, SEA(E)-(F)CC-1 would mean this person is based in Southeast Asia, but is an expatriate rather than a local. They are a former cybercriminal, and the first of this type that I interviewed as part of the project.

Table I and Table II contain the country/regional signifiers, as well as the profession signifiers. They also provide information on the distribution of the participants, by geography and profession respectively.

Along with the interviews, supplementary data was also gathered from other sources, including legal documents, forum archives, copies of chat logs, and open source material.

TABLE I
DISTRIBUTION OF PARTICIPANTS (GEOGRAPHY)

Code	Meaning	Number of Participants
AUS	Australia	8
BRA	Brazil	9
CHN	China	7
EE	Eastern Europe	5
GER	Germany	1
HK	Hong Kong	7
IND	India	3
INT	International	6
IRE	Ireland	2
KOR	South Korea	5
LAT	Latvia	3
MY	Malaysia	8
MENA	Middle East and North Africa	1
NA	North America	5
NLD	Netherlands	4
NIG	Nigeria	15
RDT	Redacted	5
ROM	Romania	16
RUS	Russia	18
SA	South America	1
SEA	Southeast Asia	3
SGP	Singapore	6
SWI	Switzerland	2
THA	Thailand	4
UDL	Undisclosed	2
UK	United Kingdom	24
UKR	Ukraine	10
US	United States	41
VN	Vietnam	13
WE	Western Europe	4

TABLE II
DISTRIBUTION OF PARTICIPANTS (PROFESSION)

Code	Profession	Number of Participants
A	Academic	1
CC	Cybercriminal	20
CSP	Cybersecurity Professional	97
FSP	Financial Sector Professional	11
H	Hacker	4
ITP	IT Professional	4
J	Journalist	3
LE	Law Enforcement Agent	72
OO	International Organization Officer	6
P	Prosecutor	15
RDT	Redacted	5

III. THE TOP LAYER: OPEN FORUMS AND MARKETPLACES

The most visible layer of the cybercrime industry is large, open sites. Some are chiefly discussion forums centered on networking and the sharing of information, while others are far more commercially focused. With its founding in 2011, Silk Road began a new period of Dark Web sites. Their profile has grown significantly since this point. But while these sites have attracted much attention, from a social and economic perspective little has changed from the online illicit marketplaces that came before. They all still largely operate like criminal eBays [15]. As noted above, these sites might be "hidden," but access is not difficult for those with a Tor browser. Once inside, these marketplaces operate surprisingly openly. In fact, some interview subjects were quite dismissive of these sites, which they believed were catering to a lower level of cybercriminal, perhaps offering lower quality services or goods (US-LE-10, NA-(F)CC-2).

The Dark Web fixation can also obscure the sustained presence of many marketplaces and forums that continue not to use Tor or other platforms to "hide." In fact, a number of leading Russian-speaking sites do not make use of such technology. Perhaps these actors don't require an off the shelf solution to protect themselves, as they have other technical fixes. But they may also feel insulated within their jurisdictions. The Dark Web has clearly become an important part of the open access scene, but other sites still remain in this space. Generally

these Clear Web sites offer only limited protections to their members, the threat of scams are ever-present and the wares are often inferior than those to be found in more closed communities (NA-(F)CC-2, SEA-(F)CC-2, UKR-CSP-1).

There are not too many analytical points to made in this section, as both Dark Web sites and other open access, or easily accessible (i.e. through simple registration), sites are embedded throughout the academic literature on cybercrime. In some sense it has defined this literature over the past decade. We have seen qualitative analyses [6]; we have seen quantitative analyses [16]. We have seen the investigation of both English and Russian language forums [17]. We have seen studies based on cybercriminal trust and reputation in these networks [5, 7], and assessments of law enforcement operations designed to disrupt these groups [3, 4]. We have also seen a range of different theoretical frameworks applied across these journal articles.

For a relatively niche sub-discipline, there is a surprisingly large literature on these open forums. The state of the literature suggests that a good deal of foundational work has been carried out and the basic dynamics of these forums are now fairly well understood. As a result, going forward it seems that the focus of research on this most open layer of the underground economy is best suited to addressing new questions and applying novel methods. There are certain fields in the social sciences where many researchers make use of the same data, or the same types of data. This is the case when exploiting standard publicly available surveys as a primary mode of research; scholars have to work on developing interesting research questions and applying methodological innovations to drive the field forward. This may be the fate of the cybercrime field if it remains strongly focused on open access data. But there also remain other research approaches available in the organizational layers of cybercrime that are hidden below the surface.

IV. The Middle Layer: Vetted Forums and Marketplaces

If there were no law enforcement pressure on cybercriminals, open forums and marketplaces would likely dominate. But with that threat, some feel the need to operate within closed settings. A number of the former cybercriminals that I interviewed were aware of law enforcement presence on forums and took care as a result (NA-(F)CC-2, NA-(F)CC-3, NA-(F)CC-4, EE-(F)CC-2). While joining a closed marketplace does not eliminate this threat, it does ensure some vetting of members. This process may also present a hurdle to "rippers" who wish to scam other cybercriminals.

Perhaps the most common system for vetting prospective members is to require that existing members of the community vouch for them. The standard procedure is that two vouchers are required (UKR-CSP-1, NIG-(F)LE-1, RUS-CSP-5, RUS-CSP-6), though certain sites might require even more referees and/or may also require that these users have been long-standing members of the group (UDL-CSP-1). To limit insincere references, sites may hold vouchers accountable for any misconduct of a new member. These referees may have to help cover the victim losses in the event of a scam, or be banned themselves (UDL-CSP-1, NA-(F)CC-2). This vetting process is designed to show that the community is a safe place to do business. Though, of course, it is far from a perfect system as some scams still occur, and some law enforcement agents can still penetrate these closed marketplaces.

The other key mechanism for regulating membership is by charging a membership fee (RUS-CSP5, RUS-CSP-6, US-LE-2, SEA-(F)CC-2, UKR-(F)LE-2). Some sites can charge large fees, while others are surprisingly small (e.g. 100 USD). These smaller amounts may seem trivial, but in practice they can meaningfully regulate membership. For instance, even a small sum might be too much for a "noob" or young student to justify. And while law enforcement agents could have such a payment cleared internally, some private security companies have rules of engagement that prevent any money at all being paid to cybercriminals (IRE-CSP-2, NLD(E)-CSP-1).

North American former cybercriminal, Scott, explained the importance of these closed forums (NA-(F)CC-2). During his time of operation, he felt there was "too much heat" on the forum scene and "had already made a bunch of contacts and didn't really have a need for the forums any longer." Later on he rejoined the forum scene, as most of his partners had disappeared by this point. But some caution still remained and many cybercriminals he knew were scared to be on larger, more open forums. Instead, Scott and his confreres were attracted to marketplaces that were "more 'elite' in general and more 'closed' so I guess people felt they were more safe" (NA-(F)CC-2). Providing more detail on this layer of underground, he wrote:

> *As for the more "elite" closed forums, etc., there was really nothing different about them at the time other than it was just more secretive among the known people that were trusted for a while. Some were only known to people in their "inner circle." Some only were for Russians etc.. . . As for the number of members on some of the other forums . . . I don't remember for sure but we are talking numbers in the 100's as opposed to 1000's. . . . I remember one hacking forum with as low as 80-something members, I think (and some of those are multiple logins from same people I'm sure) (NA-(F)CC-2).*

Even among these closed forums, there appears to be a scale. While a number of sites might vet members, other limitations might include regulating the size of the overall membership or limiting the linguistic background of community. Maksym, a Ukrainian security professional with a detailed knowledge of the forum scene, argued that the space in between very open and very closed marketplaces is probably the most active in terms of collaboration and trade (UKR-CSP-1). These middle sites likely have somewhat experienced members, but can still operate relatively openly. Extremely closed forums might put such a premium on trust and caution that less commercial activity actually goes on. These groups

might also limit the size of the membership, which could lead to less "new blood" to drive the trade forward and purchase products (RUS-CSP-5, RUS-CSP-6).

The academic literature on closed sites is far less extensive than the literature on open forums. There is a simple reason for this: the data is not often easily accessible. Academic researchers would have great difficulty entering these sites because they themselves would need to be vouched in and would need some criminal bona fides or deception to do this. It seems unlikely that this wouldn't raise red flags during ethics and risk assessment applications. As a result, the literature in this area has so far focused on databases of leaked forums [18]. Dupont and colleagues have analyzed perhaps the most significant closed forum so far in the form of Darkode, which also derived from a leaked source [19].

In terms of driving research forward on this layer of the underground economy, there are two possible avenues. Researchers could continue to mine leaked archives. There are limitations on the data that is out there, but there are certainly leaked databases that have yet to be analyzed or fully analyzed. One complication with this approach is that, because researchers are not gathering the data themselves, they need to take extra care in determining how complete the dataset is and/or whether it might have been manipulated through the leaking process. For instance, one common weakness with forum data (both top and middle layers) is that it only shows public facing interactions, whereas deals and other communications are often conducted through personal messages or commonly off the site altogether (US-LE-2).

The other avenue for accessing data on closed forums might be through law enforcement contacts or those companies that have managed to gain access to these more elite forums. This presents its own challenges, and many organizations may refuse to release such data for research. But it is certainly worth exploring. If such data might be released, there would be a tremendous upside in terms of shining a light on these shadowy forums and gaining a far more nuanced understanding of how they operate.

V. The Bottom Layer: Closed Groups

Marketplaces and forums are the most visible part of the cybercrime ecosystem. But it would be wrong to think that they are the only organizational cog within the underground economy. As noted by former cybercriminal Scott, there is significant distrust of forums by a segment of the cybercriminal community (NA-(F)CC-2). While some retreated to smaller more elite marketplaces, others left the forum scene altogether and have gone further underground (US-LE-10).

Other cybercriminals had never truly engaged with forums in the first place. For example, Western European former cybercriminal Sean put matters this way:

I never got involved in the ShadowCrew side of things. I found that to be . . . there was more structure and business behind it. I didn't like it very much. That was more for the lower level carders. Whereas I was in a completely sort of different realm to them. So I didn't get involved in that . . . (WE-(F)CC-1).

Another former cybercriminal, Dave, was equally suspicious of the people who populated forums:

They wouldn't have the connections, which means they don't have the reputation, which means they haven't impressed someone. So it's pretty easy in the Internet, when you start getting good at anything in an illegal field, you start making friends and you impress people then get into those circles . . . . So I worked always with someone who came from a mutual recommendation, so someone else recommended them, "this guy's good." So to meet some guy random on the Internet, "I don't know you from a bar of soap. So, no way" (SEA(E)-(F)CC-1).

The core function of forums appears to be networking. Some scholars view them as "convergence settings" for online offenders [20, 21]. But the collected data suggest that once one has enough contacts, it's possible just to engage directly with these partners. Others may seek chat groups, which are smaller and more personal than forums, allowing cybercriminals to work only with those that are well known and already trusted. In the present day, Jabber is a very common platform being used by cybercriminals (US-LE-2, UDL-CSP-1, NLD(E)-CSP-1, US-(F)LE-1). It is often employed with a combination of social protections, such as small group size with only trusted members, along with technical measures like encryption and VPNs. With this development, the organization of cybercrime has returned somewhat to its roots. Before forums took hold, chat groups through IRC or otherwise were a common mechanism for hackers and then cybercriminals to meet and engage. One security professional noted both the importance of Jabber, along with the recent rise of apps like Telegram for illicit trading, which he noted is "almost a step back to the more real time IRC days" (IRE-CSP-2).

Within this bottom layer is not only chat group channels, but also operational groupings of cybercriminals. These individuals may have specific channels to coordinate their activities, or they may coordinate through more direct communications. In reality, cybercriminal group structures are like crews or firms, where each member has a specific role to play. Taking malware groups as an example, it appears that these online structures can be limited in size, usually between three and eight people (UDL-CSP-1, UK-CSP-2, UKR-CSP-1). Maksym, the Ukrainian security researcher, provided an example of how a group might be structured that is centered on developing malware. While there is variation across the industry, this example centered on the author of the code, who is the key organizer. This boss may also employ a programmer to assist with aspects of the coding, who would be kept on salary. S/he would also employ one or more vendors to sell the product in marketplaces or otherwise. These vendors are often salaried, but can also make sales commissions (UKR-CSP-1).

Eastern European former cybercriminal Ivan also wrote about the structure of these operational groupings: "if you already know reliable people (i.e. have a "private team"), you can easily move to IM and PGP type of communication with them, without ever bothering to visit a forum whatsoever–why bother if you are already making decent money?" (EE-(F)CC-3).

Of course, cybercriminal group structures vary widely and are often suited to the specific type of business these crews are engaged in. The main point is that marketplaces and forums are only one type of organizational structure. They are centered on networking and trading. But studying these formations tells us little about the groups that actually carry out cybercrime. Even closed chat groups that are based around trading, don't always speak directly to the groups that carry out cybercrime. There are reasons that some components of a commercial activity are brought inside the firm, rather than seeking all services and goods in the market [22]. There also needs to be an acknowledgement of where the goods and services traded in online marketplaces come from in the first place.

The bottom layer of the underground economy is probably the one that has been least investigated by scholars. This is because these structures are far less visible and the data is difficult to obtain. There has been some discussion of IRC type groups that have been around since earlier days [23-25], but little work has been done on the more secretive, and often protected, Jabber groups that have become more widespread in recent times. While studies of traditional organized crime have already engaged in analyses of criminal firms [12, 26], the cybercrime literature has been largely silent on the subject of operational groups that carry out attacks and scams. In order to take this research area forward, serious thought must be given to how to obtain data on these closed groups. With persistent difficulties with accessing these groups and scraping data, engagement with law enforcement might be a point of exploration, and has led to the release of some data in the past already [23]. Interviews with law enforcement agents, offenders and others might also be a method for shedding further light on this bottom layer of the online cybercriminal industry.

VI. The Molten Core: Offline Groupings

Many often think of cybercrime as a virtual and online phenomenon. Digital data has also been the focus of most cybercrime literature up to this point (see the above sections). But the often-ignored reality is that there is a significant offline dimension within cybercrime. A number of offenders appear to know each other in person, and in certain cases operate together in the physical world.

Cash-out crews are very commonly offline structures. This seems rather intuitive, as these groups often move between ATMs withdrawing cash with counterfeit cards, or make purchases inside shops. There is a strong physical component, requiring a degree of monitoring from the leader of the group (NA-(F)CC-2). In a number of cases, the boss of such groups will also recruit known associates, who they might trust already and who might have an existing criminal background (WE-(F)CC-1, NA-(F)CC-2, UKR-CSP-3).

This offline dimension is not limited to the less technical aspects of the cybercrime business, but can also be found among those involved in hacking or malware too. For example, there are not only online "teams" like those described by Ivan above. But there are also teams of cybercriminals physically working together and rooted in specific locations around Eastern Europe (EE-(F)CC-2). These teams are often centered on a key leader and a geographical hub. Eastern European former cybercriminal, Andrey, believed that such teams have included centers like Odessa, Moscow, Donetsk and Sebastopol (EE-(F)CC-2).

In certain cases, offline structures become so entrenched that they even begin to look like technology companies. In one 2012 example, a number of arrests were made in Moscow, against a group exploiting the Carberp malware to steal money from online bank accounts. The leaders of the group were two brothers who were running the operation out of rented office space, with the outward appearance of a start-up [27]. On an even larger scale was the well-known cyber boogieman, the Russian Business Network (RBN). Effectively an ISP for criminals offering bulletproof hosting, RBN had a physical base in St. Petersburg with both an office and salaried employees [28, 29]. In a similar vein, Liberty Reserve was a start-up that ran a virtual currency platform. But its user-base was also largely criminal. With around 50 employees, it operated out of business-park in Costa Rica. It's neighbors were companies like Hewlett Packard and Western Union [30].

In some parts of the world, offline organization even appears to be dominant over digital coordination between offenders. For instance, online auction fraud is a popular criminal endeavor in parts of Romania. The schemes are often conducted by groups, rather than individuals, which are embedded in the physical world and often centered on geographical hubs within the country. These groups have clear hierarchies and a division of roles (ROM-(F)LE-1, ROM-(F)LE-2, ROM-LE-1). This is found in the separation between those who carry out the fraud, and those money mules (known as "arrows") who are responsible for getting the gains back to the scam organizers (ROM-(F)LE-1, ROM-(F)LE-2, ROM-LE-1). Offenders often come from trusted groupings and may be from the same communities (ROM-P-1).

Nigerian cybercrime is also strongly rooted in the physical world. These offenders are most famous for the 419 or advance fee fraud scams (NIG-(F)LE-1, NIG-CSP-1, NIG-LE-6). But in recent years, they have also branched out into other areas. The structure of these operations was originally built around Internet cafes, but with the rise of mobile access, the importance of these locations has diminished (NIG (F)LE-1, NIG-ITP-1). Nigerian offenders appear quite loosely structured, but are fairly dependent on existing personal relationships. In a number of cases, these cybercriminals may be connected through past schooling or other social ties (NIG-(F)LE-1, NIG-LE-6). They continue to value in-person relationships even when they move overseas and operate scams from other

countries (MY-LE-3, US-P-2, NLD-LE-1, NLD-LE-2, UK-LE-2, US-LE-9, US-LE-10 US-(F)LE-6, IND-(F)LE-1).

While this offline layer of cybercrime might be near invisible to those researchers who focus on digital forms of data, a niche literature is starting to emerge. Leukfeldt and colleagues have noted that online forums play a limited role within cybercrime and that "social ties" play a significant role within cybercrime groups [20, 31, 32]. Lusthaus (and Varese) have also investigated the importance of the offline dimension of cybercrime. In particular, they have examined how cybercriminal networks are often rooted within geographical hubs, where offenders are often a product of their environments [13, 15].

This niche literature has shown the value of trying to investigate this seemingly hidden component of cybercrime. In terms of driving research forward in this area, it's not so much that new approaches are required but that we need greater application of old approaches. These works are quite closely linked to existing methods in the study of organized crime more broadly [10, 11, 33]. They show that use of police files and other legal data, along with interviews and fieldwork, can be effective in driving knowledge forward in this space. But what these initial works have identified is that the offline dimension of cybercrime is surprisingly large. The forms of data and methods required to study it are also very time-consuming. As a result, to better understand this deep "core" of the underground economy, a much larger concentration of researchers is required to get involved in collecting data in this space and analyzing it.

VII. Conclusion

This paper has outlined the distinct layers of social and economic organization within the world of cybercrime. It has highlighted that conventional scholarly approaches are primarily focused on just one layer of the underground economy. This is the top layer of open-access (or easy to access) forums and marketplaces, which is associated with the concept of the Dark Web. While some might argue is it dark or hidden, in research terms this layer is actually the most visible component of cybercrime, with the easiest to access data.

Beneath the Dark Web, the other layers of the underground economy should not be ignored. There are gaps in the literature and considerable terrain for scholars to explore. Directly underneath the open forums are the middle layer of vetted forums and marketplaces, which generally contain more cautious and professional operators. Even more cautious are those who eschew forums, but choose to operate in the bottom layer of the underground economy within much smaller closed groupings, using platforms like Jabber. Finally, the molten core of cybercrime appears to be the offline dimension, where a surprising number of offenders collaborate in person.

All of these layers are worthy of study and addressing them will drive knowledge forward in the field. It is important to understand that they all contribute to the overall cybercriminal enterprise and each must be investigated to gain a clear picture of the whole. It is also important to understand the interactions between these strata, particularly the ways that offenders might move between them, perhaps throughout distinct stages of their criminal careers. An assessment of the relative damage/costs caused by each layer of the underground may also help focus intervention strategies going forward. Additionally, studying how interventions against one layer might (or not) displace offenders to another part of the underground would be a worthy topic.

In the upper layers of cybercrime, attention is best placed on developing interesting questions and innovative methodologies. For instance, one topic that could be further explored through both qualitative and quantitative methods is how individuals make use of the formal mechanisms provided by forums and marketplaces to enhance trade, and how effective these mechanisms are in practice. As we move down into the depths, the challenge is far more about uncovering and accessing useful data in the first place. There are very many research questions that could be addressed in these layers, including a better understanding of: the structures of operational groupings; the motivations/tactics of offenders; and how cybercriminals connect with the traditional criminal world and their broader context. While research into attackers and cybercriminal operations is growing, there is no shortage of work still left to do.

Acknowledgment

This research benefitted greatly from the guidance and support of Federico Varese. I am also grateful to countless others who provided assistance and advice throughout the project. But chiefly I am indebted to the participants in this study, who were extremely generous with their time and knowledge, and who made this project possible. Part of the fieldwork for this study was carried out as a Clarendon Scholar. Nuffield College, the John Fell Fund, and the Commonwealth Bank of Australia also provided valuable support. Finally, I thank UNSW Canberra Cyber for their partnership in the Human Cybercriminal Project.

References

[1] "Hacker Lexicon: What is the Dark Web?" https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, [Online; accessed 20-February-2019].

[2] J. Madhavan, D. Ko, L. Kot, V. Ganapathy, A. Rasmussen, and A. Halevy, "Google's Deep-Web Crawl," in PVLDB , pp. 1241–1252, 2008.

[3] D. Decary-Hetu, and L. Giommon, "Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous," Crime, Law and Social Change, vol. 67, no. 1, pp. 55–75, 2017.

[4] I. Ladegaard, "We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets," British Journal of Criminology, vol. 58, no. 2, pp. 414–433, 2018.

[5] W. Przepiorka, L. Norbutas, and R. Corten, "Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs," European Sociological Review, vol. 6, no. 1, pp. 752–764, 2017.

[6] T. Holt, and E. Lampke, "Exploring Stolen Data Markets Online: Products and Market Forces," Criminal Justice Studies, vol. 23, no. 1, pp. 33–50, 2010.

[7] B. Dupont, A. Cote, C. Savine, and D. Decary-Hetu, "The Ecology of Trust among Hackers," Global Crime, vol. 17, no. 2, pp. 129–151, 2016.
[8] T. Holt, "Examining the Forces Shaping Cybercrime Markets Online," Social Science Computer Review, vol. 31, no. 2, pp. 165–177, 2013.
[9] J. Lusthaus, Industry of Anonymity: Inside the Business of Cybercrime, Cambridge: Harvard University Press, 2018.
[10] M. Sanchez-Jankowski, Islands in the Street. Berkley and Oxford: University of California Press, 1991.
[11] F. Varese, The Russian Mafia: Private Protection in a New Market Economy. Oxford: Oxford University Press, 2001.
[12] D. Gambetta, The Sicilian Mafia: The Business of Private Protection. Cambridge and London: Harvard University Press, 1993.
[13] J. Lusthaus, and F. Varese, "Offline and Local: The Hidden Face of Cybercrime," Policing, vol. Online First, pp. 1–11, 2017.
[14] 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.
[15] J. Lusthaus, "Honour Among (Cyber)thieves?," European Journal of Sociology, vol. 59, no. 2, pp. 191–223, 2018.
[16] D. Decary-Hetu, and B. Dupont, Reputation in a Dark Network of Online Criminals," Global Crime, vol. 14, no. 2-3, pp. 175–196, 2013.
[17] T. Holt, O. Smirnova, Y. T. Chua, and H. Copes, "Examining the Risk Reduction Strategies of Actors in Online Criminal Markets," Global Crime, vol. 16, no. 2, pp. 81–103, 2015.
[18] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. Voelker, "An Analysis of Underground Forums," in Internet Measurement Conference, pp. 71–79, 2011.
[19] B. Dupont, A. Cote, J.-I. Boutin, and J. Fernandez, "Darkode: Recruitment Patterns and Transactional Features of the Most Dangerous Cybercrime Forum in the World," American Behavioral Scientist, vol. 61, no. 11, pp. 1219–1243, 2017.
[20] R. Leukfeldt, E. Kleemans, and W. Stol, "The Use of Online Crime Markets by Cybercriminal Networks: A View From Within," American Behavioral Scientist, vol. 61, no. 11, pp. 13871402, 2017.
[21] M. Soudijn, and B. Zegers, "Cybercrime and Virtual Offender Convergence Settings," Trends in Organized Crime, vol. 15, no. 2-3, pp. 111-129, 2012.
[22] R. Coase, "The Nature of the Firm," Economica, vol. 4, no. 16, pp. 386–405, 1937.
[23] B. Dupont, "Skills and Trust: A Tour Inside the Hard Drives of Computer Hackers," Crime and Networks, C. Morselli, ed., pp. 195–217, New York: Routledge, 2014.
[24] J. Lusthaus, "Trust in the World of Cybercrime," Global Crime, vol. 13, no. 2, pp. 71–94, 2012.
[25] C. Herley, and D. Florencio, "Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy," Economics of Information Security and Privacy, T. Moore, D. Pym and C. Ioannidis, eds., pp. 33–53, Boston: Springer, 2010.
[26] P. Reuter, Disorganized Crime: The Economics of the Visible Hand. Cambridge, Mass; London: MIT Press, 1983.
[27] "Eight Arrested in Moscow After Allegedly Stealing Millions Using Carberp Trojan." http://www.securityweek.com/eight-arrested-moscow-after-allegedly-stealing-millions-using-carberp-trojan [Online; accessed 20-February-2019].
[28] J. Graham ed., Cyber Fraud: Tactics, Techniques, and Procedures. Boca Raton: CRC Press, 2009.
[29] B. Krebs, Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door. Naperville: Sourcebooks, 2014.
[30] "Bank of the Underworld." http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/ [Online; accessed 20-February-2019].
[31] 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.
[32] R. Leukfeldt, "Cybercrime and social ties," Trends in Organized Crime, vol. 17, no. 4, pp. 231–249, 2014.
[33] E. Kleemans, and C. D. Poot, "Criminal careers in organized crime and social opportunity structure," European Journal of Criminology, vol. 5, no. 1, pp. 69-98, 2008.