CRIMINOLOGY
RESEARCH GRANT

Darknet drug traders: A qualitative exploration of the career trajectories and perceptions of risk and reward of online drug vendors

Rasmus Munksgaard
James Martin

Report to the Criminology Research Advisory Council
Grant: CRG 50/16–17

October 2020

This project was supported by a Criminology Research Grant.
The views expressed are the responsibility of the author and are not necessarily those of the Council.

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: www.aic.gov.au/crg

ISBN 978 1 925304 67 1 (Online)

This research was supported by a Criminology Research Grant. The views expressed are those of the author and do not necessarily reflect the position of the Criminology Research Advisory Council or the Australian Government.

This report was reviewed through a double-blind peer review process.

Edited and typeset by the Australian Institute of Criminology.

Contents

Figures

Acronyms and abbreviations

DNM	darknet market
DNS	domain name system
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
NPS	new psychoactive substance
OOBV	online-to-online buyer–vendor
OPSEC	operational security
PGP	Pretty Good Privacy (encryption)

Abstract

A growing share of drug distribution takes place through cryptomarkets—illicit online drug markets which supply the lower levels of the drug trade. Though the economy at large is well understood and the motivations and demographics of buyers as well, the population of drug sellers has received less scrutiny. In this study we address this research gap through the largest qualitative study of cryptomarket vendors to date.

We find that sellers begin their careers in varying ways, some moving their business online, others moving into cryptomarket distribution from buying, reselling or supplying friends or from other cybercrimes. We further observe that economic and non-economic motivations frequently overlap, and that strategies for managing risk vary extensively. We conclude with a discussion of our findings from a policy perspective, focusing on the implications for policing drug markets and health policies.

Introduction

Since the launch of Silk Road in 2011, cryptomarkets—also known as anonymous online markets (Christin 2013; Soska & Christin 2015) or darknet markets (Broséus et al. 2016)—have become the subject of media attention and scholarly research. They have matured into a small, though no longer negligible, component of illicit drug markets in the 21st century. Despite intense transnational law enforcement efforts, involving seizures, prosecutions and arrests around the world, including in Australia, cryptomarkets have continued to grow, showing considerable resilience and potential for lasting growth.

Predominantly, research on cryptomarkets has taken a quantitative approach using data collected through automated processes to examine the frequency and volume of sales, origin, vendors and more (for an overview, see Martin, Cunliffe & Munksgaard 2019). Qualitative studies have examined in depth the behaviour and motivations of buyers through interviews (Bancroft & Reid 2016a, 2016b; Barratt et al. 2016; Van Hout & Bingham 2013), and functioning and practices through ethnographic analysis of open sources (Bakken, Moeller & Sandberg 2018; Ladegaard 2018; Moeller, Munksgaard & Demant 2017; Morselli et al. 2017). To date, only one study has involved interviews with vendors, with a total of 10 participants (Van Hout & Bingham 2014). Vendors are a critical component of the cryptomarket ecosystem, and the lack of research into vendors as a population suggests a significant research and knowledge gap. This study seeks to rectify this by conducting the largest qualitative study of this population to date.

Literature review

The online trade in illicit drugs has expanded significantly in recent years. This growth is due in large part to the emergence of cryptomarkets: anonymous online forums 'where goods and services are exchanged between parties who use digital encryption to conceal their identities' (Martin 2014a: 356). These peculiar 'darknet' websites are a recent innovation, with the first massively popular cryptomarket, the infamous and now defunct Silk Road, commencing operations in 2011 (Barratt 2012). Since then, dozens of other cryptomarkets have emerged that trade in all manner of illicit goods and services, from computer hacking and stolen credit card information to pornography and unlicensed firearms. (Pornography is typically sold as logins to various websites hosting adult content. However, we note that cryptomarkets do not host child sexual exploitation material and typically will forbid any such content; Martin 2014a, 2014b.) By far the largest product category traded on cryptomarkets is illicit drugs (Christin 2013; Dolliver 2015; Soska & Christin 2015). The online trade in illicit drugs has particular relevance to Australia, which currently has the dubious honour of hosting more online drug dealers per capita than any other country except the Netherlands (Martin 2018).

Aside from the illegality of the goods and services typically traded on cryptomarkets, these websites function in much the same way as legitimate 'surface web' trading sites such as eBay and Amazon. They provide virtual meeting places for thousands of drug dealers to advertise their wares and connect with potential customers, thereby facilitating a vast global network of illicit exchange. Online drug deals are carried out using an intriguing combination of highly sophisticated and simple technologies, with user identities and locations concealed from authorities through the use of digital encryption and electronic currencies, while goods are delivered, with deceptive simplicity, to customers via traditional 'snail mail' postal networks or courier services (Martin 2014a, 2014b).

The proliferation of cryptomarkets presents a fascinating area of inquiry for criminologists, computer scientists, drugs researchers and other scholars seeking to understand how new technology is impacting the global illicit drugs market. In the four years since Barratt first brought Silk Road to the attention of academia (2012), a further 45 studies have been published on the topic of cryptomarkets. The steadily growing repository of studies in this area includes a recently published 'cryptomarket special edition' of the *International Journal of Drug Policy.* The studies feature a diverse range of research methodologies, from quantitative surveys (Barratt, Ferris & Winstock 2016; Barratt et al. 2016) and qualitative, in-depth interviews conducted with online drug vendors, law enforcement, consumers and site administrators (Barratt et al. 2016; Lavorgna 2014; Maddox et al. 2016; Tzanetakis et al. 2016; Van Hout & Bingham 2014, 2013) to theoretical and conceptual analyses based on direct, unobtrusive observation (Martin 2014a, 2014b).

Academics with programming skills are also innovating sophisticated technical solutions to gathering data online, most notably through the development of software 'crawlers' (Aldridge & Décary-Hétu 2016, 2014; Christin 2013; Décary-Hétu, Paquet-Clouston & Aldridge 2016; Demant, Munksgaard & Houborg 2016; Dolliver 2015; Soska & Christin 2015). These powerful and technologically sophisticated research tools automatically collect and sort publicly available information that is hosted by cryptomarkets (eg vendor names, product prices and textual and numerical customer reviews). Crawler data has also been shared between researchers across a number of scholarly disciplines and, in some instances, has been made publicly available, thereby facilitating innovative quantitative and qualitative archival analysis (see, for example, Munksgaard & Demant 2016; Martin 2018). Other recent additions to the scholarly literature in this area include studies exploring the ethical and methodological dimensions of cryptomarket research (Barratt & Maddox 2016; Martin 2016; Martin & Christin 2016).

As in many fields of research, quantitative cryptomarket research and qualitative cryptomarket research are interrelated and inform one another in a reflexive and ongoing iterative process. Qualitative research helps to define the objects of study, articulating new concepts and theories and identifying prominent issues for further consideration. Quantitative research provides numerical and representational validity, often in relation to qualitative research, and assists in testing hypotheses. An example of this interaction across methodologies with regard to cryptomarket research is neatly revealed by studies conducted by members of the research team: Dr Martin's research monograph (Martin 2014b) identified, among other issues, that political ideology plays a prominent role in discussions on cryptomarket forums. This issue was explored in a subsequent quantitative study conducted by Munksgaard and Demant (2016), who used textual analysis of crawler data to track how political discourse on cryptomarkets has evolved and shifted in response to significant events, such as the unexpected closure of a site at the hands of law enforcement.

As a qualitative study involving the use of encrypted interviews with cryptomarket participants, this project is informed by similar darknet ethnographic research conducted by: Barratt et al. (2016); Maddox et al. (2016); Tzanetakis et al. (2016); Lavorgna (2014); Moeller, Munksgaard and Demant (2017); and Van Hout and Bingham (2014, 2013). Of these studies, only one (Van Hout & Bingham 2014) involved interviews with online dealers, highlighting the under-researched nature of this population. The Van Hout and Bingham (2014) study examined the nature of vendor experiences in the early days of Silk Road and offered important insights into why cryptomarket vendors commenced their online offending. This project is intended to build on this previous research, delving deeper into questions about vendor perceptions of risk and reward within contemporary cryptomarkets, and aims to inform current debates and facilitate further scholarly inquiry into the online illicit drugs trade.

Cryptomarkets

Cryptomarkets are, at their most basic, organisationally decentralised market platforms, similar to legal platform enterprises such as eBay, Etsy and Uber, wherein goods and services can be exchanged directly between buyers and sellers on a platform controlled by a central authority (Barratt 2012; Martin 2014a, 2014b). As in their licit parallels, administrators charge a commission but remain otherwise uninvolved in the actual sales, which are between individuals and firms ('vendors') operating on their websites. In exchange for a commission, administrators provide dispute resolution, escrow systems and critical technical infrastructure, including storefronts and private message functionality (Christin 2013; Martin 2014a, 2014b; Moeller, Munksgaard & Demant 2017; Morselli et al. 2017). Unlike their licit parallels, however, cryptomarkets face the challenge that they and the activity on them are illegal. Consequently, additional security measures must be taken to ensure user anonymity. The key innovations made to stay secure are the use of technologies for encryption and anonymisation: namely, Tor, Bitcoin and PGP encryption.

Cryptomarkets typically use the Tor network, also known as the 'darknet', to disguise the location of the server hosting the site and anonymise and encrypt user traffic (Dingledine, Mathewson & Syverson 2004; Jardine 2016; Spitters, Verbruggen & Staalduinen 2014). Use of Tor precludes many of the enforcement strategies typically employed against illicit online content, such as ordering the website to be taken down by the host or blocking it on a DNS level (Goldsmith 2000; Hutchings & Holt 2017). Because of this, cryptomarkets cannot immediately be blocked or shut down, though law enforcement has succeeded in some cases (Décary-Hétu & Giommoni 2017). At the level of financial transactions, cryptomarkets use cryptocurrencies—principally Bitcoin and other alternatives like Monero, Ethereum and Litecoin—to avoid financial regimes of money laundering control and supervision (Böhme et al. 2015; Martin 2014b). Using cryptocurrencies, cryptomarket users are able to circumvent traditional payment channels (eg credit card institutions, banks and intermediaries), which could otherwise compromise, curtail or inform on their activity. Finally, cryptomarket users are encouraged to use PGP encryption when sending sensitive information (Bancroft & Reid 2016a; Demant, Munksgaard & Houborg 2016). Doing so ensures that, if the website is seized by law enforcement, sensitive and identifying user information cannot be accessed.

The cryptomarket economy

Since the launch of Silk Road in 2011, the cryptomarket ecosystem has demonstrated continuous growth and resilience against law enforcement interventions (Christin 2013; Décary-Hétu & Giommoni 2017; Soska & Christin 2015). Silk Road was originally launched with some self-imposed regulations as to what products could be sold (Ormsby 2014). These excluded from sale goods and services which were considered harmful to others (eg weapons, child sexual exploitation material and stolen data), and the majority of economic action was centred on the distribution of illicit drugs (Aldridge & Décary-Hétu 2014; Martin 2014a, 2014b). Following the seizure of Silk Road, an increased overlap between markets for stolen data (eg stolen credentials and credit card information) was observed by both community members (DeepDotWeb 2015) and researchers. The sale of stolen data and other non-physical products (eg bespoke malware) is now typical, though illicit substances still constitute the majority of product sales (Soska & Christin 2015).

Contrary to the pre-existing online trade in new psychoactive substances (NPS) (Brunt et al. 2017; EMCDDA & Europol 2016; Kjellgren & Jonsson 2013), cryptomarkets predominantly trade in well-known drugs such as cannabis, cocaine, MDMA and methamphetamine, with cannabis and MDMA being responsible for between 30 percent and 50 percent of all generated revenue (Aldridge & Décary-Hétu 2014; Demant, Munksgaard & Houborg 2016; Soska & Christin 2015). In terms of quantity, scholars have found that the majority of cryptomarket transactions are small, falling within thresholds of personal supply and social supply, but that trade in large quantities on the scale of redistribution generates significant proportions of the revenue (Aldridge & Décary-Hétu 2014, 2016; Demant, Munksgaard & Houborg 2016). For example, Aldridge and Décary-Hétu (2016) observed that products priced above US$1,000 generated a quarter of the revenue on Silk Road, while 49 percent of products were priced below US$100. Thus, cryptomarkets predominantly supply well-known illicit substances for personal consumption.

In the context of global drug markets, cryptomarkets remain relatively small in scope in terms of pure economic indicators. However, from cryptomarkets' nascence, scholars have pointed towards their transformative potential, as the platforms allow buyers and sellers to transcend the geographical limitations of local drug markets and trade on an international platform (Aldridge & Décary-Hétu 2016; Martin 2014a, 2014b). Given the skewed economics of drug markets, wherein price and quality often vary significantly across minor distances (Reuter & Caulkins 1998), this might encourage traders to use cryptomarkets to buy and sell drugs across, rather than within, different regions. However, scholars have found that economic activity on cryptomarkets is predominantly concentrated within a few Western nations and is often domestic or regional rather than transnational in nature (Décary-Hétu, Paquet-Clouston & Aldridge 2016; Demant, Munksgaard & Houborg 2018; Dittus, Wright & Graham 2018; Dolliver, Ericson & Love 2016; Tzanetakis 2018).

Cryptomarket vendors

As detailed above, there is comparatively little qualitative research on cryptomarkets, and only Van Hout and Bingham (2014) have interviewed vendors. Consequently, most knowledge about cryptomarket vendors stems from quantitative research and is often premised on known but unverified assumptions (see, for example, Soska & Christin 2015). While the study by Van Hout and Bingham (2014) provides indispensable knowledge, the population and environment studied in 2014 differ significantly from the contemporary cryptomarket scene. (We note that several of our interviewees reminisced fondly about the 'old days' and described those times as qualitatively different.) Firstly, cryptomarkets have grown considerably since this study (Soska & Christin 2015) and, secondly, the interviewees operated on Silk Road, which was a cryptomarket established for political ends and thus the cultural and social context is not immediately comparable to that of the current scene, which has grown less political (Munksgaard & Demant 2016).

The population of vendors who distribute drugs on cryptomarkets is relatively small and often phases in and out of activity. In the most recent study of the largest cryptomarket, AlphaBay, Tzanetakis (2018) found 2,188 drug vendors, of which 1,750 had made at least one sale over a period of one year. The study found that, at the market's period of peak activity, 922 drug vendors were active at the same time. Similarly, Soska and Christin (2015) found that vendors were active for short periods of time, with half being active for less than 220 days. The scope of economic activity among vendors differed extensively, with some vendors registered on cryptomarkets never making one sale. Tzanetakis (2018) found that 21 percent did not exceed US$1,000 in sales during their lifetime and 57 percent did not exceed US$10,000. A small fraction of vendors, however, generate large revenues. Depending on the measurement used, Tzanetakis (2018) sets US$200,000 as a limit, finding only five percent in this category, while Paquet-Clouston, Décary-Hétu and Morselli (2018) use a more sophisticated measure and find one percent qualify as 'high-level' vendors. These findings are congruent with previous studies (Christin 2013; Soska & Christin 2015). In addition to being relatively small and highly stratified, the vendor population also exhibits specialisation, with most vendors selling only a few categories of substances (Paquet-Clouston, Décary-Hétu & Morselli 2018).

Aims

While quantitative research has identified broad characteristics in the vendor population, studies invariably remark on the relative complexity of the subject and discuss some obvious caveats. Soska and Christin (2015) caution that their findings on the lifespan of vendors' profiles cannot detect if a vendor has changed pseudonym (ie username), which could be a reasonable defence against law enforcement detection. Similarly, the findings from Tzanetakis (2018) and Paquet-Clouston, Décary-Hétu and Morselli (2018) do not concern the absolute revenue of vendors but only that which is observable on the cryptomarket through digital trace analysis. It might well be that, after developing some trust in each other, vendors and buyers move to other means and begin to transact outside the observable market system, escrow and commission, in what are known as 'direct deals' (Barratt et al. 2016). By extension, topics such as motivations for selling drugs online, dealers' careers, and perceptions and management of risk cannot be adequately examined quantitatively. In other words, there are aspects of cryptomarket drug distribution which quantitative research is simply not fit to study using current methods and approaches. Thus, while cryptomarket research has advanced significantly in past years, a key demographic—vendors—remains relatively under-studied. This suggests a critical gap in the current knowledge of cryptomarkets, because the behaviours and profiles of vendors are a key component of the cryptomarket economy: vendors supply the products, set the prices and are largely responsible for the positive and negative experiences of customers.

This study took an exploratory approach to understanding this population of offenders and was centred on the 'career trajectories' of vendors. Little is known about what motivates these individuals to operate on cryptomarkets to start with, and the study therefore addresses a basic question concerning motivation and attraction to this mode of drug dealing. From this, we extended into other related and more specific themes: vendors' relation and engagement in traditional drug markets, conceptions of risk and practical aspects of managing it, and practical aspects of starting up an operation and day-to-day business practices. This approach sought to allow sellers to articulate their motivations without restricting them to one particular frame (eg choosing cryptomarkets exclusively as a means of risk reduction), in recognition of the heterogeneity of drug-dealing careers and motivations (Coomber 2006; Sandberg 2012; Dwyer & Moore 2010).

This project therefore aims to generate new understanding regarding:

- the career trajectories of online dealers, including whether dealers are either currently or formerly involved with conventional illicit drug trading;
- the motivations for selling drugs online, incorporating attitudes to both financial and non-financial rewards (eg thrill, status);
- how risks are perceived and managed by online dealers, including those posed by both law enforcement and predatory criminals (eg fraudsters, hackers, extortionists); and
- how dealers perceive efforts to police online drug trading, including through targeted (ie online investigations) and non-targeted operations (eg border interdiction).

Method and data

We conducted 13 semi-structured qualitative interviews between March 2017 and March 2018 with cryptomarket vendors, the largest cohort of vendors in the literature. There is only one other study in which vendors are interviewed (Van Hout & Bingham 2014). This semi-structured approach was chosen in recognition of the differentiation in motivations which we expected to observe. Recruitment was aided by gatekeepers to the community: namely, the unofficial news website for the cryptomarket community, DeepDotWeb, and the author of the book *Silk Road*, Eileen Ormsby (Ormsby 2014). Both posted a call for participants that also included a description of the research team and previous work. Interviewees would contact the research team through communication channels described in the call. Two interviews were marked as incomplete: one was based on a pilot interview guide; in the other, the interviewee stopped responding.

All participants were offered compensation of A$40 in Bitcoin or Monero. Recognising the issues of a lack of anonymity in Bitcoin transactions, Monero was offered as an alternative and interviewees were also offered the opportunity to donate their compensation to a charity. The majority chose to donate the reciprocity payment to the charity of their choosing. Only two respondents took the donation for themselves, whereas the remainder declined, donated to a charity or wanted it sent to a third party. From our conversations, we suggest that the vendors chose these options because of the relatively small size of the compensation as opposed to their revenues.

Paquet-Clouston, Décary-Hétu and Morselli (2018) use a classification of vendors in which 90 percent, nine percent and one percent represent small-, medium- and large-scale vendors. We used an ad hoc classification of our sellers, in which those with a yearly revenue above $100,000 were considered large scale, those above $10,000 were considered medium scale and the remaining were small scale. We discussed this classification with vendors, and two were comfortable being classified as ‘large scale’. While we did not seek to elicit background and demographic information, only one interviewee presented as female, whereas the remainder to a greater or lesser extent presented as male. With the exception of one vendor, all mentioned operating out of Western countries, congruous with the patterns of supply and demand on cryptomarkets (Tzanetakis 2018). Seven of the 13 vendors revealed a history of having dealt offline, through social supply, retail or larger quantities. While the cohort of respondents contained large-, medium- and small-scale vendors from the most active regions in the cryptomarket drug trade, the recruitment strategy is likely to have privileged some segments of the population: namely, those who follow the media used for communicating the call to respondents and those who are proficient in English.

To ensure the safety of participants, we followed practices for encrypted communications used in previous research interviewing cryptomarket buyers and vendors (see Barratt et al. 2016; Van Hout & Bingham 2014), improving slightly on some aspects (namely, the use of an amnesiac operating system by the research team). In practice, we established multiple avenues of communication (email, asynchronous chat and private messages) over which informants could contact the research team and kept all data (transcripts, passwords and logins) on an isolated operating system with full disk encryption. Further, we instructed interviewees not to discuss operational details such as their packaging methods ('stealth') or money-laundering methods in a manner that could jeopardise them. Interviews were conducted using the medium preferred by the interviewees, which included asynchronous communication (eg email and private message) and synchronous solutions (eg instant messaging). The estimated length of interviews was intended to be one to two hours, but synchronous interviews would often become significantly longer, as vendors would be doing their job at the same time (eg packaging, talking to customers and handling complaints). Often, these chats would take place over several days so as not to interfere too much with each vendor's business.

Interview questions were framed under a notion of career trajectories and covered vendors' careers chronologically, taking detours into themes such as risk from law enforcement and malicious peers, practical aspects of their organisation, and interactions and relationships with customers, while the crux of each interview was the motivations for selling drugs on cryptomarkets. Despite the broad and general scope of these questions, we did not experience vendors declining to answer any questions, though the level of detail provided varied.

Ethical concerns about this research centred on the maintenance of anonymity for research participants. As noted above, the research team went to significant lengths to ensure this. Ethics approval for this project was granted by the Macquarie University Human Research Ethics Committee in December 2016.

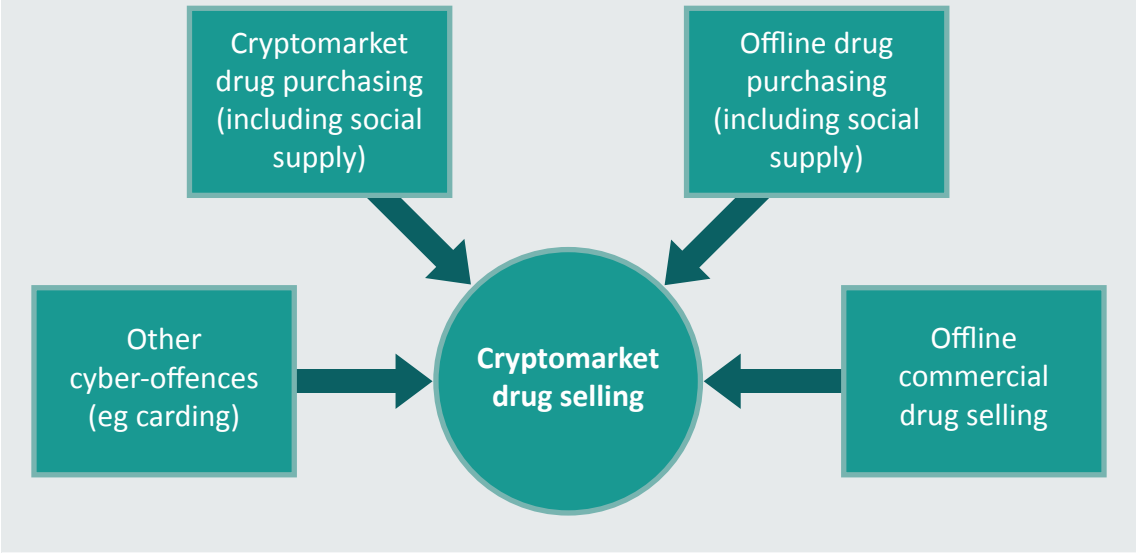
Findings

In the following sections, we illuminate central themes addressed in the interviews with cryptomarket vendors. These themes were informed by our interview questions, which were crafted to elicit information about career trajectories, material and non-material motivations, pathways, and perceptions and management of risks, building on earlier research from Van Hout and Bingham (2014). The structure of this section is 'chronological', in the sense that we begin with motivations and introductions to the darknet drugs trade, after which we analyse the ongoing careers of vendors.

Career trajectories

One of the principal aims of this research was to determine how online dealers became involved in this form of offending. Given the qualitative nature of this research and the relatively small sample size, we do not claim that the career trajectories presented below are representative of this population of offenders as a whole. However, our sense is that the different factors that shape online dealer career trajectories are likely to be common, though further research will be required to validate this assumption.

Figure 1: Pathways to cryptomarket drug supply



Cryptomarket drug purchasing

Interviewees reported a variety of career pathways into the cryptomarket drugs trade. One of the most common factors that precipitated online vending was experience accessing a cryptomarket to acquire drugs for personal consumption. Several respondents described their initial exposure to the 'cryptomarket scene', as a buyer in the first instance, as a vivid and informative experience. Interviewees discussed being attracted to the technology comprising the cryptomarket ecosystem (Bitcoin, Tor, etc) and being impressed with the simplicity of using cryptomarkets to purchase drugs, the relatively cheap prices for consumers compared to offline sources of drug supply, and the profitability that was readily apparent for vendors:

> Interviewee 12: Two years before I began vending I bought [drugs via cryptomarkets]. Never once had a problem. I would simply find a vendor with high reviews, follow protocol and get my package. Every time it was simple. Which is partially why I started vending.

> Interviewee 8: I've always been fond of The Internet…so I knew it was possible to find other ways [to buy drugs] at that time and started to find our stuff on it. Prices were good, bitcoin was easy at that time and we definitely had a lot of fun.

> Interviewee 4: I bought [drugs via cryptomarkets] for a couple of years before I basically switched roles entirely. Only buying never selling… One of the main reasons I made the switch was because I saw the potential bitcoin had. And I simply had a desire for money more than I did for drugs. Simple as it sounds…[I] saw an opportunity to make an extra buck essentially.

Offline drug purchasing (including social supply)

The interviewees above each described a relatively slow transition from buyer to seller, taking place over several years. This slow transition or 'drift' from drug consumer to commercial cryptomarket vendor was, in several cases, mediated by an additional stage, which involved the non-commercial social supply of drugs to friends and acquaintances. In most cases, the involvement in social supply occurred prior to accessing cryptomarkets. The perceived difference between commercial and non-commercial drug supply was starkly revealed by one interviewee who, when questioned about the difference between supplying drugs after acquiring them from offline sources compared with supplying them from cryptomarkets, provided the following response:

> Interviewee 8: Actually I couldn't give you a lot of differences about selling on DNMs and how I dealt before because I never dealt before! Of course I was providing friends and maybe friends from friends. But that was a very closed circle. I started [selling drugs] on DNMs.

This seemingly self-contradictory statement reveals a deeply held, though legally tenuous, belief that is also common among offline dealers (Coomber 2006): that only commercially motivated sales to strangers constitute 'real' drug dealing. Social supply, on the other hand, was perceived as a largely altruistic act, intended to merely help 'sort out' people who lacked the necessary connections to secure their own drugs independently. While the interviewee above was quick to reject the notion that they were previously involved in drug dealing, other interviewees with a history of social supply were less particular about avoiding labelling their prior dealing in this manner, as evidenced by the quotations from two separate cryptomarket vendors below:

> Interviewer: You dealt offline as well?
>
> Interviewee 12: Yes, just to friends mostly. Or I'd sell bulk as they'd do the leg work.

> Interviewer: So first off I'm curious about getting started. You began on Silk Road?
>
> Interviewee 3: Yep. Silk Road was the first cryptomarket I sold on. I sold offline and through other mediums before that though.

Offline commercial drug selling

In all, approximately half of our respondents (7 out of 13) reported selling drugs for either commercial or non-commercial social supply purposes before commencing their online vending. Some of these interviewees reported purchasing drugs via cryptomarkets and then 'on-selling' surplus product back onto cryptomarkets, while others bought and sold drugs in larger quantities via interpersonal, offline networks only. Notably, only two continued selling drugs offline once they had properly established their online vending enterprise, with the majority discontinuing interpersonal drug sales in favour of selling via cryptomarkets.

The typical rationale for preferring online drug sales was that they were perceived to be more profitable and significantly less risky than offline dealing (vendor perceptions of risk are discussed in more detail in the section below). As a result, the shift from offline to online-only drug supply was perceived to reduce the psychological stress of mitigating the various hazards inherent to offline dealing (transporting drugs to retailing locations, interacting with and revealing one's identity to customers, etc):

> Interviewee 4: I sold weed mostly before [commencing selling on cryptomarkets]. Bought on DNMs and locally and sold to frat houses primarily. It got too crazy though. Rumours came back to me and ransoms figured me out so I quit. Plus weed smells so much and I was always paranoid about mailing stuff and driving etc.

It is important to note that the psychological stress of selling drugs via cryptomarkets, while unanimously perceived as preferable to offline dealing, was also described as taxing, particularly in the early stages, when vendors were unfamiliar with managing the various hazards of their work. The interviewee below describes how the experience of acquiring and selling drugs online, particularly in large amounts, was accompanied by pervasive feelings of fear and trepidation:

> Interviewee 2: I was honestly shitting bricks thinking about ordering bulk MDMA, mainly because I only had like 5k at that time and no job. So if I ordered a lot and it was a scam, I probably would've freaked out. I ended up ordering 56g's of MDMA and my first drug deal ever was for 2 oz's of MDMA. I ordered from [WELL KNOWN VENDOR 3], so my first real order was not only 2 zips of MDMA but also international LOL.
>
> I went and made like $2300 or something off the first 56g's, and after that he wanted more, so the next 3 months I started ordering 112g's of MDMA from [WELL KNOWN VENDOR 2] because he had just started getting bulk MDMA. I would order around 224g's of MDMA a month, and pretty soon the guy I knew requested that I get him some acid. So I sold about 4 pages a month and a couple hundred grams of MDMA to the same guy, all bought through [WELL KNOWN VENDOR 2].
>
> Interviewer: So this was a dealer in your local city, who you just kept supplying through DNMs?
>
> Interviewee 2: Yes. I have never sold personal amounts of drugs to anyone. I don't have the stomach for it, to be honest.

While statements such as those above offer valuable insights into the psychological and logistical challenges facing cryptomarket vendors, this quotation is also revealing in another sense—it demonstrates the use of cryptomarkets to both buy *and* sell illicit drugs. Online-to-online buyer–vendors (OOBVs), are distinguished from all other types of drug suppliers in that they have no physical interaction with any other member of a drug distribution network. This form of drug supply seems particularly suitable for those who may be interested in the profits of drug dealing and who are not deterred by its illegality but, in the words of the above vendor, otherwise 'lack the stomach' for in-person forms of drug exchange, which carry the potential for violence and other forms of confrontation and exploitation. While the existence of OOBVs has been theorised previously (see Cunliffe et al. 2017; Martin 2019), this is, to our knowledge, the first time their existence has been empirically confirmed by academic research.

Other cyber-offences

The final career pathway evident in our subject group involved neither purchasing nor selling drugs in any offline or online context but rather occurred through prior participation in other illegal activities committed online. Several respondents reported involvement in various cyber-offences, particularly online credit card fraud or 'carding', before switching to selling drugs on cryptomarkets:

Interviewee 9: When I was under 18 I was involved with this guy who was over 18 and basically using me to commit computer crimes he taught me that and I actually saw him use it and run from the cops, lol.

Interviewer: You were involved with a guy who used you to commit computer crimes?

Interviewee 9: Yes, I was never arrested for it which is crazy because of the shit I did on a Windows computer using an just an R DP but this was the 90s.

Interviewer: Can I ask what it was? Actually quite a few vendors have done similar things.

Interviewee 9: I can't be too specific but carding/bank shit… At one point I asked my friend's dad to help me cash out and his response was 'that's a lot of scratch, son'.

Interviewer: So when you started on DNMs you were prepared for the tech side of things

Interviewee 9: Yes, although I had no experience on Linux but I was pretty well versed in anything Windows based as well as some basic hacking.

The link between illegal carding and the cryptomarket drugs trade makes sense considering that the two illegal markets—one for stolen credit card information, the other for illicit drugs—are often hosted on the same platforms. Contemporary cryptomarkets often have a thriving trade in both types of products (Soska & Christin 2015), unlike earlier sites such as Silk Road, which imposed bans on goods and services that were associated with predatory crimes such as fraud (Martin 2014a).

Perhaps more important, however, is that experiences such as those recounted above demonstrate how people skilled in the use of the IT necessary to commit one form of cybercrime (knowledge of operating systems and their vulnerabilities, hacking, encryption, etc) are able to transfer these skills to facilitate other forms of online offending—in this case, cryptomarket vending. This finding suggests that the accumulation of IT skills has particular value to people engaging in online crime, not only in committing offences safely but also in affording them the flexibility to move from one type of online offence to another as risks change and new opportunities for profit emerge.

Material and non-material motivations

As raised in the previous section, interviewees were typically motivated to commence cryptomarket vending by the prospect of making significant amounts of money. For some interviewees, this realisation occurred gradually in a context of either personal drug consumption or personal consumption coupled with social supply. For others, the realisation of the potential for significant profit took place in a much shorter span of time, as was the case with the vendors quoted below:

> Interviewee 12: I was still just a buyer [when I first accessed a cryptomarket]. That's until I got my first pack of real molly [MDMA]… I couldn't believe what ppl would pay me. Then I found I can buy Molly for $4G and sell for $60 a gram.

The vendors above are referring to the opportunities that cryptomarkets present to purchase drugs cheaply from foreign countries and then resell them locally, either back on to a cryptomarket or into offline drug markets. This practice is essentially one of arbitrage—that is, taking advantage of price differences between different drug markets, with the cryptomarket acting as a virtual broker by connecting disparate buyers and sellers. The capacity for cryptomarkets to facilitate brokerage in this manner has led to their conceptualisation as a 'superbroker' (Martin 2014a), one capable of simultaneously facilitating many thousands of drug exchanges between buyers and sellers located around the world.

Despite the potential for cryptomarkets to link geographically disparate drug markets, opportunities for arbitrage persist due the preference of many customers to source drugs domestically rather than run the risk of packages being intercepted by customs as they enter the country (Cunliffe et al. 2017). By importing drugs themselves, vendors assume the risk of postal interception at the border and, in turn, charge a premium to customers for doing so. The ease with which cryptomarkets may be searched for different drug types, prices and locations enables new OOBVs to identify these positions of arbitrage and to establish a profitable drug-selling enterprise with no connection to offline sources of drug supply.

The potential for profit was the most common motivation to begin cryptomarket vending. However, some interviewees also expressed more politically oriented motivations for their involvement in the online drugs trade. For these vendors, not only was selling drugs online an act that would lead to personal financial enrichment; it was also consistent with beliefs about the potential for cryptomarkets to reduce drug-related harm and challenge the current regime of global drug prohibition:

> Interviewee 8: So I started to vend in the early 2015 if I remember. Buying was maybe one year before. So I'm not an old SR [Silk Road] guru but these aspects you are speaking of actually matter to me. As depicted before I probably sound like a guy who tried to make a few bucks on his spare time. But the ideas/concepts of harm reduction, ethical drug dealing, or politics might actually have 'helped me' in taking that decision. I definitely stand for legalization or decriminalization of most drugs. New progressives talking about the subject and I definitely see DNMs as a step or milestone in rethinking the relation we have with it and how we apprehend it. It does not rid away the fact that I dealt drugs, but I see it in a better way than street dealing. For the rest it is more a philosophical/moral problem: Isn't selling drugs immoral etc etc and this discussion might never end. During that time, people dare another approach, organize themselves and try different ways, once again it is fluid and it flows. Only stagnant water turns bad.

The notion that selling drugs via cryptomarkets may reduce drug-related harm is consistent with a growing body of international research focused on this issue (Aldridge, Stevens & Barratt 2018; Bancroft 2017; Barratt et al. 2016; Barratt, Ferris & Winstock 2016; Aldridge & Décary-Hétu 2016; Martin 2019, 2014b). However, there is also a self-serving aspect to this line of reasoning that is consistent with Sykes and Matza's (1957) concept of techniques of neutralisation, whereby offenders seek to ameliorate the guilt associated with their offending through the employment of a variety of self-protective rationalisations. In the case of the interviewee above, for example, their decision to sell drugs was framed as at least partly prosocial. This is consistent with the technique of neutralisation 'appealing to higher loyalties', whereby engaging in offending is rationalised on the basis that it serves a higher purpose—in this case, the reduction of drug-related harm. Other techniques of neutralisation expressed by interviewees included 'denial of responsibility'—claiming that the drug use they facilitated was not harmful—and 'condemning the condemners', positing that the apparatus of global drug prohibition produces greater harm than the selling of illicit drugs.

Other interviewees also engaged with the moral dimensions of their offending but responded in different ways. For the vendor below, their history of drug supply was characterised by experiences of guilt and responsibility for supplying drugs that led to serious user harms observed from a close, personal perspective:

> Interviewee 3: I started selling illegal shit like fake IDs and grams of weed around 13 and had grown up in a religious household. As much as I brushed everything off from a morality perspective, I just kept feeling as if I was in the wrong & that I was responsible for some of the people I sold to. That obviously dissipated. I'd guess one of my biggest problems was watching people throw their lives away. I had no objection to people doing what they want with their bodies and all. But some people were incredible to be around when sober. Incredibly sharp and full of inspiration. A few cases still stick with me though. One was the reason I stopped selling pharma opioids. 16 maybe. This girl had never used anything outside of the medical realm but her friends had convinced her to try hydrocodone recreationally. So I started giving it to her. We had been friends for a long time and all. But probably within a month she started asking for entire bottles at a time and her life revolved around opiates. I cut her off and quit selling opioids soon after.

The statement above reveals how involvement in illicit drug supply can lead to uncomfortable personal realisations that prompt feelings of accountability and changes in vendor behaviour—in this case, avoiding selling drugs that are perceived to be excessively harmful. Similar sentiments were also expressed by a number of interviewees, who avoided selling drugs that they believed would result in unavoidable harm to their customers or that they would not use themselves. It is worth noting, however, that, unlike in the instance above, cryptomarket vendors do not physically interact with their customers. This maintenance of physical separation is likely to prevent vendors from witnessing the potentially harmful consequences resulting from their drug supply, which insulates them from the psychological consequences associated with harms that may be suffered by their customers.

In addition to the financial and political motivations that prompted engagement in cryptomarket vending, a number of interviewees described more mundane pleasures associated with their work. This included feelings of autonomy and liberation from legal employment and the drudgeries with which it may be associated (overbearing bosses, working to other people's schedules, etc). Instead, cryptomarket vending was associated with a lifestyle characterised by personal empowerment and individual agency. Interviewees also described creative satisfaction associated with the problem solving necessary to buy, sell and smuggle drugs without coming to the attention of law enforcement:

> Interviewee 10: I am very creative. I like it when customs opens something and have it in their hands, but don't recognise it. I did for example a soap stealth—[which involved] melting soap and putting mylar sealed drugs inside of it, then using citrus oil in the soap and putting the soap into a mylar bag also. The fun part is they can detect the mylar but when they open it they don't expect that inside the soap is also mylar so they don't double scan it, but seeing the soap with label on it…and their mind says 'nothing wrong'.
>
> Interviewer: You've wasted half their day.
>
> Interviewee 10: Haha, no, they do a good job.

The levity with which the above interviewee described imagining their drug consignment being inspected by customs authorities was somewhat surprising. What would for many be a harrowing experience was instead reinterpreted as something fun, even playful. Responses such as these indicate that, among some vendors at least, the dangers inherent in online drug supply (eg postal interdiction) are also perceived as opportunities for enjoyment and the application of intellect in ways that result in satisfaction. This suggests that rather than producing a deterrent effect, as one might typically expect, risks posed by law enforcement can also inadvertently motivate vendors by creating challenging but manageable problems that are gratifying to solve.

Becoming a darknet drug vendor

Establishing a safe and profitable cryptomarket vending practice is not easy, and interviewees described overcoming a range of practical challenges in establishing their enterprises. These generally fell into one of two categories: those associated with ensuring their individual safety and anonymity (encryption, postal stealth practices, etc), otherwise referred to as operational security or OPSEC, and those that were more business-oriented and involved breaking into competitive online drug markets so one could begin making a profit. Sources of information that interviewees used to learn how to operate safely and profitably on cryptomarkets included: mentors, business partners and other associates, discussion forums and online 'how to' guides, and, surprisingly in several instances, other vendors and customers.

As discussed earlier in this report, some vendors had had previous experience with IT and the commission of other cybercrimes or had spent significant amounts of time as buyers on cryptomarkets. For these vendors, the encryption elements of ensuring proper OPSEC (PGP, TAILS, etc) were already familiar and could be implemented relatively easily. For vendors lacking IT experience, however, difficulties in learning the basics of encryption could be significant and time consuming to overcome. Some interviewees described the learning process taking weeks or even months before a sufficient level of technical proficiency could be attained. This process could be aided by others, however. The interviewee below, for example, was able to rely on the assistance of their offline drug supplier, and subsequent cryptomarket trading partner, to learn their way around some of the fundamental technologies necessary for cryptomarket trading:

> Interviewee 3: I got started when one of my suppliers showed me a secure messaging application he had been working on. He talked about the need for better encryption when communicating and wanted me to stop using Wickr with him. Later on, he asked if I wanted to open a vendor account with him on Silk Road. I had not even heard of the darknet. I do think I had tried some Bitcoin faucets and played online poker for Bitcoin, but otherwise I'd heard of none of the things he (supplier) talked about. But the idea fascinated me and I agreed to do the sales and he would still sell his product through me. He had to spend hours showing me—over the phone—how set up Tor, a Bitcoin wallet, and (I think) Kleopatra.

Learning encryption is critical to selling drugs online, yet it represents only one half of the OPSEC challenge facing cryptomarket vendors. The other half concerns managing postal delivery of drug consignments in such a way that: (a) they defy detection by authorities and make it successfully to customers (commonly referred to as 'stealth'); and (b) in the event they are seized by authorities, they do not reveal incriminating information about the vendor who sent them (the section below contains details of some of the postal risk management techniques discussed by interviewees).

As was the case with learning encryption, discussion forums and online guides provided a useful starting point for the development of stealth techniques, with several vendors reporting tweaking and perfecting different forms of popular concealment, in what was often described as an enjoyable, problem-solving experience. Less-anticipated sources of knowledge for the sharing of stealth techniques included other vendors, who, in several instances, were reportedly willing to share their specialised knowledge freely to others engaged in cryptomarket vending:

> Interviewee 2: I learned some of it [stealth and safe postal techniques] from [WELL KNOWN VENDOR 2], but that was mainly how to deal with controlled deliveries. I am very good at problem solving.

The sharing of useful information with potential competitors is indicative of an atmosphere of collective identity and solidarity among vendors. Despite the competition for customers, vendors typically described feelings of affinity with others who were engaged in the same line of work and who faced similar threats from law enforcement. This prompted information sharing in what could be perceived as reciprocal acts of defiance and community:

> Interviewer: So on DNMs you have a lot of competition. What's your relation to them? Do you talk to any?
>
> Interviewee 7: Yeah, we're actually all pretty cool with each other, very secretive but it's cool asking for pointers as a noob or even just secret vendor forums, it's like a fraternity.

This willingness to discuss stealth techniques that could be used to frustrate the efforts of postal inspection agencies was similarly shared between vendors and customers. This suggests that vendors share altruistic sentiments not only with each other but also with those who may be considered part of the drug-using or drug-dealing 'underground'. In some instances, customers who had expertise of their own offered this help in an unsolicited manner, while in other cases they were rewarded for their assistance with discounts or free drug samples:

> Interviewer: What about the stealth, how did you get about learning how to do that?
>
> Interviewee 2: Lol its hard and stressful as hell being a vendor, and stealth is actually easy. I just asked a postal inspector that bought coke from me how to get shit through. Everybody loves coke right?

> Interviewee 1: My stealth is one off the best around, check it inside the FB [customer feedback]. We learned from the years. We learned that thanks for customers. Customer sometimes explained which stealth they received from [other] vendors.

In addition to learning appropriate postal and online OPSEC, vendors required business strategies to start their vending careers in earnest. Paquet-Clouston, Décary-Hétu and Morselli (2018) suggest that cryptomarket drug sales are highly skewed in favour of a small number of vendors who carry out the vast majority of online drug transactions. This particular structural characteristic of cryptomarkets, where vendors are assessed by customers according to customer feedback, therefore works to the benefit of established vendors with good reputations and poses significant obstacles to new vendors seeking to break into the market:

> Interviewee 8: Why would someone trust a seller with no feedback and limited offers? I guess my first sell took me a bit more than two and a half months if I remember (maybe 3).

Vendors reported a number of different techniques used to overcome this challenge and attract customers. This included marketing techniques such as posting messages on discussion forums and the distribution of free samples. These techniques helped to overcome the reluctance that customers typically feel when purchasing drugs from new vendors who have little in the way of customer feedback. Indeed, feedback is seen as an indicator of both product quality and trustworthiness:

> Interviewer: What about getting customers back when you started out. You mentioned building hype on reddit. Was it difficult to make those first few sales?
>
> Interviewee 9: Not really. Contacted a few key members of [forum] and sent samples, and had a cheap sample listing on market. First week was slow. 2 or 3 samples a day. After that it grew fast. Started moving a few 8ths and [edibles]…before you knew it, ounces a day and more [edibles] than Willy Wonka… To be honest man I approached it like a legit business—service and product on point, [and the] rest will follow.

Vendors who were proactive in building their customer base through the use of marketing techniques were more likely to report increases in sales. This suggests that barriers to entry into cryptomarket trading were manageable for those who had an entrepreneurial attitude and who were willing to treat their illicit trading enterprise with the care and due diligence perceived to facilitate success in the legitimate retailing sector:

> Interviewee 9: It's just like legit business, if your products and service stand out, you'll grow rapidly and do well.

These findings are consistent with earlier theoretical work that posits that one of the primary attractions of cryptomarket vending is that it can be differentiated from offline trading, which necessitates interactions with customers who are potentially problematic or even dangerous (Martin 2018). By contrast, interviewees considered cryptomarket vending to more closely resemble work in the legal employment sector, with more manageable risks, and profits that could be attained if one employed appropriate business strategies (eg marketing techniques).

Perceptions and management of risks

All of our interviewees considered cryptomarket vending to be far less risky than offline dealing. This is consistent with a significant body of cryptomarket research that discusses the benefits to cryptomarket vendors and buyers of relying on an online trading platform, in which threats and experiences of violence are much less commonplace than in some offline drug markets (Martin 2018, 2014a, 2014b; Barratt, Ferris & Winstock 2016). Among interviewees, this perception was shared by both those with no previous involvement in offline dealing and those with direct personal experience of drug supply in online and offline contexts:

> Interviewee 2: Yes, no more death threats lol… Let me tell you first hand, I have been beat and robbed just like the movies, drugs get crazy.

We should note that, while cryptomarkets were universally considered to be much less violent than other drug-trading environments, interviewees occasionally encountered instances of violence, either threatened or realised. One vendor described a supplier subjecting them to violence at gunpoint, while others described customers threatening them with violence:

> Interviewee 2: [I've dealt with] crazy resellers…who threaten to hunt me down and kill me and even hire hackers to find me.

One of the central preoccupations of risk was therefore physical separation from customers. Customers were considered as possible sources of risk in their own right, whether as potentially violent predators who could extort or rob drug suppliers, as sources of problematic confrontation or as potential informers for law enforcement.

Despite perceptions of relative safety and other similarities with legal employment (such as a reduced risk of violence and use of 'legitimate' business strategies), interviewees remained preoccupied with the proactive management of risks, the greatest of which were considered to come from law enforcement. Interviewees sought to reduce the risk of identification by law enforcement through appropriate OPSEC in relation to their online communications, appropriate use of encryption and careful management of postal deliveries. Interviewees perceived—correctly, in our view—that postal interdiction represented the greatest risk of detection by authorities. Interviewees controlled these risks with varying degrees of diligence and sophistication, including the use of stealth techniques to prevent authorities from detecting drug consignments as they travelled through the post:

> Interviewee 12: The pills I sell come in strips of 10… Shipping the pills in strips I haven't mastered just 'cuz they rattle no matter what you do. I've considered trying to vacuum seal them to see if that helps… I tried taking them out of the packs and putting them in mylar bags but my customers weren't fond of that because they're not marked.

In addition to ensuring that drugs were concealed to evade detection by postal authorities, interviewees reported employing techniques that could help prevent identification in the event that law enforcement engaged in undercover buys might seize drug consignments and subject them to forensic examination. Simple precautions that were commonly used to impede forensic examination included the wearing of double pairs of rubber gloves when handling any drugs or postal materials to avoid leaving fingerprints:

> Interviewee 5: As a vendor you have to stay alert all the time. Simple precautions such as checking what cars are parked, and what kind of people are in the cars, especially when dropping of in a mailbox, wearing gloves etc all that stuff. If you do that—and outsource the in store shipping to someone else—you're pretty much set. Of course, there are risks but they can be minimal.

In addition to the risk reduction measures outlined above (such as the use of gloves and observation of commonly used postal facilities), interviewees also discussed the need to vary the use of post boxes to avoid establishing patterns of behaviour that could possibly lead to identification. While some interviewees were relatively blasé about these postal aspects of OPSEC, others reported going to significant lengths to ensure that postal drop-offs were appropriately randomised to avoid potential profiling:

> Interviewee 2: Using a maximum of 10 packs per blue bin, and using the same return address only 10 times before changing the name, then swap names, hit a new zip code with a maximum of 50 packs dispersed over a couple mile radius, and then make sure you drive 15-30 miles and rinse and repeat. Make sure you switch it up every time, different blue bins, different times, different towns, different zip codes, make sure that there is no way you're leaving a discernible trail.

Despite the availability of a range of practices that could reduce vendor risk and improve one's OPSEC, it was surprising to learn that many interviewees knowingly eschewed at least some of these practices. While one could reasonably interpret this failure to maximise opportunities to reduce risk from law enforcement as representing a lack of caution on the part of vendors, interviewees generally perceived their risk of arrest to be low. Vendors therefore implemented only those OPSEC measures that they considered necessary to ensure their safety. This affords vendors the ability to scale up operational security measures if they perceive changes to their risk profile—for example, in the event that law enforcement allocates more resources to mail screening and forensic analysis of seized drugs.

Discussion

This research contributes a range of novel findings, some of which correspond with earlier cryptomarket research, and others which may be considered additions to debates surrounding how and why people participate in cryptomarket drug vending. The overwhelming majority of interviewees explicitly identified the potential for making significant profit in a context of reduced risk as the major attraction of participating in the cryptomarket drugs trade. The realisation of the opportunity to trade drugs safely and profitably online often occurred when interviewees began purchasing drugs on cryptomarkets, either for their own personal consumption or to facilitate non-commercial social supply. Several interviewees described this as gradual process that was consistent with 'digital drift' (Goldsmith & Brewer 2015), whereby offenders become involved in greater levels of offending without necessarily making a conscious decision to do so. This process was surprising given that, unlike selling in offline contexts, where one may easily sell surplus drugs to proximate friends or acquaintances, cryptomarket vending involves a number of additional steps or barriers to entry, such as the setting up of a vendor trading account and the payment of vendor fees. We anticipated, incorrectly, that these barriers to entry would preclude unconscious drift into online drug selling and that only those who made a deliberate decision to sell drugs online would become commercial cryptomarket vendors.

Other findings also have relevance to broader criminological research about the nature of, and motivations for, offending. For example, vendor rationalisations about the (in)appropriateness of selling drugs via cryptomarkets often—though not always—corresponded with Sykes and Matza's (1957) classic techniques of neutralisation, such as 'denial of injury' and 'appealing to higher loyalties'. Vendors were assisted in making rationalisations that downplayed or ameliorated the potentially harmful psychological effects of their offending via interactions with peers and other members of the 'cryptomarket community', who shared their experiences and political opposition to drug prohibition on user forums and in private communications.

As a result of employing these techniques of neutralisation, some vendors perceived themselves as engaging in prosocial work in defiance of an overbearing and hypocritical state that, through the imposition of drug prohibition, enhanced a range of drug-related harms (systemic violence, product adulteration, etc). These findings are consistent with Martin's 'gentrification hypothesis' (2018), which suggests that a key attraction to participation in the cryptomarket drugs trade is the perception that it represents a less harmful alternative to conventional drug trading. The absence of violent norms that exist in some offline drug markets contrasted with technologically mediated interactions with other drug market participants, which were characterised by courtesy and respect akin to what is witnessed in the legitimate retailing sector.

The ways in which vendors discussed the non-material motivations for their work and the creative satisfaction that could be derived from confronting and overcoming risk recall earlier theorising around edgework (Lyng 2004) and the seductions of crime (Katz 1988). In the context of cryptomarket drug vending, our interviewees provided clear evidence of enjoyment in confronting risk in ways which confound orthodox notions of deterrence. Here, the dangers of apprehension by law enforcement were reinterpreted, not as sources of danger to be avoided but rather as opportunities for excitement that were otherwise unavailable in legal work. While vendors were also attracted to the relatively fewer risks that they perceived to be prevalent in the online trading environment, risks that were perceived as manageable were reinterpreted as benefits, rather than disincentives, that could motivate further engagement in the cryptomarket drugs trade.

We further found that, while it may seem easy to 'set up shop', vendors would often struggle with a variety of issues like stealth, encryption and even making their first sale. A 'Matthew principle' can therefore be argued to be in effect in cryptomarkets, as successful vendors with stellar reputations receive a higher reward (Hardy & Norgaard 2015; Przepiorka, Norbutas & Corten 2018), and the difficulty which other, less profitable vendors have experienced may explain why so many cryptomarket vendors make few sales or none at all (Paquet-Clouston, Décary-Hétu & Morselli 2018; Tzanetakis 2018). The vendors we interviewed had all attained a level of success they themselves appreciated, but it had required them to learn new skills and to research how to be as safe as possible, a process which could take months. Interestingly, we found that learning and the acquisition of knowledge were not a passive absorption of information from forums but were often a social and relational process: one vendor learned encryption while on the phone with his business partner, and several had received information on their competitors' stealth through their customers. Most evident of this social dimension was that several vendors had transitioned from being buyers, which had given them a knowledge base that could inform their use of cryptomarkets.

Although cryptomarket vendors are typically specialised and their financial success differs extensively (Pacquet-Clouston 2018; Tzanetakis 2018), we found that in spite of the diversity of our cohort the interviewees shared several commonalities. They were motivated not only by monetary gains but also by the qualities of 'gentrification' and social norms prevalent in, and particular to, cryptomarkets.

As noted previously, the limited number of respondents precludes the making of claims representative of cryptomarket vendors as a whole. In addition, it seems likely to us that some vendors may have been more motivated to participate in this study than others and that this asymmetry is likely to have influenced our findings and the resultant discussion. In particular, we suspect that those vendors who have a strong belief in the non-material benefits of the darknet drugs trade—in a personal as well as a broader social sense—were more likely to participate and share their experiences than those whose involvement in cryptomarket vending was prompted by material motivations alone.

Policy implications

Despite the exploratory nature of this research, our findings suggest some broad policy implications for state and federal law enforcement agencies, public health agencies and medical professionals responsible for the distribution of prescription drugs. Given the increasing usage of cryptomarkets both in Australia and overseas, there is a growing need to develop appropriate policy responses.

Law enforcement

From a policing point of view, cryptomarket drug trading presents a wicked problem, with seemingly intractable challenges ranging across the entire spectrum, from the tactical through to the strategic and ideological. Tactically, cryptomarkets are extraordinarily difficult to police. Users are protected by powerful encryption technologies (Tor, PGP, Bitcoin, etc), complicating both identification of offenders and evidence gathering. Traders are often located in different countries, necessitating international policing operations and extradition treaties in those instances where offenders can be charged but are based overseas. Existing techniques used to target offline drug suppliers, such as conventional buy–bust operations and raids on drug-dealing 'hotspots', are redundant; cryptomarket vendors do not meet in person with their customers, which precludes the 'bust' component of a typical buy–bust, and the virtual trading environment eliminates the possibility of a 'raid', at least in any conventional sense. Instead, investigators overseas have turned to resource-intensive cyber-operations, requiring advanced IT skills and expertise, which are often in short supply even in large and well-resourced policing agencies (Martin 2014a).

While there have been a number of successful law enforcement takedowns of cryptomarkets—the cyber equivalent of a raid—these operations have resulted in relatively few arrests and limited seizure of assets, suggesting that the outcomes of any such operation are unlikely to justify the expenditure that they require. Of course, arrests and seizures are not the only measure of operational success, and takedowns could perhaps be justified if they significantly disrupt the cryptomarket trading environment or otherwise deter prospective users from engaging in online drug trading. However, a number of studies conducted in the aftermath of mass law enforcement takedowns indicate that, while takedowns can disrupt cryptomarket trading in the short term, users typically migrate to other cryptomarkets and quickly resume trading to pre-takedown levels (Décary-Hétu & Giommoni 2017). The deterrent effect of cryptomarket-related arrests is also highly questionable, with at least one study (Ladegaard 2017) demonstrating that high-profile arrests of cryptomarket administrators and vendors actually *increase* rather than decrease the frequency of online drug transactions, as publicity around cryptomarkets draws attention to their viability as a source of drug supply.

Strategically, the dynamics of law enforcement takedowns and subsequent cryptomarket replacement and user migration are difficult to counter. There are simply too many cryptomarkets in operation and development at any one time for law enforcement agencies to target them effectively. Further, most of these sites will be taken offline before they reach 'maturity', due to exit scams and predatory hacks undertaken by other online offenders, and begin trading in large enough quantities to warrant law enforcement intervention (EMCDDA & Europol 2016). Ironically, the volatility inherent to the market ecosystem works to protect cryptomarkets from law enforcement; the rapid turnover of cryptomarkets means that any site could be taken offline at any moment, rendering any resources that law enforcement agencies have already committed to breaching their cyber-defences wasted.

From an ideological perspective, cryptomarkets are also problematic for law enforcement. While less political than in the heyday of Silk Road (Munksgaard & Demant 2016), cryptomarket discussion forums remain potent sites for political debate on the perceived evils of prohibition. Radical libertarian ideologies which reject heavy-handed state intervention in the drug lives of citizens are common intellectual fodder for forum participants; these intersect with harm reduction narratives which claim that drug prohibition is a form of harm maximisation that increases violence and other drug-related harms, thus adversely affecting the health of both individual users and society as a whole. These arguments provide a compelling, and arguably self-serving, case for cryptomarket users to reject drug prohibition and engage in cryptomarket trading as a safer and less violent alternative to the street-based drugs trade. As discussed earlier in this report, cryptomarket vendors employ these arguments against law enforcement-led prohibition to ameliorate the guilt associated with their offending.

Our research validates earlier studies that have suggested that darknet drug dealers are highly cognisant of, and proactive in, managing risks posed by law enforcement (Bancroft & Reid 2016a). Interviewees identify these risks and formulate effective anonymising and counter-interdiction measures using a variety of methods, including, particularly, analysis of public police reports and media articles concerning previous arrests of other offenders involved in the trafficking of drugs via the darknet. Other members of the darknet 'community', including fellow vendors and customers, constitute a further important source of information about risks posed by law enforcement. Discussion of these risks takes place on cryptomarket discussion forums as well as in private, encrypted communications. In combination with the customer feedback mechanisms used on cryptomarkets, communications between members of the darknet community provide vendors with a readily accessible, constantly updated and well-informed guide to the various risks posed by law enforcement, as well as to tried and tested countermeasures.

There are two principal avenues whereby darknet drug vendors may be identified by law enforcement: (1) by exploiting technological vulnerabilities in either Tor or cryptocurrencies; and (2) via monitoring and interdiction of drug consignments sent through domestic and international postal systems. Interviewees identified—correctly, in our view—that the greatest risks posed by law enforcement are at these latter postal stages of distribution. As discussed in the *Perceptions and management of risks* section above, interviewees outlined sophisticated 'stealth' strategies to conceal drug consignments to evade detection. Interviewees also reported regularly changing the routines associated with their use of postal systems in order to disrupt profiling by law enforcement and maintain anonymity.

It may be tempting to interpret these findings as evidence of the need for greater policing resources in conducting cyber-investigations, such as blockchain analysis to de-anonymise cryptocurrency transactions, and for more intensive screening of mail, both domestically and at the border. We would argue against both of these interpretations, for two principal reasons.

Firstly, increased allocation of finite policing resources is unlikely to meet with sustained success, as darknet drug vendors are proactive in identifying and managing risks posed by law enforcement. This takes place both in discussion forums, where such events are collectively dissected and analysed, and individually, as several vendors we interviewed had gained extensive knowledge of how others were caught. Online vendors are quick to adapt to changes in policing and postal screening operations and are likely to respond to increased surveillance with additional counter-measures of their own (use of cryptocurrency tumblers, more sophisticated postal stealth, etc). Indeed, previous analysis by Cunliffe et al. (2017) suggests that, despite major increases in Australian border postal screening facilities over the past few years, darknet drug vendors located overseas are not deterred from sending illicit drugs into the country. While evidence suggests that border screening may deter some local buyers from purchasing drugs from overseas vendors (Cunliffe et al. 2017), these purchases are still likely to be made but will instead be sourced from local suppliers, either online or offline. Increased border screening may therefore inadvertently work to the benefit of locally based organised crime groups, which stand to profit from more stringent border controls reducing competition from darknet dealers located outside of the country.

Secondly, interviewees consistently reported participating in the darknet drugs trade because it offered a way to continue trading illicit drugs but with a reduced risk of violence, both from customers and from other market participants. These findings echo previous research suggesting that buyers and sellers of illicit drugs are drawn to cryptomarkets because they offer a novel avenue whereby better quality, less adulterated drugs may be bought and sold in a context of reduced risk. The likelihood that the ever-increasing proportion of illicit drug transactions taking place via cryptomarkets may in fact reduce the range and severity of harms associated with illicit drug transactions, especially violence, therefore poses a dilemma for law enforcement agencies: that is, even if effective measures could be introduced to crack down on the darknet drugs trade, would these measures work to the benefit and safety of the general public?

Given that demand for illicit drugs remains high in Australia and that cracking down on the darknet drugs trade would likely reroute users and dealers back into more harmful conventional, offline drug distribution networks, the answer to this question, for the time being at least, appears to be no. On the evidence available, it appears that the most likely outcome resulting from a successful crackdown on the darknet drugs trade would be that drug-related harms and violence would increase and that established organised crime groups which use violence to control and monopolise the offline illicit drugs trade would benefit and profit from reduced competition from online sources of drug supply.

Health agencies

Several of our respondents reported entering the darknet drugs trade as a result of access to pharmaceutical drugs that had been rerouted from legitimate sources of supply (manufacturers, chemists, etc). Legitimate sources of pharmaceutical drugs were considered important for customers, who had expressed to interviewees wariness about unpackaged or unlabelled pharmaceutical drugs being possible counterfeits. Given this rerouting of legally manufactured prescription drugs into the illicit drugs market, we would argue that an effective policy response would be to introduce greater controls and surveillance of the distribution and prescription of legal pharmaceutical drugs throughout the entire licit supply chain. These policy measures would likely assist in curbing the supply of pharmaceutical drugs to cryptomarkets.

Lastly, this research validates previous studies that have found that darknet dealers are highly responsive to demand from consumers and will attempt to adapt their business practices and product availability on the basis of consumer demand. Rather than focus taxpayer resources on supply reduction measures (eg via enhanced postal screening), a more effective and efficient policy response would be to increase health services aimed at demand and harm reduction. This approach would assist in reducing demand and drug-related harms resulting from the online and offline illicit drug trades.

Conclusion

This research aimed to answer a range of questions about the offending behaviour of cryptomarket vendors, including how and why people became involved with online drug vending, whether motivations to persist in vending included both material and non-material factors, and how cryptomarket vendors perceived and managed risks, whether emanating from law enforcement or other sources. Our research findings contribute some rare insights into each of these questions. Vendors became involved with selling drugs on cryptomarkets via at least one of the following pathways: purchasing and using drugs either on cryptomarkets or via offline sources (including small-scale social supply), offline commercial drug supply, or the commission of other cybercrimes. Interviewees shared a variety of material and non-material motivations for their participation in cryptomarket drug vending, including, particularly, the desire for financial reward and the avoidance of risks that were considered to be much more acute in offline drug markets. Principal among these were reduced risks of violence and detection by law enforcement, both of which were considered more manageable due to the anonymity afforded by darknet encryption and the geographical separation maintained between market participants.

Also revealing was how interviewees described the particular organisation of cryptomarkets creating brokerage or arbitrage positions. These allowed some vendors to reap a significant benefit from moving their business online. This desire to financially benefit from cryptomarket trading was complemented by a simultaneous fondness and appreciation for what Martin (2018) has suggested are gentrified norms of cryptomarket behaviour and transactions. Vendors view this gentrification as carrying significant benefits—namely, a low risk of violence and more professional transactional norms. We further find that vendors face significant barriers of entry, as suggested by Pacquet-Clouston, Décary-Hétu and Morselli (2018)—namely, in the form of technology and competences, which they must acquire and familiarise themselves with in order to operate on cryptomarkets. As with challenges posed by law enforcement, these barriers were considered to be manageable, and vendors reported assisting one another in a community-minded spirit of reciprocity in the face of risks posed by law enforcement.

References

URLs correct as at May 2020

Aldridge J & Décary-Hétu D 2016. Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy* 35: 7–15. DOI: 10.1016/j.drugpo.2016.04.020

Aldridge J & Décary-Hétu D 2014. Not an 'Ebay for drugs': The cryptomarket 'Silk Road' as a paradigm shifting criminal innovation. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2436643

Aldridge J, Stevens A & Barratt MJ 2018. Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction* 113(5): 789–796. https://doi.org/10.1111/add.13899

Bakken SA, Moeller K & Sandberg S 2018. Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology* 15(4): 442–460

Bancroft A 2017. Responsible use to responsible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk & Society* 19(7–8): 336–350

Bancroft A & Reid PS 2016a. Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society* 20(4): 497–512. DOI: 10.1080/1369118X.2016.1187643

Bancroft A & Reid PS 2016b. Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy* 35: 42–49

Barratt MJ 2012. Silk Road: eBay for drugs. *Addiction* 107(3): 683.

Barratt MJ, Ferris JA & Winstock AR 2016. Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy* 35: 24–31. https://doi.org/10.1016/j.drugpo.2016.04.019

Barratt MJ, Lenton S, Maddox A & Allen M 2016. 'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy* 35: 50–57. https://doi.org/10.1016/j.drugpo.2016.04.006

Barratt MJ & Maddox A 2016. Active engagement with stigmatised communities through digital ethnography. *Qualitative Research* 16(6): 701–719. https://doi.org/10.1177/1468794116648766

Böhme R, Christin N, Edelman B & Moore T 2015. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives* 29(2): 213–238. DOI: 10.1257/jep.29.2.213

Broséus J, Rhumorbarbe D, Mireault C, Ouellette V, Crispino F & Décary-Hétu D 2016. Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International* 264: 7–14. https://doi.org/10.1016/j.forsciint.2016.02.045

Broséus J, Rhumorbarbe D, Morelato M, Staehli L & Rossy Q 2017. A geographical analysis of trafficking on a popular darknet market. *Forensic Science International* 277: 88–102. https://doi.org/10.1016/j.forsciint.2017.05.021

Brunt TM, Atkinson AM, Nefau T, Martinez M, Lahaie E, Malzcewski A, Pazitny M, Belackova V & Brandt SD 2017. Online test purchased new psychoactive substances in 5 different European countries: A snapshot study of chemical composition and price. *International Journal of Drug Policy* 44: 105–114. DOI: 10.1016/j.drugpo.2017.03.006

Christin N 2013. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Proceedings of the 22nd International Conference on World Wide Web: Rio de Janeiro: 213–224. https://doi.org/10.1145/2488388.2488408

Coomber R 2006, *Pusher myths: Re-situating the drug seller*. London: Free Association Books

Cunliffe J, Martin J, Décary-Hétu D & Aldridge J 2017. An island apart? Risks and prices in the Australian cryptomarket drug trade. *International Journal of Drug Policy* 50: 64–73. DOI: 10.1016/j.drugpo.2017.09.005

Décary-Hétu D & Giommoni L 2017. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change* 67(1): 55–75. DOI: 10.1007/ s10611-016-9644-4

Décary-Hétu D, Paquet-Clouston M & Aldridge J 2016. Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy* 35: 69–76. DOI: 10.1016/j.drugpo.2016.06.003

DeepDotWeb 2015. *Evolution market background: Carding forums, Ponzi schemes and LE.* Retrieved from https://www.deepdotweb.com/2015/03/18/evolution-market-background-carding-forums-ponzi-schemes-le/

Demant J, Munksgaard R, Décary-Hétu D & Aldridge J 2018. Going local on a global platform. *International Criminal Justice Review* 28(3): 255–274. https://doi.org/10.1177/1057567718769719

Demant J, Munksgaard R & Houborg E 2016. Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime* 21(1): 42–61. DOI: 10.1007/s12117-016-9281-4

Dingledine R, Mathewson N & Syverson P 2004. *Tor: The second-generation onion router*. Fort Belvoir, Virginia: Defense Technical Information Center (DTIC). http://www.dtic.mil/dtic/tr/fulltext/u2/a465464.pdf

Dittus M, Wright J & Graham M 2018. *Platform criminalism: The 'last-mile' geography of the darknet market supply chain*. Proceedings of the 27th Conference on World Wide Web. Lyon, France: 277–286. https://doi.org/10.1145/3178876.3186094

Dolliver DS 2015. Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *International Journal of Drug Policy* 26(11): 1113–1123. DOI: http://dx.doi.org/10.1016/j.drugpo.2015.01.008

Dolliver DS, Ericson SP & Love KL 2016. A geographic analysis of drug trafficking patterns on the Tor network. *Geographical Review* 108(1): 45–68. DOI: 10.1111/gere.12241

Dolliver DS & Kenney JL 2016. Characteristics of drug vendors on the Tor network: A cryptomarket comparison. *Victims & Offenders* 11: 600–620

Duxbury SW & Haynie DL 2018. Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks* 52: 238–250. DOI: 10.1016/ j.socnet.2017.09.002

Duxbury SW & Haynie DL 2017. The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology* 34: 921–941. DOI: 10.1007/s10940-017-9359-4

Dwyer R & Moore D 2010. Beyond neoclassical economics: Social process, agency and the maintenance of order in an Australian illicit drug marketplace. *International Journal of Drug Policy* 21: 390–398. https://doi.org/10.1016/j.drugpo.2010.03.001

EMCDDA & Europol 2016. *EU drug markets report: Strategic overview.* European Monitoring Centre for Drugs and Drug Addiction & Europol. Luxembourg: Publications Office of the European Union. DOI: 10.2810/216248

Goldsmith J 2000. Unilateral regulation of the internet: A modest defence. *European Journal of International Law* 11(1): 135–148

Goldsmith A & Brewer R 2015. Digital drift and the criminal interaction order. *Theoretical Criminology* 19(1): 112–130

Hardy RA & Norgaard JR 2015. Reputation in the internet black market: An empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics* 12(3): 515–539. DOI: 10.1017/S1744137415000454

Hutchings A & Holt TJ 2017. The online stolen data market: Disruption and intervention approaches. *Global Crime* 18(1): 11–30. DOI: 10.1080/ 17440572.2016.1197123

Jardine E 2016. Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society* 20(2): 435–452. DOI: 10.1177/1461444816639976

Katz J 1988. *Seductions of crime: Moral and sensual attractions in doing evil*. New York: Basic Books

Kjellgren A & Jonsson K 2013. Methoxetamine (MXE)—A phenomenological study of experiences induced by a 'legal high' from the internet. *Journal of Psychoactive Drugs* 45(3): 276–286. DOI: 10.1080/02791072.2013.803647

Ladegaard I 2018. Instantly hooked? Freebies and samples of opioids, cannabis, MDMA, and other drugs in an illicit e-commerce market. *Journal of Drug Issues* 48(2): 226–245. https://doi.org/10.1177/0022042617746975

Ladegaard I 2017. 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* 58(2): 414–433

Lavorgna A 2014. Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. *Trends in Organized Crime* 17(4): 250–270

Lyng S 2004. Crime, edgework and corporeal transaction. *Theoretical Criminology* 8(3): 359–375

Maddox A, Barratt MJ, Allen M & Lenton S 2016. Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society* 19(1): 111–126. https://doi.org/10.1080/1369118X.2015.1093531

Martin J 2019. Revisiting drugs on the darknet: Key issues and debates in the cryptomarket drugs trade. In M Tzanetakis & H Stover (eds), *Drogen, Darknet und Organisierte Kriminalität.* Baden-Baden, Germany: Nomos: 209–228

Martin J 2018. Cryptomarkets, systemic violence and the 'gentrification hypothesis.' *Addiction* 113(5): 797–798. https://doi.org/10.1111/add.14029

Martin J 2016. Illuminating the dark net: Methods and ethics in cryptomarket research. In M Adorjan & R Ricciardelli (eds), *Engaging with Ethics in International Criminological Research.* London: Routledge: 192–211

Martin J 2014a. *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs.* Basingstoke, UK: Palgrave Macmillan

Martin J 2014b. Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice* 14(3): 351–367. DOI: 10.1177/1748895813505234

Martin J & Christin N 2016. Ethics in cryptomarket research. *International Journal of Drug Policy* 35: 84–91

Moeller K, Munksgaard R & Demant J 2017. Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist* 61(11): 1427–1450. https://doi.org/10.1177/0002764217734269

Morselli C 2001. Structuring Mr Nice: Entrepreneurial opportunities and brokerage positioning in the cannabis trade. *Crime, Law & Social Change* 35(3): 203–244

Morselli C, Décary-Hétu D, Paquet-Clouston M & Aldridge J 2017. Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review* 27(4): 237–254. https://doi.org/10.1177/1057567717709498

Munksgaard R & Demant J 2016. Mixing politics and crime: The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy* 35: 77–83. https://doi.org/10.1016/j.drugpo.2016.04.021

Munksgaard R, Demant J & Branwen G 2016. A replication and methodological critique of the study 'Evaluating drug trafficking on the Tor Network'. *International Journal of Drug Policy* 35: 92–96. DOI: 10.1016/j.drugpo.2016.02.027

Norgaard JR 2017. *Economics of illicit behaviors: Exchange in the internet Wild West* (Doctoral dissertation). George Mason University, Fairfax, Virginia. https://search.proquest.com/docview/1937504264?pq-origsite=gscholar

Ormsby E 2014. *Silk Road*. Melbourne: Palgrave Macmillan Australia

Paquet-Clouston M, Décary-Hétu D & Morselli C 2018. Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy* 54: 87–98. https://doi.org/10.1016/j.drugpo.2018.01.003

Przepiorka W, Norbutas L & Corten R 2017. Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. *European Sociological Review* 33(6): 752–764. DOI: 10.1093/esr/jcx072

Reuter P & Caulkins J 1998. What price data tells us about drug markets. *Journal of Drug Issues* 28(3): 593–513

Sandberg S 2012. The importance of culture for cannabis markets: Towards an economic sociology of illegal drug markets. *British Journal of Criminology* 52(6): 1133–1151. https://doi.org/10.1093/bjc/azs031

Soska K & Christin N 2015. *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem*. Proceedings of the 24th USENIX Security Symposium. Washington DC: USENIX: 33–48

Spitters M, Verbruggen S & Staalduinen MV 2014. *Towards a comprehensive insight into the thematic organization of the Tor hidden services*. Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference. The Hague: JISIC: 220–223. DOI: 10.1109/JISIC.2014.40

Sykes GM & Matza D 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review* 22(6): 664–670

Tzanetakis M 2018. Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy* 56: 176–186. https://doi.org/10.1016/j.drugpo.2018.01.022

Tzanetakis M, Kamphausen G, Werse B & von Laufenberg R 2016. The transparency paradox: Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy* 35: 58–68

Van Buskirk J, Naicker S, Roxburgh A, Bruno R & Burns L 2016. Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *International Journal of Drug Policy* 35: 16–23. DOI: 10.1016/j.drugpo.2016.07.004

Van Hout MC & Bingham T 2014. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy* 25(2): 183–189. https://doi.org/10.1016/j.drugpo.2013.10.009

Van Hout MC & Bingham T 2013. 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy* 24(6): 524–529

CRG reports

CRG 50/16–17

Rasmus Munksgaard is a doctoral candidate at the École de Criminologie at the Université de Montréal.

James Martin is Associate Professor of Criminology at Swinburne University.

www.aic.gov.au/crg