University of Manchester, University of Montreal

Cryptomarkets: The Darknet As An Online Drug Market Innovation

Final report to NESTA

Judith Aldridge, David Décary-Hétu
04/01/2015

Table of contents

1.0 INTRODUCTION

This project sought to use data scraped from the hidden or 'dark net' to enhance our understanding of a new business innovation, the 'cryptomarket'. Cryptomarkets are the most recent development in the commercialization of the Internet. They are the underground and often illicit counterpart of online retailers and use anonymizing technologies to hide the identity of visitors and the physical location of their servers. The best-known cryptomarket was *Silk Road 1*. Before being shut down by the FBI in October 2013, this cryptomarket enabled anyone to mail order illegal drugs and other goods with anonymous bitcoin payments. Following its demise, cryptomarkets have proliferated, in spite of another law enforcement crackdown in November 2014 shutting several. Cryptomarkets hold the promise to change online commerce by providing an anonymous shopping experience for both illicit and licit products and services. Just as the Internet enabled a revolution in the entertainment industry with the creation of peer-to-peer software, cryptomarkets hold the promise for disruptive impact of online commerce. The funding we received from Nesta enabled us to build a crawler to scrape data from hidden 'post Silk Road' (second-generation) cryptomarkets to enhance our understanding of them as a phenomenon, and of the increasingly blurred boundary between legitimate and illicit markets. In this report we aim to answer these questions:

Are cryptomarkets geared towards sale to consumers or resellers? Drug cryptomarkets have been described as selling exclusively to drug users making purchases for personal use, but our preliminary research published in a working paper (Aldridge & Décary-Hétu, 2014) suggests that the majority of the revenue generated on Silk Road resulted from purchases in quantities typical of drug dealers sourcing their supply. This is important: 'business-to-business' sales will have a qualitatively different and larger impact on the distribution of products by shifting distribution channels.

Are cryptomarkets truly global in reach? Online retailers have access to a worldwide market, and may therefore facilitate the distribution of goods and services in places that were previously hard to reach. There are however increased risks for vendors and buyers when dealing with partners located in different countries, and in order to reduce this risk cryptomarket vendors may elect not to exploit cross-border opportunities. To understand the impact of cryptomarkets, it is essential to understand the balance between security and efficiency that is struck through national and international transactions.

Are cryptomarkets inevitably a 'bad' innovation? It is often assumed that technological innovation is a socially positive development by driving economic growth, but in reality innovations have implications both positive and negative. Even cryptomarkets specializing exclusively in illegal goods and services – which may appear to exacerbate social problems, for example by increasing access to illegal drugs – carry with them clear positives. Drug cryptomarkets, for example, may substantially reduce problems of violence in drug markets, and increase access to better quality substances. And of course, not all cryptomarkets involve the sale of illegal goods and services: it's not only those with 'something to hide' who may wish to transact business anonymously online. We will document both the socially 'positive' and 'negative' aspects of this innovation.

How did we create the crawler? The Nesta funding that we received was used to create the web crawler, what we've called the DATACRYPTO tool. In conversations with Nesta during the course of the project, we were asked to describe how we did this in technical terms. The final section of the report details this process.

2.0 CRYPTOMARKET SALES: GEARED TO CONSUMERS OR RESELLERS?

2.1 Introduction

Researchers have characterised buyers on cryptomarkets as *drug users* making purchases for their *own consumption* (Christin, 2013; Martin, 2013). This has been echoed by other academics (e.g. Barratt, 2012), journalists (e.g. Economist, 2012) and media blogs (A. Chen, 2011) who describe them as a kind of "eBay" or "Amazon" for drugs. At least superficially, the resemblance to these exemplars of "business-to-customer" e-commerce is compelling, because cryptomarkets share many structural features with these marketplaces, including buyers being able to leave feedback on their purchases. However, the analysis of data derived in September 2013from *Silk Road 1* described in the working paper "Not an eBay for Drugs" (Aldridge & Décary-Hétu, 2014) suggested that this characterisation was not wholly correct. This analysis confirmed that a substantial proportion of customers were likely to have been drug dealers sourcing stock online to sell offline. Much has happened in the world of cryptomarkets since we collected those data, including a proliferation of many new marketplaces, alongside market closures due to administrator scams and law enforcement seizures. Will our characterisation remain true cryptomarkets nearly two years later?

2.2 Silk Road as a transformative criminal innovation

Cryptomarkets have not invented any new technology but have brought together many innovations that have considerably changed online shopping for illicit products and services. Cryptomarkets have the hallmarks of substantial innovation (Barratt, 2012; Christin, 2013; Martin, 2013; Van Hout & Bingham, 2014). They provide vendors with (1) a worldwide market for their products, (2) the capacity to sell to customers not already known to them, (3) the ability to trade anonymously and (4) in a relatively low risk environment. Cryptomarkets are more than just incremental innovation; their innovation is both substantial and manifold.

Cryptomarket vendors can effectively transcend the physical restrictions of a local drugs market – the people they could physically reach to transact with – to supply through postal delivery a worldwide market of customers. And in spite of the fact that many (especially recreational) drug markets have moved from 'open' to 'closed' in recent years (e.g. May & Hough, 2004), cryptomarkets make transactions with unknown customers a vastly less risky undertaking by putting in place a number of protections that have not been previously seen together in a criminal market. First, cryptomarkets protect by hosting their websites website on The Onion Router (Tor) network. Tor makes it exceptionally difficult for anyone – including law enforcement agencies – to monitor the activities of individuals and websites, effectively making cryptomarket vendors near invisible and difficult to trace. Second, payments are made with the digital peer-to-peer cryptocurrency, 'bitcoin', the use of which is difficult to connect with users' real life identities. Third, cryptomarkets enforce a strict escrow system. Although buyers pay up front for their purchases, payments are only released to vendors when the delivery is confirmed. In case of a dispute, cryptomarket administrators adjudicate. Finally, vendors' reputations from previous transactions are made available through eBay-style 'feedback' for buyers to assess before purchases.

All this means that cryptomarket vendors are effectively able to trade in an environment with many fewer of the risks typically associated with drug markets, including non-payment from customers, theft of product and cash, and violence (Bouchard, 2007; Bouchard & Tremblay, 2005; Levitt & Venkatesh, 2000; Reuter & Kleiman, 1986). Recent research using a case study approach suggests that vendors commence

trading because they perceived the cryptomarkets' infrastructure to be "low risk, high traffic, high mark-up, secure and anonymous" (Van Hout & Bingham, 2014: 183). This assessment, however, is premised on the characterisation of cryptomarkets where only the vendors are drug dealers. If cryptomarket customers are also drug dealers sourcing stock there, the extent of this already substantial innovation becomes even greater. Indeed, cryptomarkets would not only alter the way business is done at the retail level but at the wholesale and retail level. The impact on the structure of drug markets would be even greater since a larger number of participants would be users of cryptomarkets and could increase their security.

2.3 Aims of the analysis

Our first and overarching aim here is to develop an understanding of cryptomarkets as a criminal innovation connected to the potential that they may serve customers who are drug dealers sourcing stock, therefore at least in part using a 'business-to-business' model. Christin in his attempt to document, characterise and quantify *Silk Road 1*, the first cryptomarket launched in 2011, concludes that "the quantities sold are rather small (e.g., a few grams of marijuana)" (Christin, 2013 p. 218). Martin (2013) suggests that Silk Road's sellers were importers and cultivators, selling directly to consumers, literally bypassing the wholesale 'middle' level of the drugs market. Getting a handle on precisely how much of cryptomarkets should be characterised as selling 'business-to-business' requires looking at the revenue generated by large versus small quantity listings, and not just at the listings themselves, as Christin did in his analysis.

2.4 Data collection

Data for this section were collected using the DATACRYPTO, the development of which is described in Section 5. This tool is a web crawler that indexes all of the web pages on a website, extracts the relevant information and then stores it in a database. It is therefore very similar to what Google does with the entire 'clear net' – but on a much smaller scale.

Table 1: Distribution of listings across cryptomarkets

MARKET	N
Abraxas	161
BlackBank	350
Evolution	10,988
Nucleus	604
TOTAL	**12,103**

Table 1 presents the distribution of listings by marketplace that were collected by DATACRYPTO during one crawl in early 2015. For each listing, we extracted the type of product being sold, the price of the

listing as well as the number of feedbacks posted by past buyers. Originally, 48,201 listings were collected[1] but a number had to be removed from the dataset because: 1) of a missing *type of product* field in the listing (n=1,869); 2) of a listing price of $0 USD (n=49) and; 3) because of a listing price over $50,000 USD[2] (n=33). As past literature has focused on drug dealing on cryptomarkets, we also removed the 34,507 listings that were for other types of products[3]. We were left with a total of 12,103 listings.

2.5 Measurements

We collated data pulled from listings (N=12,103) for six categories of drugs: cannabis (n=4,031), ecstasy (n=2,354), opioids (n=67), prescriptions (n=1,852), psychedelics (n=1,433) and stimulants (n=2,366).

It is not possible to determine, on the basis of the price or quantity of a transaction alone – without asking buyers themselves – whether a purchase is for resale or for use. An ounce of marijuana can, for example, be the purchase of someone stocking up for daily personal use, or the purchase by someone planning on profitable resale (or indeed both). Moreover, we know that a substantial grey area exists in the phenomenon of 'social supply'. Coomber and Moyle (2013) argue that 'social' drug supply, often known in the UK as 'sorting' amongst friends (Aldridge, Measham, & Williams, 2011), is a common way that friendship groups share supply activities in ways that are essentially non-commercial, or only minimally so. Social supply cannot neatly be categorised either as the actions of drug dealers nor of those purchasing for personal use only; it contains elements of both.

We settled on an inductive solution after various data exploratory strategies were employed. First, we ordered drug listings by purchase price, from lowest to highest. Then we explored drug purchase price by dividing the sample of listings into various quantiles (equal sized groups), and examined the minimum, maximum and mean prices in the quantiles when the sample was divided into two, three, four, five and six quantiles. For reasons we describe in the results, we finally settled on summarising and presenting the listing data in quintiles (five equally sized groups) by *price* in the following ways:

1. The price range including maximum and mean for each quintile in USD.
2. The mean number of sales per year which is measured by the number of feedbacks posted for each listing. This measure is an indication of the number of sales a vendor should expect to make on any given day. This is the same proxy transaction measure that was used by (Christin, 2013).
3. Sum of yearly revenues for all listings in each quintile which was measured by the product of the number of sales for a listing by its price.
4. The market share was obtained by dividing the yearly revenues of all listings in a quintile by the sum of all sales across all quintiles of a drug type. This provides an estimation of the relative importance of a quintile across each drug type.

---

[1] The scrape also collected 13,133 listings from Agora, the second largest cryptomarket. These listings were not included in our dataset because Agora only lists the last 20 feedbacks for each listing. This limited our ability to estimate the number of sales for these listings and they were therefore removed.

[2] Our experience has taught us that vendors sometimes price their listings at wildly high prices when they are out of stock. This is done so the listing page can stay active while making sure that no one will place an order. The cut-off price for such backorder listings is around $50,000 USD.

[3] These 34,507 listings included many licit and illicit products such as books, computer parts and clothing. They also included a large portion of drug listings that were not categorized into one of the six main categories that were the focused of this section (Cannabis, Ecstasy, Opioids, Prescription, Psychedelics and Stimulants).

2.6 Results

Table 2 summarises the characteristics of the listings when ordered into quintiles by price, for six categories of drugs.

Table 2: Price and market share of listings

	QUINTILE	N	PRICE			MEAN NUMBER OF SALES PER YEAR	SUM OF YEARLY REVENUES	MARKET SHARE
			MIN	MAX	MEAN			
Cannabis (N = 4,031)	1	808	$0.14	$27.88	$15.67	77	$888 327.84	3%
	2	804	$27.93	$57.59	$41.10	86	$2,890,302.96	11%
	3	808	$57.78	$128.10	$88.18	53	$3,692,817.12	14%
	4	805	$128.12	$360.38	$210.89	41	$6,512,002.20	25%
	5	806	$360.80	$29,620.08	$1,445.05	17	$11,737,983.12	46%
Ecstasy (N = 2,354)	1	473	$0.95	$39.92	$20.89	86	$835,859.64	7%
	2	469	$39.94	$107.57	$69.66	55	$1,645,538.52	13%
	3	471	$107.81	$263.76	$172.48	38	$2,942,742.60	23%
	4	471	$264.25	$835.31	$478.40	14	$2,929,819.56	23%
	5	470	$835.85	$22,528.14	$3,024.71	5	$4,278,769.20	34%
Opioids (N = 67)	1	13	$13.63	$34.55	$22.09	6	$2,196.48	2%
	2	14	$36.23	$88.48	$64.46	3	$2,925.00	3%
	3	13	$100.39	$127.60	$113.58	15	$23,332.20	24%
	4	14	$148.32	$285.61	$197.16	0	$0.00	0%
	5	13	$286.79	$1,192.82	$528.06	8	$68,036.40	71%
Prescription (N = 1,852)	1	370	$0.02	$18.88	$9.74	38	$138,666.60	4%
	2	371	$18.95	$47.32	$30.93	41	$446,862.12	14%
	3	370	$47.46	$95.11	$68.60	18	$445,614.36	14%

	4	371	$95.35	$232.68	$147.75	14	$673,121.28	21%
	5	370	$233.32	$16,455.60	$826.57	7	$1,467,367.68	46%
Psychedelics (N = 1,433)	1	286	$0.02	$26.05	$15.12	85	$357,760.80	6%
	2	288	$26.07	$55.86	$39.39	84	$953,197.44	16%
	3	286	$55.88	$122.76	$84.81	74	$1,667,974.20	28%
	4	287	$123.70	$339.62	$209.79	23	$1,338,410.52	22%
	5	286	$340.35	$37,684.99	$1,731.26	6	$1,640,913.12	28%
Stimulants (N = 2,366)	1	474	$0.02	$50.87	$27.37	113	$1 313 801.16	7%
	2	473	$50.92	$104.52	$74.12	116	$3 857 510.88	20%
	3	473	$104.63	$244.51	$162.62	67	$4 960 739.64	25%
	4	473	$245.15	$622.09	$393.08	26	$4 387 809.12	22%
	5	473	$623.95	$39 038.65	$2 781.96	9	$5 087 671.80	26%

Most of the listings in every drug category we examined were for drugs sold at prices consistent with purchases being made for personal use. This was clear for listings in the first quintile for each drug category (that is, up to $27.88 for cannabis; $39.92 for ecstasy; $34.55 for opioids; $18.88 for prescription drugs; $26.05 for psychedelics; and $50.87 for stimulants). These maximum prices seem highly unlikely to be the purchases of drug dealers sourcing stock, because they more typical of prices paid for one or a few doses, depending on the drug in question (Global Drugs Survey, 2013).

However, prices for listings in the top quintile (and in some cases the top two quintiles), in contrast, were in amounts consistent with the hypothesis that purchases were likely to have been made by buyers with re-sale intent; that is, by *drug dealers*. The top quintile (that is, the top 20%) of listings for cannabis had prices that ranged from $360.80 to $29,620.08. Although it is possible that some buyers making purchases of cannabis spending this amount of money *may* have been buying for personal use over a longer term, or perhaps making 'social supply' purchases on behalf of a group of friends, this is highly unlikely to be typical for all purchases made within these 'top quintile' listings. In the other five drug categories in the table too, the price range of listings in the top quintile seems likely to be predominantly aimed at buyers with resale intent. We conclude, on this basis, that about 20% of the listings were aimed at buyers making purchases with resale intent.

That 'top quintile' listings were likely to have been purchased by drug dealers sourcing stock seems even more likely when we look at *mean purchase price* in the top quintile for each drug category: $1,44.05 for cannabis, $3,024.71 for ecstasy, $528.06 for opioids, $826.57 for prescription, $1,731.26 for psychedelics and $2,781.96 for stimulants. These represent purchases in amounts highly unlikely to be typical of buyers making personal-use sized purchases. Indeed, some listings were priced sufficiently highly (in excess of a few thousand dollars up to $20,000 and more) to suggest that some vendors aimed their product at retail level drug dealers with a view to holding stock for long periods, or even to those operating at the wholesale level.

It is not enough to know that there are *listings* aimed at a 'drug dealer' market. We need to know whether the frequency of purchases made in these top-quintile listings – and thus the revenue being generated – were important in understanding the marketplace; if only trivial numbers of transactions were generated with these high-priced listings, then we should rightly conclude that cryptomarkets are, contrary to our hypothesis, primarily a marketplace catering to drug users making purchases for personal use.

When we look at *the number of sales per year* in Table 1, we find that transactions were, predictably, less frequent for the most highly priced listings (except for opioids). So for cannabis, there were 77 sales per year per listing on average in the cheapest quintile listings, and this figure dropped to 17 sales in the most expensive listings. The same pattern occurs for all drug categories in Table 1. However, as the sum of *yearly revenues* makes clear, a majority of the revenue generated for most drugs was for highly priced listings. The highest price top quintile listings generated estimated sales in one year of: $11.7 million for cannabis (accounting for 46% of all cannabis revenue); $4.3 million for ecstasy (accounting for 34% of all ecstasy revenue); $68,000 for opioids (accounting for 71% of all opioids revenue); $1.5 million for prescription drugs (accounting for 46% of all prescription drug revenue); $1.6 million for psychedelics (26% of all psychedelic revenue), and $5.1 million for stimulants, (accounting for 26% of all stimulant revenue). The bottom quintile of listings for the drugs we examined (for amounts unequivocally in 'personal use' quantities), in contrast, each generated only 2-7% of the revenue for the drug categories in the table.

2.7 Discussion

Our findings provide clear evidence that many customers on cryptomarkets will have been drug dealers sourcing stock, and that in revenue terms, these kinds of 'business-to-business' sales are a key cryptomarket business. Moreover, purchase price at the very top end was sufficiently high to conclude that at least some cryptomarket customers were likely to have been operating at the wholesale end of the market themselves. Our results directly contradict the characterisation Martin (2013) makes of cryptomarkets, whose sellers, he says, are importers and cultivators selling directly to consumers, literally bypassing the wholesale 'middle' level of the drugs market. In contrast, we show that cryptomarkets might best be characterised as the very location for the middle level of the drug market. Indeed, cryptomarket seem to have functioned as a virtual broker, connecting upper, middle and retail level sellers.

These second-generation cryptomarkets remain therefore an important criminal innovation, and still not just a kind of 'eBay for drugs'. Before the advent of online availability of bulk-quantity illegal drugs, dealers had to have on-the-ground connections and relationships of trust built with middle level drug dealers and/or importers in order to be able to acquire product (McCarthy & Hagan, 2001; Morselli, 2001), alongside a tough reputation (Topalli, Wright, & Fornango, 2002). With the advent of the cryptomarkets, almost anyone with sufficient technological skills can access stock. In other words, the type of 'subcultural capital' (Thornton, 1995) required to be a drug dealer is likely to be different for those who operate on a cryptomarket. This new breed of drug dealer is also likely to be relatively free from the violence typically associated with traditional drug markets (Blumstein, 1995; Caulkins & Reuter, 2009; Reuter, 2009). Whereas violence was commonly used to gain market share, protect turfs and resolve conflicts, the virtual location and anonymity that the cryptomarkets provide reduces or eliminates the need – or even the ability – to resort to violence. This changes are likely to have a deep impact on the skills needed to succeed in crime markets (McCarthy & Hagan, 2001). In the drugs cryptomarket era, having good customer service and writing skills, having a good reputation via 'feedback' as a vendor or buyers – may be more important than muscles and face-to-face connections.

Accessing drugs in the 'virtual' world is likely to have the consequence of reducing other types of risk too because the cryptomarkets' features (escrow, feedback, mail order) may function to reduce problems with non-payment. As well, the widespread use of credit by drug dealers when acquiring stock, termed by Salinas (2014) as 'black credit', is not possible on a cryptomarket, which operates more like a virtual cash-and-carry business. This makes the bar for market entry (i.e. cash up front for stock purchase) for a drug retailer higher, but also reduces the risk of conflict connected to non-payment of debt. This is not to deny that newer and different risks will not accompany virtual drugs markets, and future research will be required to document these.

Another area of interest will be the internationalisation of cryptomarkets. Silk Road allowed drug users to order from almost any country. Buyers can therefore shop around for drugs that would not be available to them locally, or find dealers with much lower prices. The question remains, however, as to whether drug users will take advantage of online illicit marketplaces to find mostly local suppliers or whether will they, in contrast, seek the best price for their drugs no matter the location. The answer to this will come in the next section.

3.0 THE INTERNATIONAL NATURE OF CRYPTOMARKETS

3.1 Introduction

Cryptomarkets make possible massive and truly global criminal networks. If it proves to be the case that cryptomarkets break down international barriers and allow drug supply to occur amongst criminal operators on a global scale, this contradicts what we know about the nature of traditional criminal organisations, which tend to be both small and geographically contained. We consider here the extent to which cryptomarkets actually do have global reach, and the implications for existing theory about the nature of organized criminal groups facilitated by the Internet.

3.2 The international nature of organized crime

Even today, the most compelling description of how organized crime groups operate given the illegality of their products and services is provided by Reuter (1983). Reuter identifies four characteristics common to most forms of organized crime. First, organized crime groups tend to remain small in size. This reduces the risks of detection by law enforcement and facilitates group members monitoring one another. Second, organized crime groups tend to specialize in a limited number of illicit activities. This specialization increases effectiveness while reducing the risks of detection and disruption by limiting the number of law enforcement agencies that have jurisdiction over the group's activities. Third, organized crime groups often compete with many other similar groups but are unable to control large shares of any one illicit market. This is due to the very low barrier to entry in criminal markets resulting in many newcomers introducing competition, and to the greater risks associated with running an all-too-visible criminal monopoly. Finally, and of particular interest given our purpose here, Reuter explains that organized crime groups tend to be limited in their geographical dispersion. Monitoring associates is easier when they are nearby. Offenders may steal from associates within their own group, and detecting this kind of activity can be difficult, for example in the context of street drug dealing. Monitoring associates who are nearby geographically is therefore difficult even in ideal circumstances, and this problem is intensified when associates are located in other cities, countries or even continents where local knowledge and resources will be limited.

While difficult for the reasons stated above, geographical expansion is not impossible given the right circumstances. Morselli, Turcotte, and Tenti (2010) summarize the factors that can influence the geographical dispersion of criminal groups in two ways: *push* factors and *pull* factors. Push factors are those leading organized crime groups to leave a certain area while pull factors are those that attract a group to a new location. Morselli et al. (2010) have identified a number of domains in which these factors operate, but our purposes here, we will limit ourselves to the push and pull factors related to criminal markets.

Push factors related to criminal markets include the level of law-enforcement in the environment and the level of competition from other criminal groups. The intensity of law enforcement will vary from jurisdiction to jurisdiction, as will the severity of penal sanctions. In some settings, therefore, offenders can operate much more freely from the rule of law, making the risks associated with illicit market participation relatively low. High levels of law enforcement should therefore 'push' away rational offenders who will look elsewhere for more lenient jurisdictions. Competition may also explain why organized crime groups decide to migrate. Competition in criminal markets is known to be high (Reuter, 1983), stimulated by low barriers to entry and a steady stream of new participants looking to replace

individuals who are arrested, injured or who decided to quit. Even if these groups are not seeking to control any one criminal market as a whole, they all seek to control a share of it. Becoming 'established' in these criminal settings is challenging, especially since these groups cannot easily publically advertise or promote themselves given the illegal nature of their work. Organized crime groups must therefore rely on word of mouth to promote their products and trustworthiness. This vastly limits their potential to grow and to build a reputation that can be leveraged against competing groups. In this context, it may therefore be easier to relocate than to compete.

When the decision to migrate or expand is made, organized crime groups must select suitable destinations, and the factors that determine which locations are chosen are the 'pull' factors. First, these groups may select destinations with high demand for the products and services they offer. So, for example, illegal drug producers in Europe may wish to expand to countries like the US because of the large domestic demand there for illicit drugs. Moving close to customers is important but so might be moving closer to suppliers. Organized crime groups may decide to move closer to where their products originate in order to reduce the number of intermediaries or the ability of law enforcement to intercept their products *en route*. Lax law enforcement in new jurisdictions is another factor that might 'pull' groups to a new lower risk environment for them to operate. Lax law-enforcement is often associated with high levels of corruption within local agencies of criminal justice, thereby reducing the risk that law-enforcement in these prospective new jurisdictions may increase their interdiction efforts in the future.

The work of Reuter (1983) and much of the research summarized in the report by Morselli et al. (2010) base their conclusion on empirical data collected in connection to traditional organized crime groups involved in well-known activities such as the illicit drug trade, bookmaking and loan sharking. In these situations, it easy to understand how difficult it would be for an organization to expand geographically while simultaneously monitoring the activities of associates and evading arrest. Nevertheless, what we have witnessed with drug cryptomarkets is just that: drug supply on a truly global scale. Vendors can purchase their products locally and decide to sell them online to customers either in their own country or in multiple countries around the globe. Vendors who do not have the local contacts to supply products can also go online to purchase in bulk and then resell either online of offline in their own country. The aim of this section is to contribute to this understanding of internationalization of organized crime groups by studying the international features of cryptomarkets.

The decision to ship drugs across international borders is an important one for vendors because of the higher risks involved. Indeed, sending illicit products through the mail to other countries subjects the sender and receiver to higher scrutiny as the packages may be inspected at the border when leaving one country or entering another. It also increases the time for delivery, time during which the buyer's payment is held into escrow. As many international deliveries may take up to a few weeks or more, vendors will have the hurdle of trying to finance their on-going operations while waiting for the payments from these international sales to clear. And if a package is seized at a border, a vendor will have to deal with a dissatisfied customer and the risk of receiving negative feedback as a result, as well as being out-of-pocket for the transaction, perhaps even re-sending a fresh shipment to resolve the problem. Finally, vendors who sell internationally will have to deal with buyers with diverse in backgrounds, language and culture. This increases the risk of miscommunication arising from a lack of understanding between the buyer and the vendor.

Cryptomarkets administrators and their users are aware of the risks associated with international shipments. Vendors are able to indicate which countries outside their own (if any) that they are willing to ship to, and buyers are given the option to restrict their product searchers to only those vendors located within their own jurisdictions. Shipment to some countries may be perceived to carry more risk than

others. Australia for example is known to inspect almost all of the packages that come in or out of the country in order to stop contraband and untaxed sales of legitimate products (Martin, 2014). On the other hand, some vendors will be located in countries where demand for their products is low. As such, it may be difficult for vendors in smaller countries in Africa, South America and Eastern Europe to find customers in their own countries. For example, many prescription drug vendors are located in India, but with prescription drugs little regulated in that country, the domestic market for these drugs will be minimal (Unnikrishnan & Arathoon, 2008). These often-conflicting factors combine to determine whether vendors elect to sell domestically or internationally.

These decisions will determine the impact cryptomarkets have within and outside of illicit markets. Cryptomarkets have been described as worldwide markets where anyone can make purchases from anywhere (Martin, 2014), thus allowing access to rare or otherwise locally unavailable drugs. It also holds the promise to reduce price asymmetries and increase therefore competition between organized crime groups who were once protected by the lack of competitors in their area. To understand the impact that cryptomarkets are likely to have, it is essential to understand whether they are geared towards one large international market or a series of smaller domestic markets. The aim of this paper is therefore to better understand the true international footprint of cryptomarkets, to evaluate the presence of each domestic market (listings that only sell to customers in the same country as the vendor) and to understand the factors that explain the vendors' decision to ship internationally or not.

Our hypothesis is that vendors located in countries with a substantial market will generally elect to sell only domestically. However, vendors located in smaller countries, or in locations with little local demand, many will have no choice but to sell internationally. The overall sales generated by domestic listings should therefore be higher than those of international listings.

3.3 Data and methods

The data for this section come from a scrape of five cryptomarkets (Evolution, Nucleus, Abraxas, BlackBank and Silkkitien) that was taken in early 2015. Initially, the scrape collected 50,463 listings[4] but 14,633 listings were removed from the dataset for a number of reasons: 1) 5,375 because the country of origin of the vendor was missing; 2) 9,126 because the country where the listings could be shipped to was missing; 3) 427 because the price of the listing was missing and; 4) 65 because the price of the listing was over $50,000 USD. Table 1 presents the distribution of the remaining 35,831 listings.

[4] This number of listings differs from that in Section 2 because it includes all of the listings, not just those that were advertising illicit drugs. It also adds another market, Silkkitien, that was not included in Section 2 because its listings were not classified properly.

Table 1: Number of listings collected on cryptomarkets

MARKET	NUMBER OF LISTINGS
Evolution	28,939
Nucleus	3,496
Abraxas	1,722
BlackBank	1,022
Silkkitien	652
TOTAL	**35,831**

Evolution is by far the biggest market with over 28,000 listings. The other four markets have between 652 listings (Silkkitien) and 3,496 listings (Nucleus). Over 90% of the listings collected were for illicit drugs though a number of them also sold other illicit goods and services like stolen credit card numbers and stolen credentials for online accounts for Netflix or Amazon.

To understand the international nature of cryptomarkets, we began by measuring the distribution of listings geographically. To do so, we identified the countries with sufficiently substantial numbers of listings for inclusion in the analysis, and therefore calculated the number of listings per country for the 12 most popular countries from which listings were shipped to or from. We also identified the 12 most popular countries based on the sales they generated. In many cases, vendors indicated that they could ship from broad regions (ex: Europe, Scandinavia). All of those listings were grouped together under the *Broad region* label. A final group of listings indicated that they were shipping from or to fake countries (e.g. 'Torland', 'United Snakes of Captivity'). These listings were grouped together under the *Unknown country* label.

We then divided the listings into two categories: those that only shipped within the country of the vendor (*domestic* listings) and those that were available for shipping outside of the vendor's country. We calculated for both groups the number of listings as well as the mean revenue each listing generated and the sum of all listings within that category.

Finally, we built a logistic regression model that predicted the decision of vendors to sell domestically or internationally. The dependent variable in the model is a dichotomous variable where *0* means that the listing is only shipping domestically and *1* means that the listing is available outside of the vendor's country. The independent variables were generated deductively using past research on the mobility of organized crime group activities (Morselli et al., 2010) and are divided into three categories. The first pertains to the listings' characteristics; namely their price (logged) and the number of feedbacks they received (logged)[5].

The second category is related to the vendor's characteristics, which include the vendor rating, the diversity of the products vendors listed, and the number products vendors listed in total. The vendors' rating is a dichotomous variable where *0* means that vendors have a rating that is less than 95% positive while *1* means that the vendors have a rating that is 95% positive and over. Christin (2013) showed that

[5] The number of feedbacks is used as an indicator of the number of sales generated by listings.

feedback of vendors on *Silk Road 1* were almost exclusively positive. Given the large number of vendors competing for the same customers, it is safe to assume that it will almost always be possible to find a seller with a very high (95% positive and over) rating. The 95% mark separates vendors who are seen as reliable (with perhaps a few problems here and there) and those that are seen as problematic or possibly problematic. The diversity of products is measured by the number of categories of products for sale that a vendor lists. A vendor selling drugs in the categories *MDMA*, *cannabis* and *cocaine* would therefore have a diversity index of *3*. Vendors often have multiple listings active at any one time. This is especially true for very active vendors who have a wide customer base. We control for this level of activity by a measure of the number of vendor listings. Vendors with many active listings might be better organized and more professional, and perhaps more able to stealthily ship products internationally. This could impact the vendors' decision to ship internationally or not.

Finally, the third category of independent variable includes country and market level characteristics such as the drug expenditures in the vendor's country (logged), the level of law enforcement, the corruption level and the number of competing listings. The drug expenditures measures comes from the UNODC World Report (2005) and is a proxy for the domestic demand for illicit products sold on cryptomarkets. Although not all listings were drug related, the vast majority are, meaning that the market for illicit drugs should be a good indicator of each national demand for products sold on cryptomarkets. The level of enforcement comes from the Global Peace Index (as reported by the University of Sherbrooke, 2014) and ranges from *1* to *4* where 4 is the highest level of enforcement. This measure is based on the number of police officers per 100,000 population. The corruption level rangers from *0* to *100* where a score of *100* represents a highly corrupted country. It is measured annually by Amnesty International (Amnesty International, 2014). Finally, the number of competing listings measures the number of listings for the same type of product in the same country. This variable allows us to measure domestic competition among vendors and we would expect that a higher level of competition would drive vendors to sell more internationally than domestically.

Because some listings were listed as being shipped from/to broad regions or from/to unknown countries, country characteristics could not be derived, so these listings were removed for the logistic regression. 14,727 listings were therefore removed leaving with 21,104 valid listings.

3.4 Results

Cryptomarkets are thought to attract vendors from many countries around the world. Table 2 presents the distribution of these vendors based on the country from which they ship their products.

Table 2: Distribution of countries from which vendors ship

SHIP FROM	N	%
Broad region	14,346	40.04%
USA	5,468	15.26%
China	2,943	8.21%
UK	2,629	7.34%
Germany	2,003	5.59%
Netherlands	1,829	5.10%
Australia	1,403	3.92%
Canada	962	2.68%
Finland	728	2.03%
Sweden	657	1.83%
Poland	375	1.05%
Other countries	2,488	6.94%
TOTAL	**35 831**	**100.00%**

14,346 listings (40.04%) did not list a single country of origin and instead indicated broad regions (e.g. Europe, America, Asia, Scandinavia). Among the countries that were identified, the USA dominated with 5,468 listings (15.26%). That is almost double the next country in the list, China, who has 2,943 listings (8.21%). Other important countries include those in Europe (United Kingdom, Germany, Netherlands, Finland, Sweden Poland), Oceania (Australia) and North America (Canada). 45 countries (grouped under *Other countries*) represented the remaining 6.94% of listings. Among these are somewhat suspicious listings such as 4 listings from North Korea and 1 listing from the Christmas Islands. Still, Table 2 provides empirical evidence that cryptomarkets have been adopted by vendors active on all continents.

Table 3: Distribution of countries where vendors are willing to ship

SHIP TO	N	%
Broad region	28,106	78.44%
USA	3,977	11.10%
Australia	1,329	3.71%
UK	720	2.01%
Finland	640	1.79%
Sweden	430	1.20%
Germany	238	0.66%
Canada	125	0.35%
Norway	56	0.16%
France	53	0.15%
Netherlands	38	0.11%
Other countries	119	0.33%
TOTAL	**35,831**	**100.00%**

Table 3 presents the distribution of countries where vendors are willing to ship. Most vendors are willing to ship across national borders and to broad regions (28,106 listings or 78.44% of the sample). In many cases, these broad regions are strong regional partners. Vendors from the United States are often willing to ship internationally but only to Canada. The same is true for vendors from Scandinavia who are more often than not willing to ship to neighbouring Sweden, Denmark, Norway or Finland. The USA remains the dominant single country with 3,977 listings (11.10%). The other 45 countries only represented 119 listings (0.33%).

Table 4: Distribution of sales based on the origin of vendors

SHIP FROM	SUM OF YEARLY SALES (USD)	%
USA	$29,085,607.20	30.07%
Broad regions	$15,166,764.84	15.68%
UK	$12,342,200.16	12.76%
Germany	$8,957,213.88	9.26%
Canada	$8,502,143.52	8.79%
Australia	$8,274,992.04	8.55%
Netherlands	$6,293,746.32	6.51%
Belgium	$2,120,260.32	2.19%
Sweden	$2,062,386.84	2.13%
France	$594,923.88	0.62%
China	$538,281.24	0.56%
Other countries	$2,790,195.60	2.88%
TOTAL	**$96,728,715.84**	**100.00%**

Although only 15.26% of listings were from the USA, 30.07% of sales were generated by these listings (over $29 million USD). This is almost twice the revenue generated by vendors who sell from broad regions (over $15 million USD). China, the country with the second largest number of listings (8.21%), is in 11th place with a little over $500,000 USD in sales. The other countries listed in Table 4 all have a larger market share than their proportion of listings. The remaining 45 countries (grouped under *Other countries*) generated almost $3 million USD for 2.88% of all sales.

Table 5: Distribution of sales based on the destination of listings

SHIP TO	SUM OF YEARLY SALES	%
Broad regions	$54,359,882.64	56.20%
USA	$26,153,890.68	27.04%
Australia	$8,203,065.96	8.48%
UK	$3,512,284.32	3.63%
Canada	$1,538,633.04	1.59%
Sweden	$1,266,628.80	1.31%
Germany	$578,691.72	0.60%
Finland	$474,456.24	0.49%
Norway	$337,265.76	0.35%
France	$125,043.96	0.13%
Ireland	$67,215.36	0.07%
Other countries	$111,657.36	0.12%
TOTAL	**$96,728,715.84**	**100.00%**

USA customers generated at least 27.04% of revenues on cryptomarkets though that figure could be much higher depending on the number of Americans who are included in the *Broad region*. The bulk of sales (over $54 million USD) were made by listings that offered to ship to broad regions, making it impossible to identify the countries in which these customers were located. Still, we see the same countries listed here as before, namely Australia, UK, Canada, Sweden, Germany, Finland, Norway and France. Ireland appears to be more of a customer than an exporter but is limited with 0.07% of sales destined solely to Ireland generating a fairly small proportion of revenue (over $67,000 USD). Shipments to the other 45 countries (grouped under *Other countries*) were responsible for 0.12% of purchases (over $110,000 USD).

Table 6: On the willingness to ship internationally

	N	Mean yearly revenues of each listing	Sum of yearly revenues for all listings
NOT willing to ship internationally	7,277	$5,613.07	$40,846,288.68
Willing to ship internationally	28,554	$1,957.08	$55,882,427.16

The numbers presented in Table 2 to 5 seemed to indicate that cryptomarkets were geared towards international sales. However, as we can see in Table 6, the 20% of listings made by vendors willing to ship internationally on average generate substantially less revenue ($1,957.08 compared to $5,613.07 for the

listings of the 80% of vendors shipping only domestically). International listings, whilst more numerous, are therefore less profitable. This could be due to two reasons: first, these listings may be for larger/more expensive products. This could mean that purchases made domestically were on average much bigger or that they sold more often. Vendors willing to ship internationally generated the bulk of sales but it seemed to come with a much lower profitability per listing. This confirms our hypothesis that, where sufficient domestic demand (and therefore profit potential) exists, vendors will avoid the risk of international shipping.

Table 7: Logistic regression model predicting the decision to sell internationally

	B	**S. E.**	**Exp(B)**	**Sig.**
Price (logged)	0.108	0.026	1.115	0.000
Number of feedbacks (logged)	0.032	0.022	1.033	0.135
Vendor rating (over 95% positive)	-0.350	0.048	0.705	0.000
Product diversity	0.088	0.010	1.092	0.000
Number of listings of vendor	0.006	0.001	1.006	0.000
Drug expenditures in the vendor's country (logged)	-2.319	0.059	0.098	0.000
Level of enforcement in the vendor's country	1.487	0.098	4.426	0.000
Corruption level in the vendor's country	3.910	0.161	49.887	0.000
Number of competing listings	-0.001	0.000	0.999	0.000
Constant	9.127	0.325	9,202.398	0.000
N		21,104		
Cox & Snell R^2		0.314		
Nagelkerke R^2		0.433		

Table 7 presents the logistic regression model that predicts the decision of vendors to sell internationally. The model is statistically significant (p = 0.000) and is able to correctly classify 77.3% of all listings. The beta (B) predicts the direction of the relationship between the dependent variable and each independent variable. At the listing level, only price is significant and indicates that the higher the price of a listing, the better the odds are that the listings will be available for international shipment. All vendor characteristics are significant and positive with the exception of vendor rating. A vendor with a less than pristine reputation (under 95% positive feedback) may therefore need to sell internationally to find customers willing to buy from them. Vendors' product diversity is correlated with the decision to ship internationally. Vendors who are more active (higher number of listings) are more inclined to sell internationally. Finally, at the country level, higher drug expenditures in a vendor's country will reduce the odds of a vendor opting to sell internationally. The level of police enforcement motivates vendors to ship internationally as does the corruption level of the vendor's country. The number of competitors in a country appears to pull

vendors in that country though the odds ratio for that variable indicates that the impact of completion is very small (Exp(B) = 0.999).

3.5 Discussion

Our results show that cryptomarkets have reached all continents with vendors in over 55 countries. The distribution of listings demonstrates that not all countries have vendors who are equally vested in cryptomarkets. Indeed, a small number of countries control a large proportion of the listings. Vendors appear to come mainly from Western industrialized countries. Customers also appear to come from the same countries though these are harder to track given the large proportion of sales generated in broad regions . In both cases, the fact that many vendors are unwilling or unable to list only one country as their country of origin limits our ability to track cryptomarket users and their online transactions.

Our results indicate that most vendors are willing to ship internationally – or at least to neighbouring countries. These vendors generate up to 58% of cryptomarket sales though it is impossible at this point to evaluate their market share more accurately.

Organised criminal groups usually operate on a geographically small scale. Our research, in contrast, shows that cryptomarkets have made possible sales on an international level. However, our findings also replicate extant theory on this question: the very same risk factors that prevent traditional organised groups from expanding also operate on drug cryptomarkets. Not all cryptomarket vendors are willing to sell internationally, and those that make the choice to do so in spite of the associated risks generate comparatively less revenue than vendors who have the luxury of being able to sell domestically only. Our logistic regression model featured many of the push and pull factors that explain the migration of more traditional organized crime groups. While it is true that cryptomarkets facilitate international sales of products and services, we find here yet more evidence that the Internet, as transformative as it can be, does not change the core of the criminal practices. The results from our model replicates what has previously been found to be true about the migration of organized crime groups.

As expected, a higher level of domestic law-enforcement will push vendors away from a domestic market. Arrests involving cryptomarket participants are still not numerous. Branwen (2015b) has counted 167 cryptomarket arrests, 29% of which were for vendors. Still, the perceived risk of participating in cryptomarkets may be higher in some countries than others and this can motivate vendors to sell internationally rather than domestically. Vendors may hope that should the package be intercepted abroad, it will be difficult for the receiving country to work in tandem with law enforcement agencies in the vendor's jurisdiction to build a case against the vendor. Counter-intuitively, the relationship between the number of domestic competitors and the decision to ship internationally was negative. However, the odds ratio of almost 1 suggests that whatever the effect of domestic competition in decisions to sell internationally, it is small. While competition is an important factor to explain the mobility of traditional organized crime groups, this appears to be less important in cryptomarkets. This could be due to the expansion of the cryptomarkets over the past few years. In a market where there is always more and more demand, competition may be less important as vendors are not truly in a zero sum game. Indeed, it is always possible to increase revenues by attracting the new customers coming into cryptomarkets rather than trying to steal the competitors' clients. As such, while there is competition, cryptomarket vendors may not feel all of the negative aspects of competition in their day-to-day dealings.

Consistent with the literature on the migration of organised crime groups, countries with a high level of demand for illicit drugs will attract cryptomarket vendors looking for customers. Having access to a large demand domestically solves many of the issues that cryptomarket vendors face and may entice vendors

to target these customers in these countries. Vendors in the USA may gain very little by deciding to sell internationally and will likely opt to only sell domestically. In contrast to past research, corruption within a country appears to push vendors to sell internationally rather than domestically. It is possible that vendors in countries with a higher level of corruption may expect to earn less by selling domestically rather than internationally since these countries tend to have lower GDP and vendors who seek to maximize their profits will likely turn to Western industrialized countries to increase the price of the products they sell. Vendors may also believe that should one of their package be intercepted, the odds of being arrested for selling internationally would be much smaller given that law-enforcement in their country could be bribed to ignore the international requests for cooperation. By only doing business outside of the country, the vendors may be protecting themselves are ensuring that law-enforcement turn a blind eye to a practice that is generating revenues domestically.

Our model went above and beyond the known push and pull factors to include some control variables for the listings and the vendors. The online nature of cryptomarkets gives vendors the ability to build an online persona with a reputation. It also allows customers to review the vendors' history and pick the most reliable vendor among the many available. The number of past sales as measured by the number of feedback events is not significant, meaning that large-scale vendors are not more likely to sell internationally than domestically. Vendors who have an excellent rating, however, often decide to sell domestically. This could be because poorly-rated (or unrated) vendors have to offer their goods and services to a larger pool of potential customers, thus taking the risks involved in shipping internationally, given their less than ideal customer satisfaction metrics. The most reliable vendors therefore do not have to take the risk of selling internationally. Product diversity, which could be a feature of more established vendors, is correlated with the decision to sell internationally. This indicates a willingness to offer as many products as possible to as many customers as possible.

We have also demonstrated that while vendors can be found in many countries, only a handful of countries have generated meaningful online sales over the past year. This confirms that whilst cryptomarkets may form important links in the drug trade in the future, their impact in revenue terms for now is limited to a small number of countries.

3.6 Conclusion

Cryptomarket vendors have shown to be willing to ship internationally in many cases. This section's aim was to develop our understanding of why a vendor would accept the increased risks associated with shipping illicit products internationally. We found that many of the factors that explain the migration of organized crime group also explain the decision to sell domestically or internationally. Our results highlight once again the innovative nature of cryptomarkets, which facilitate the globalization of illicit activities. This brings us to the questions we address in the next section. With cryptomarkets facilitating worldwide drug sales, for some selling there in spite of the risks of shipping internationally, interdiction efforts of national and international law enforcement agencies are severely hampered. But is this a wholly negative development, or does this carry with it some positive implications? In Section 4 we consider the positive and negative implications of cryptomarkets for their customers, for the drug suppliers selling there, for drugs markets, and for society more widely.

4.0 ARE CRYPTOMARKETS INEVITABLY A 'BAD' INNOVATION?

It is often assumed that technological innovations are a socially positive development insofar as they drive economic growth, but in reality, innovations will have implications that are both positive and negative. Cryptomarkets specialising mostly in illegal goods and services – which may on first glance be assumed to exacerbate social problems – are a good example of this as they carry with them positive implications. In this section we evaluate the socially positive and negative potential of cryptomarkets.

4.1 Drug users: harm reduction/benefit maximisation versus increased harm

4.1.1 Drug quality and purity on cryptomarkets

Traditional retail drug markets are one specific example of a market in illegal products where customers cannot be assured of getting what they are paying for in terms of the quality of products purchased there. These markets are not regulated, except informally and from within, so a customer purchasing, for example cocaine, does not have recourse criminal or trading standards legislation if ripped off or dissatisfied with the product they obtain when purchased from a local drug dealer. Researchers writing about drug cryptomarkets, in contrast, have argued that customers are much more likely to be able to get the product they set out to buy, and to get better quality products (Barratt, Ferris, & Winstock, 2014).

Although the quality of products sold on cryptomarkets are by no means guaranteed, as is more typical in regulated markets for legal goods and services, there are features of the these marketplaces themselves that have the potential to increase the likelihood that customers will be getting better quality drugs than they might otherwise be able to obtain. The system of escrow, for example, means that payments are only released to sellers from escrow when customers receive and are satisfied with their purchase. Similarly, the eBay-style feedback system allows customers to 'comparison shop' amongst vendors selling similar products and therefore to make judgements on the basis of accumulating feedback for a product/vendor, thereby increasing the likelihood they will be buying a product likely to meet with their satisfaction. Many vendors attempt to be explicit about the quality and purity of the products they list for sale, in some cases providing lab test certificates ostensibly backing up their claims. Evidence, albeit limited, that customers are getting what they pay for is found in the overwhelmingly high levels of customer satisfaction on cryptomarkets, as indicated by the transaction feedback that accumulates for vendors and the products they list for sale. Through this feedback system customers are able to report on issues including speedy delivery, and in many cases, their reported experiences after having taken the drugs. Dissatisfied cryptomarket customers, unlike in traditional drugs markets, have recourse when they are dissatisfied: they can elect not to have their payments released from escrow, they can leave poor feedback scores that future customers can take into account when choosing a vendor for purchase, and the discussion forums associated to the markets can be used to warn future buyers.

Taken together, these marketplace features should reduce the likelihood of users experiencing harm as a result of unintentionally consuming a different drug to the intended one, or a drug of a strength that ought to have been dosed differently (overdoses resulting from variation in batches of street heroin is well documented in the literature; see for example Darke, Ross, & Hall, 1996), or simply not having the drug experience sought, which might at the least be disappointing, even if not distressing or harmful.

Moreover, we know that it is highly likely that at least some cryptomarket customers are not simply drug users making purchases for their personal use, but drug dealers sourcing stock to sell offline in local drugs markets (see Section 1 above). If it is in fact the case that poor drug quality is less likely to result from drug

cryptomarket purchases, then this benefit may effectively be passed on via the products purchased online and then sold on in local drugs markets too.

The possibility that the drugs purchased from cryptomarkets are actually better on measures of quality however, at present remains a working hypothesis. There are a number of reasons that the high customer satisfaction we see evidenced on cryptomarkets is, on its own, not a sufficiently strong indicator of product quality. Drug cryptomarkets are not unique amongst online marketplaces (like eBay for example) in showing generally extremely high customer feedback ratings (Melnik & Alm, 2002), and this must therefore not necessarily be taken at face value. Feedback can be rigged if vendors effectivelyl make their own purchases repeatedly using multiple accounts. Customers too may be unwilling to leave negative feedback for a vendor even if dissatisfied: other vendors may be deterred from selling to a customer who has previously left poor feedback ratings, or who have not allowed their payments to be 'finalised' by releasing their payments from escrow. Moreover, unless customers themselves carry out tests of the products they purchase, they cannot be certain of its quality, or even the psychoactive substance contained. It is difficult to ascertain quality and strength from use alone, given that many cutting agents, for example used in cocaine, include stimulant substances designed to mimic cocaine's effects (Lapachinske, Okai, dos Santos, de Bairros, & Yonamine, 2015). Alongside the profusion of many stimulant-based Novel Psychoactive Substances (NPS) available legally for purchase on the Internet in recent years (ref), opportunities are increased for dealers to sell as cocaine substances that contain little or even no cocaine. Another example of this kind of substitution has been identified for drugs sold as LSD, where more cheaply, and until recently legally, available NBOMe drugs with overlapping psychoactive effects are sold instead (Lawn, Barratt, Williams, Horne, & Winstock, 2014).

The possibility that drugs purchased from cryptomarkets may actually be better on measures of quality remains a hypothesis that needs to be tested empirically. Properly designed research that, for example compares the quality of appropriately selected drugs purchased from cryptomarkets with those purchased on traditional street markets is one way to test the hypothesis. Recent research by Caudevilla-Gálligo (2015) shows positive results on the quality of cryptomarket purchases for 129 samples submitted by cryptomarket customers to Energy Control's testing service. In 120 (93%) of the samples submitted, the drug that customers thought they had purchased was only psychoactive substance detected. The purity of cocaine samples submitted (n = 54) were high (mean 70.4% purity) compared to that we see reported for street seizures in the UK for example, which over the period from 2003 to 2013 averaged at 34% (Burton, Thomson, Visintin, & Wright, 2014).

This brings us to the question that some might ask: is having access stronger/purer drugs always a 'good' thing? Those in favour of prohibition are likely to take the view that a solution to the drugs 'problem' cannot be found by supplying drug users with better quality drugs; indeed, they may see this as exacerbating the problem, proposing instead solutions that prevent drug users from accessing illegal drugs in the first place. Even if we are to accept that it is better for users of illegal drugs at least to get what they are paying for, we know that overdoses sometimes increase when a purer product enters the market and users are unable to adjust their doses accordingly (Darke et al., 1996), and recent reports about 'super strength' ecstasy have reportedly led to deaths (Power, 2015).

4.1.2 Do drug cryptomarkets reduce the non-drug related risks to their customers?

There a number of risks for buyers on cryptomarkets associated with making drug purchases outside of those connected to the use of drugs themselves. Two of these are considered here: the risks posed by being ripped off, and the risk of arrest.

We have already discussed above the chance that drug buyers on cryptomarkets have protections built into the structure of the marketplaces themselves (escrow, eBay-style feedback systems) that reduce the

likelihood that customers will experience fraud: by paying for drugs they do not receive, or by being sold drugs that are underweight or of poor quality, or not the drug ordered. The research referred to above in section 4.1.1 by Caudevilla (2015) is suggestive that drug quality sold on these sites is high compared to street drug quality. Nevertheless, this does not mean that fraudulent transactions are not possible, and evidence of cryptomarket customers having been ripped off by sellers is apparent in the discussion forums connected to these markets. Christin (2013) describes the practice of 'finalising early', which removes the escrow protection offered to customers when vendors insist (for example for 'new' buyers without a proven track record of payments) that a buyer release payment from escrow prior to the shipment having been received. However, taken together, these self-regulating mechanisms should reduce these kinds of rip-offs, and the overwhelmingly positive feedback evidenced on these marketplaces suggests that rip offs are the exception rather than the rule.

The possibilities for customers to be ripped-off, however, are not restricted to those perpetrated by cryptomarket vendors. When cryptomarkets close due to law enforcement shut down, hacks, or market administrator exit scams, all users, including buyers, lose whatever money remains in their accounts. Of the 59 cryptomarket closures documented by Branwen (2015a), 38 (64%) will have involved these kinds of losses, suggesting that even cryptomarkets dominated by honest vendors may close resulting in losses that affect buyers.

Research has demonstrated, for example, that drugs sold in 'closed' drug markets (in which dealers sell only to customers they know or can otherwise trust) are generally of higher quality than drugs sold in 'open' markets where dealers sell to any customer that approaches the marketplace (e.g. Edmunds, Hough, & Urquia, 1996; Lupton, Wilson, May, Warburton, & Turnbull, 2002).

The second consideration is the risk to cryptomarket customers of arrest. In spite of the two major law enforcement crackdowns that involved shutting cryptomarkets in October 2013 and November 2014, the overwhelming majority of drug transactions took place out of the reach of law enforcement. According to Branwen (2015b), as from 24 March 2015, 108 cryptomarket *customers* have been arrested (that is 67% of all arrests for which buyer/seller/operator status is known). Given the many hundreds of thousands of transactions that have taken place on these markets, at least in statistical terms, the proportion of buyers arrested seems likely to be fairly low. However, it is not possible to know how this risk might compare to the risks of making purchases in traditional retail drugs markets, given that offline drugs markets are also more or less hidden so the number of arrests of buyers as a proportion of purchases made is simply unknown. Researchers distinguish between 'closed' markets, in which dealers sell only to customers they know or can otherwise trust, and 'open' markets, in which dealers sell to any customer approaching the marketplace. In open, particularly outdoor markets, the risk to the buyer is tied directly to the transaction itself, and once this has been completed, the link between buyer and seller disappears, with no systematic trace left of the transaction. The closed markets into which many drugs markets have evolved into in recent years typically involves contact between dealers and their customers via mobile phone calls and text messages, so digital traces of the link between buyer and seller are retained and, at least theoretically, traceable. In practice, it seems likely that law enforcement efforts will target dealers rather than their customers, since law enforcement efforts in drug markets are generally resourced in the direction of dismantling markets themselves rather than targeting drug use itself as the problem. The question of whether the risk to buyers though their purchases on cryptomarkets is reduced or increased compared to traditional markets is therefore one we are unable to answer.

The question of whether these hypothetically reduced risks to buyers are a 'good' or 'bad' development again depends on perspective. Those in favour of prohibition are not likely to see the reduced potential for rip-offs or arrests for cryptomarket customers in a positive light, given their potential to facilitate

simplified access to drugs. However, those who take a legalise-and-regulate perspective (e.g. Transform, 2009) are likely to view any developments within drug markets that reduce harm for drug users to be a positive development. So even if cryptomarkets do not 'solve' the harms associated with illegal drug markets by legalizing drugs, to the extent that they reduce harms for users via other means may be seen as a positive development.

4.1.3 Will increased access to illegal drugs made possible by cryptomarkets increase use?

There are two mechanisms through which drug cryptomarkets may generate increased drug use. First, do cryptomarkets make available drugs to individuals who would not otherwise have accessed drugs through traditional markets? And second, might increased access to (potentially) high quality drugs intensify the drug use of those who are already drug users? We take each question in turn.

Martin describes cryptomarkets as networks that:

> "…comprise both vendors and purchasers of illicit drugs who, once online, are able to conduct a range of illicit activities not only on an unprecedented scale, but also with a degree of freedom that significantly exceeds what is possible through conventional, interpersonal criminal networks. […] This suggests that cryptomarkets facilitate a form of illicit drug sales that is qualitatively different from the conventional, offline variety." (Martin, 2014 p. 10).

It is possible, therefore, that the kind of trade facilitated by drug cryptomarkets may not simply replace conventional trade, but supplement it by bringing in new buyers. Christin (2014) has recently underlined the importance of this question for future research: do cryptomarkets simply displace drug purchases from traditional markets? Or do they instead provide access to drugs for those without previous access? The latter derives from the possibility that some potential drug users will have been deterred from accessing traditional drug markets, but are comparatively comfortable in making the anonymous drug purchases afforded by cryptomarkets that do not require face-to-face transactions.

If cryptomarkets do bring in 'new' drug users in this way, this suggests that this new point of access may have the result of increasing drug use prevalence. The question remains an open one: research is required to determine what proportion (if any) cryptomarket customers had not previously accessed offline drug markets. However, it seems unlikely that drug-motivated, but previously abstaining drug users, even if reluctant to access traditional drug markets, will have abstained from use for this reason alone. We know that a high proportion of drug users access their drugs through networks of individuals who are not dealers, not therefore necessarily even requiring access to the traditional retail drugs market. Only 22% of past-year drug using adults questioned in the Crime Survey for England and Wales accessed their most recently taken drugs from dealers; the rest obtained their drugs from friends, colleagues, neighbours or family members (Home Office, 2014). With this in mind, it seems unlikely that previously abstaining individuals who are nevertheless motivated to take drugs but deterred from accessing them via street dealers will have had no other access points.

However, there is a much more persuasive case to be made that cryptomarkets might increase drug use, not by effectively recruiting 'new' users, but by intensifying the use of existing users. This can happen in a number of ways. First, cryptomarkets facilitate customer access to drugs unlikely to be available through traditional local markets. There is a wide range of drugs available on cryptomarkets that might allow users to sample substances they may be interested in taking but to which they do not otherwise have access. This may be particularly the case, for example, for the extremely wide range of (often rare) psychedelic drugs available on these markets, as well as for many prescription drugs.

Secondly, cryptomarkets may facilitate access for drug users such that they may take drugs more frequently or in higher quantities or strengths. We know that large quantity/price purchases are substantial on cryptomarkets (Aldridge & Décary-Hétu, 2014, and see Section 1 above), and some of these purchases will occur amongst those who buy in bulk for personal use, perhaps increasing the likelihood of more frequent or intensive use.

There is also an indirect route through which cryptomarkets may increase the prevalence of drug use. Because we know of the importance of very large volume/price purchases on cryptomarkets (see Section 2.0), it is likely that cryptomarkets serve customers who are drug dealers sourcing stock to sell offline. To the extent that these drug dealers sourcing stock are able to stock a wider range of substances to sell in their local markets, cryptomarkets may have a knock-on effect even for drug users who do not purchase their drugs there, thereby increasing drug use prevalence at a population level.

In sum therefore, it seems possible for all these reasons that cryptomarkets may have the effect of increasing drug use prevalence in population terms, if not by recruiting previously drug-abstaining customers, then by increasing access to a wider range of drugs, or by intensifying drug use for customers who are already drug users. This leads us to a much more difficult question to answer: is this a 'good' thing or a 'bad' thing? The answer to this question depends very much on perspective. For those who view drugs exclusively as harmful, then any increase in drug taking is bad because of the increase in morbidity and mortality sometimes associated with the use of specific drugs. On the other hand, it is not inevitable that we view drug taking as an exclusively harmful undertaking. If we accept, as many commentators increasingly do, that drug taking has benefits as well as the potential for harm, (e.g. Williams, 2012, who has emphasied the pleasures and functions of drug taking), then it is not necessary to view increases in the population prevalence of drug taking as exclusively or even predominantly 'bad'. The case has been made, for example in connection to some psychedelic drugs, for their benefits (Tupper, 2008). The fact that one of the largest categories of drugs for sale on cryptomarkets is in the prescription category suggests that many customers may be self-medicating physical and psychological ill health. And in spite of the potential risks of doing so, some researchers have identified the benefits of self-mediation (Hughes, McElnay, & Fleming, 2001). The answer to the question of whether the potential increases in drug use prevalence that may be facilitated by drug cryptomarkets is a positive or negative development, therefore, requires an understanding of drug use that takes into account harms and risks balanced against pleasures and benefits (Müller & Schumann, 2011).

4.1.4 Do cryptomarkets facilitate access to harm reduction/benefit maximisation advice?

The Internet has revolutionised drug users' access to information about illegal drugs. This has included 'official' government sanctioned websites like the UK's 'talktofrank.com' or the US's National Institute for Drug Abuse website 'drugabuse.gov/drugs-abuse', which take a primary prevention approach to information provision, therefore discouraging all use and emphasising only the risks and potential harms of use. In contrast, we are now also seeing drug discussion forums like 'bluelight.org' and 'drugs-forum.com' that in the main provide participant-generated discussion centring around harm reduction and benefit maximisation (Chiauzzi, DasMahapatra, Lobo, & Barratt, 2013), including, for example, advice on dosing, determining drug content, environment for use, combining drugs, and so on.

An unprecedented development is the provision of harm reduction-oriented advice, information and discussion located directly in the forums attached to drug cryptomarkets. Fernando Caudevilla has provided a detailed description of these forums connected to the majority of drug cryptomarkets (Caudevilla-Gálligo, 2015). Caudevilla is a Spanish physician who began a risk-reduction oriented thread in 2013 on the original Silk Road ("Ask a Drug Expert Physician about Drugs and Health"), and who has since continued this work on two subsequent cryptomarkets (*Silk Road 2* and *Evolution*). These threads

were extremely popular, generating (as from February 2015) nearly 140,000 visits and 1146 questions directed to Caudevilla's pseudonym 'DoctorX'[6]. Caudevilla describes the overwhelming acceptance and support for his contributions in this forum thread, including questions from vendors looking to improve the safety of the products they sold on the markets.

This is an important development because cryptomarkets therefore provide what Caudevilla refers to as a 'virtual setting for harm reduction' (Caudevilla-Gálligo, 2015, p. 3). These forums allow vendors and their customers to discuss issues around drug quality, purity and safer use, which, as Caudevilla points out, provides significant harm reduction/benefit maximisation advantages compared to traditional retail drugs markets. And although any drug buyer can access similarly themed information in forums like bluelight.org and drugs-forum.com, it is a particular strength of cryptomarkets that this information can be accessed in the very location of drug purchase, and in connection to the particular product and batches in question. User-generated harm reduction information will not always be accurate, but the advice provided on these cryptomarkets by a drug expert like Caudevilla provides a credible supplement.

4.2 Harm reduction/benefit maximisation versus increased harm in drug markets

The features of cryptomarkets described above that serve to protect drug-buying customers serve the same function for the drug dealers who operate as vendors there. Just as buyers can examine vendor metrics to select vendors with high trust metrics generated by feedback from previous customers, vendors can examine the same metrics for buyers. Combined with escrow, and marketplace adjudication of disputes, these factors should reduce the likelihood of conflict that is often thought to be associated with offline retail drugs markets. And because transactions are anonymous and conducted in a virtual location, the possibilities for resorted to violence to resolve conflict are reduced or even removed.

Although it may seem self-evident that the virtual location of online drugs markets should reduce violence insofar as interactions there occur in virtual rather than in physical space, this potential harm reduction capacity of cryptomarkets may have limitations. Our research (see Section 1 above) showed that cryptomarket customers are likely to include drug dealers sourcing stock to sell offline. For this reason, cryptomarkets remain 'anchored' in offline drug markets, with vendors there also purchasing offline to then sell online. The requirement, therefore, to operate either wholesale purchase or retail sales in offline drug markets means that cryptomarket users may still be victims and perpetrators of violence connected to these face-to-face transactions. As well, harm can manifest in ways other than real world violence: threats or damage to reputation, 'doxing' (hacking and then threatening to expose identity) and other forms of blackmail, theft and fraud, and cyber-bullying. Finally, the violence associated to drug markets may be culturally, politically and socially conditioned (Bourgois, 2003; Johnson, Golub, & Dunlap, 2006) rather than arising as a function of the illegal market itself. To the extent that these external conditions remain unchanged, the ability of the cryptomarket to reduce violence and conflict may be limited. All these questions must be addressed empirically, but we as yet have no solid evidence that cryptomarkets have, or will, reduce drug market related violence; however, the possibility remains a good working hypothesis.

A further risk to cryptomarket vendors is the risk of arrest. There have to date been two major law enforcement crackdowns on cryptomarkets; the first in October 2013 that shut down Silk Road 1, and the second, 'Operation Onymous' in November 2014 that shut down a number of marketplaces. What was

[6] All cryptomarket forum contributors employ usernames such as the moniker 'DoctorX', but in Caudevilla's case he additionally made his professional identify available; his contributions were not therefore anonymous.

reportedly unique to latter operation, however, was the undercover agent who had been involved from the start of one of the markets, Silk Road 2, working as an administrator (Afilipoaie & Shortis, 2015). As a result, the very aspect of cryptomarkets that provides their users with confidence in the platform – anonymity – may simultaneously undermine that confidence, because anonymity obscures the identities of both criminals and law enforcement actors alike. The risk of arrest to vendors operating on these marketplaces is real, with 46 (29%) of the 161 arrests documented by Branwen (2015b), where the status of the cryptomarket user was known, having been vendors. As was the case with buyers, however, it is not possible to determine if the risk of arrest is more or less likely for drug dealers operating on drug cryptomarkets compared to those operating in traditional retail markets.

This leads us again to the question of whether the characteristics of these markets as they affect drug dealers operating there (the likelihood of reduced conflict and violence, and the possibly reduced risk of arrest) is 'good' or 'bad'. And as before, this depends on perspective. From the point of view of law enforcement, to the extent that cryptomarkets allow drug dealing to take place relatively anonymously and out of the reach of criminal justice agencies, cryptomarkets will not be a positive development where the goal is to prevent drug supply activities. On the other hand, one rationale of law enforcement in cracking down on any drug market is, ostensibly, to reduce the harm associated with these markets, particularly violence. Put another way, instead of deeming cryptomarkets as problematic because the criminals operating there are harder to reach by law enforcement, it may be worthwhile to consider the possibility that cryptomarkets make the harms traditionally associated with this kind of criminality less problematic. We turn now to some of the implications of law enforcement activities for cryptomarkets.

4.3 Law enforcement

Research suggests that law enforcement may exert a 'paradoxical' effect on drugs markets by exacerbating or indeed creating conflict and violence (Moeller & Hesse, 2013; and see systematic review by Werb et al., 2011). Prior to the first law enforcement crackdown on Silk Road in October 2013, the marketplace appears to have been stable and largely devoid of conflict, with vendors energized by a sense that this free market was a near-utopia allowing goodwill to flourish. Its vendors have been characterised as highly customer-oriented, and experiencing a mutually supportive community 'safety net' through participation in the online forums (Van Hout & Bingham, 2013).

Law enforcement actions on cryptomarkets seem also to have had unintended consequences. Within weeks of the first *Silk Road 1*'s closure in October 2013, *Silk Road 2.0* was launched, although by this time a number of rival marketplaces were vying for dominance. One of these, *Sheep*, quickly grew to a size comparable to that of *Silk Road*, but a few weeks later its administrators shut down the site claiming that a user had exploited a security loophole and stole 5,400 BTC of their users' money (at the time worth around in the range of $6 million USD) (Pangburn, 2013), although many believed this was an exit scam by the marketplace administrators abscond with the funds themselves. Throughout 2014, marketplaces grew in size with *Pandora*, *Agora*, *Hydra*, *Evolution* and *Silk Road 2.0* competing to win back the trust of vendors and buyers once the possibility of scams by marketplace administrators became apparent. The most recent exit scam by market administrators occurred on 18 March 2015 when the Evolution marketplace closed with administrators reportedly having stolen 12 million USD from buyer and seller accounts (Woolf, 2015).

In November 2014, cryptomarkets were hit once again by law enforcement agencies from Europe and the United States by 'Operation Onymous', a little over a year after the original operation against Silk Road. This time, multiple marketplaces were targeted including *Silk Road 2.0*, *Cloud 9* and *Hydra* (Department

of Justice, 2014). While many smaller marketplaces were also shut down, only the administrator of *Silk Road 2.0* was arrested, alongside a small number of vendors.

In spite of scams and law enforcement efforts, however, cryptomarkets continue to proliferate. Gwern Branwen, who has been systematically documenting and archiving these markets, counted 43 new markets having opened in 2014 and 46 having closed. Most of these closures, he estimates, were due to scams by marketplace administrators (or outside hacks), with only six closures attributable to law enforcement. Twelve markets remain in operation, nine of which opened during 2014 (Branwen, 2015a). In summary, cryptomarkets tend to have a fairly short life, and their longevity is hampered more due to scams than by law enforcement crackdowns. However, it appears that the profusion of marketplaces occurred as a direct result of law enforcement crackdowns. Moreover, the newer marketplaces that have emerged have tended not to have the same 'ethic' as *Silk Road 1*, which refused to accept listing that sold stolen items, weapons or child pornography (Christin, 2013). Markets emerging subsequent to law enforcement actions have been less restrictive in this regard. So the question of whether cryptomarkets are 'good' or 'bad' is complicated by law enforcement reactions to them.

4.4 Do cryptomarkets provide benefits for wider society?

The obvious objection to cryptomarkets is connected to the illegality of the products and services sold on these markets. Here we consider the implications of cryptomarkets for wider society in relation to the technological innovations they allow or have fostered.

First, cryptomarkets create the promise of anonymous shopping. This may not only be something that buyers and sellers of illicit goods and services value. Indeed, many individuals value their privacy and resist being tracked by governments, by the businesses they purchase from, or by the companies that handle payment systems. Many organizations like the Electronic Frontier Foundation (2015) and the American Civil Liberty Union (ACLU) have spoken up against mass surveillance and the need for privacy. The fear of being tracked is a real one: research by de Montjoye, Radaelli, Singh, and Pentland (2014), has shown that it is possible to identify a specific individual from a dataset of 1.1 million people in 90% of cases simply by looking at their credit card purchases over a period of three months. The trend for anonymous shopping and payment is gaining traction with new services being launched every month. The recently developed 'Dark Wallet' promises to merge payments from multiple sources to multiple vendors (Dark Wallet, 2015). This system combines the payments from multiple individuals to make it impossible to link a purchase to and individual. In practice, law-enforcement could monitor three individuals who have purchased socks, a knife and cannabis but would never be able to prove which customer bought which product. Cryptomarkets may therefore provide some level of protection against companies and governments monitoring individuals. For businesses whose profits derive from facilitating financial transactions, the possibility of anonymous online shopping may be an unwelcome innovation given their vested interest in monitoring customers and learning as much as they can about their consumption habits, thereby reducing the effectiveness of targeted advertising.

Second, the innovations involved in cryptomarkets as they have evolved and developed over the last three years may have implications in the 'legitimate' sphere, particularly in the payment systems. Virtual currencies were not developed for cryptomarkets but cryptomarkets fueled innovation in that field and led to the creation, for example, of 'tumblers' that hide the origin of virtual currencies, providing their users with a increased levels of anonymity associated to their transactions. Another innovation, multi-signatures escrow payments (Buterin, 2014), requires that two out of three parties be involved to make a payment from a virtual currency wallet. This decentralises transactions and removes the need for a

trusted third party like multinational financial institutions (Paypal, Google, even banks). Two individuals may select a random trustee to hold on to the payment knowing that the trustee will never be able to transfer the money without the third party's signature. This holds the promise of reducing fees and the need for large profit-generating financial institutions to take on this role. It also promises to open access to online payments where these were not accessible to certain segments of the population given their limited financial resources or lack of official identification documents. As such, cryptomarkets hold the promise to improve the virtual currencies ecosystem with new modes of interactions and a higher awareness of secure methods of payments. Indeed, as cryptomarkets are used by offenders, the need to protect the participants against opportunistic behavior of others is paramount and a stimulus for creating easy-to-use, anonymous and secure payments. While this may be good for the consumer, it is likely to be seen as a less positive development from the perspective of law-enforcement agencies, who wish to monitor virtual currency transactions. Tumblers hide the true origin of funds and make it more complicated to build cases against offenders.

Third, cryptomarkets are largely believed to be responsible for the explosion in value of bitcoins and, with it, other virtual currencies. The interest in bitcoin was limited before *Silk Road 1* became popular, prior to which very few products and services were available for purchase using the currency, with virtual currencies not accepted by the main online merchants. This is illustrated with widely quoted story in which Laszlo Hanyecz, a bitcoin enthousiast, reportedly paid 10,000 BTC to have someone deliver him a pizza. While these bitcoins weren't worth much back then, even at today's deflated price, these bitcoins are still worth about $2.5 million USD (Mack, 2013). The value of bitcoins has fluctuated in time with the fortunes of cryptomarkets, from the time when *Silk Road 1* was seized, and price of bitcoins fell from a high of $146 USD to a low of $110 USD, a drop of 25%. Some have complained that cryptomarkets have now co-opted bitcoins as the 'drug dealers' dream' (Aron, 2014), with bitcoins are now associated with all things illicit. Furthermore, the fact that bitcoin is so closely tied to the success and failure of cryptomarkets has created extreme volatility in the value of bitcoins. So while bitcoins may now have an 'illicit' reputation following their association with online drug sales, they have still garnered massive success as a result. This has also spurred interest for in cryptocurrencies like Litecoin, which are now being used by many online merchants. Strong virtual currencies provide alternatives for individuals looking to protect themselves against traditional currencies. As time passes, virtual currencies become more and more stable, limiting the risks of associated with unstable currencies. Virtual currencies however limit the state's ability to regulate its economy and financial sector.

Finally, cryptomarkets created a massive surge in the value of bitcoins, thus undermining what was intended to be a decentralised currency. Bitcoins can be acquired either by purchase or by 'mining' them (Eyal & Sirer, 2014). To mine bitcoins, miners must purchase expensive hardware (often in the form of graphics cards) that are used to solve mathematical problems that are rewarded with new bitcoins. This expensive hardware quickly becomes obsolete, making mining something that only well-funded operations that have set up for the purpose of mining can profit from (Chernova, 2015). With bitcoin mining no longer potentially profitable hobby for enthusiasts, the activity is now available only to well resourced entrepreneurs who can afford to continually update the increasingly powerful hardware required for mining, thus to an extent centralising and therefore undermining the dream of a decentralised currency. To the extent that cryptomarkets created a massive surge in the value of bitcoins, cryptomarkets created the impetus for well-funded operations to profit from mining. While bitcoin mining nevertheless generates economic growth, it is not the decentralized, democratic growth that was envisionned by its founder, Satoshi Nakamoto.

5.0 MONITORING OF ONLINE OFFENDERS BY RESEARCHERS

5.1 Introduction

Connected services and devices are more and more a part of our daily lives. We spend most of our days connected to the Internet in one way or another (Oliveira, 2014), so much that it is now difficult to differentiate between time spent online and offline. This is also of course the case for offenders. Offenders converge in online settings to communicate and collaborate with criminal networks for limited periods using a crime-as-a-service model, thereby increasing their efficiency while limiting their risks. In this section we show how researchers can take advantage of this shift to online convergence settings through developing new techniques to monitor and better understand offenders. We divide the tools available to researchers into three categories: mirroring, active monitoring and leaks. We then describe our own experience of developing a tool, DATACRYPTO, that collects all of the vendor profiles, listings and customer feedback on online illicit marketplaces known as cryptomarkets. We conclude with a discussion of the future challenges that researchers will face when using online traces left by offenders for research purposes.

5.2 The rise of the network society

The term *network society* comes from (Castells, 1996) who described the development and adoption of information technologies that have made time and space constraints virtually disappear through instantaneous communications. These changes led to the globalization of social interactions and business relationships, shifting interactions from bureaucratic and hierarchical to horizontal and networked. This created much more fluid communications over multiple coexisting networks (Wellman, 2002), enabling actors to join in or leave as their ability to communicate and participate develops. Network society and the ubiquity of the Internet means that we can now be a part of many networks at the same time (Boase & Wellman, 2006). Relationships inside these networks are sparsely-knit and ephemeral in nature, often connecting individuals who may not share many common traits. Living in a networked society means an increased social network for people both professionally and personally.

A body of literature has adopted the network framework to understand offenders (Krebs, 2002; Morselli, 2009; Sparrow, 1991). Offenders are seen as entrepreneurs who collaborate with other offenders on a project-per-project basis, the 'crime-as-a-service' model (Manky, 2013). This can be seen in the case of online financial fraud where fraudsters will network with hackers to develop a virus that can take over computers and steal credit card information (Holt, Soles, & Leslie, 2008). Once the virus is written, the fraudsters and malware writers split up and may never work together again. Similar relationships exist between fake or stolen prescription vendors and spam specialists. Spammers are hired to deliver ads to potential customers who are directed to websites owned by the prescription vendors. Once the spam campaign is completed, prescription vendors can decide to hire a different spammer or use another method altogether to reach their customers.

This networked social organization has created more than ever a need for convergence settings where offenders can meet, network and advertise their goods and services. Online settings for this activity include discussion forums, chat rooms and newsgroups. Online convergence settings offer both synchronous and asynchronous methods of communications that can be public or private. The opportunity for criminologists is afforded by vast quantity of online traces that allow us to better understand offenders (H. Chen, 2011). Indeed, many settings have now been active for over a decade and

have stored hundreds of thousands if not millions of public messages and member profiles. Not all discussions are strictly professional; as offenders spend time networking with others, they tend to discuss personal and philosophical topics, providing an expanded understanding of offenders and their characteristics. Messages are typically posted online under handles (fake names) but these handles tend not to change over time and across settings, given the time and energy invested in creating the online personas. This enables researchers to use the online communications of offenders as a source of data for their research and to study the evolution of online communities and criminal organizations through time.

Although there is a lack of empirical evidence that 'traditional' criminal organizations have moved parts of their activities online, some hypothesize that the growing profits to be made online will inevitably draw organized crime on the Internet, and emerging research has documenting these in various locations including China and some former USSR countries, and in relation to activities including trafficking and online gambling (e.g. Bhattacharjee, 2011; Broadhurst et al., 2013; Kshetri, 2013; Lavorgna, 2013; Sergi & Lavorgna, 2012).

5.3 The Internet as a source of data in academic research

The Locard principle stipulates that all criminal activities leave traces (Horswell & Fowler, 2004). As we move further and further into an always connected, networked world, offenders are increasingly likely to interact with each other in online convergence settings – and to leave traces of their interactions online. Online traces are starting to be used by researchers and criminologists and can be categorized into three groups: traces gathered through the mirroring of traces, active monitoring of traces and the exploitation of leaks.

Mirroring, also known as web crawling, is the indexing and copying of web pages (Olston & Najork, 2010). This is the technique that Google uses to index the Internet. Crawlers – custom software built to mirror websites – start by downloading a single web page and finding all its hyperlinks referring to other web pages. It then visits the linked web pages one by one, searching for more content to download and more links to follow. This process has the advantage of capturing all of the traces left online on a web site like a discussion forum and requires very little manual work. Moreover, as the crawler downloads the raw HTML code, it is possible to search that code for traces that may be hidden in comments or invisible text. However, crawlers put a burden on web servers. If they are not carefully tuned, they can add such a heavy load to a server that it will be unable to deliver content to regular visitors (Thelwall & Stuart, 2006). Web crawlers are also very easy to detect as they tend to follow a discernible patterns. This allows web site administrators to block them by blacklisting the IP address they come from. To mirror websites, *HTTrack* is commonly used, as it is free and relatively easy to use (Marill, Boyko, Ashenfelder, & Graham, 2004). It must be used in conjunction with other software tools known as web scrapers however. Indeed, HTTrack will only crawl web sites and download web pages. It is therefore unable to extract key information from web pages; that it the web scrapers' role. Web scrapers can be taught what content is important on a web page (ex: name of person posting a message, content of message, date the message was posted on) and then store that information in a database or spreadsheet. This can be challenging if the web pages collected do not have a common layout and/or structure. Indeed, the scraper must be able to recognize the content it needs to extract and doing so requires a certain level of similarity between the web pages.

There are a number of examples of researchers employing mirroring techniques to understand criminal networks. Christin (2013) used the HTTTrack software to index all of the listings, vendor profiles and feedback from the original *Silk Road* marketplace. Chen's work (2012) is one of the most detailed account of how mirroring can be used to gather data on terrorists and other types of offenders. Décary-Hétu,

Dupont, and Fortin (2014) created their own custom tool to download a copy of all of the pirated copyrighted content that was distributed online between 2003 and 2009. Their study demonstrates the importance of peer reputation and the correlates of performance in the hacker world.

A second method of gathering online traces is the active monitoring of the kinds of traces that emerge from the synchronous and more ephemeral communications that occur in online chatrooms and social networks like Instagram, Facebook and Twitter (Fallmann, Wondracek, & Platzer, 2010). Content on these platforms is often short lived and needs to be collected as soon as it is posted, before it is taken down or replaced by newer content. Active monitoring crawlers must be able to monitor server communications, analyze their content and extract the required information from them. These crawlers must be able to deal with large simultaneous influx of data in the case that many individuals share content at the same time. Offenders who network through synchronous communications are typically wary of being monitored, however. They often protect the convergence settings where they meet with passwords or kick out unknown or inactive 'robots' that only listen and never participate in the communications. Active monitoring crawlers must therefore be able to connect and reconnect automatically and to change their online pseudonyms dynamically in order to keep monitoring offenders effectively. Active monitoring provides untainted and direct traces on offenders. Nevertheless, offenders may be aware that their communications could be monitored, and behave accordingly, even if it is difficult for them to keep their guards up for extended periods of time. Chat room and social network communications also generate rich qualitative data that provide in-depth understanding of convergence settings. On the other side, setting up an active monitoring crawler can be difficult and gaining access to the most private convergence setting takes time and requires researchers to interact with offenders and gain their trust. This kind of deception is an ethical issue for researchers regarding the consent of research subjects (Elovici, Fire, Herzberg, & Shulman, 2014) and requires approval by institutional ethics review boards. Another ethical problem is ensuring that collected traces are anonymised and encrypted in order to protect offenders from law enforcement activities.

There are a number of examples of researchers collecting traces in this way to understand criminal networks. Décary-Hétu et al. (2014) used active monitoring to gather data on offenders who carried out discussions in Internet Relay Chat (IRC) chat rooms to build activity logs to detect offenders who use multiple online identities. Franklin, Perrig, Paxson, and Savage (2007) used a similar technique to find that many offenders who sold stolen credit card numbers in these chat rooms were actually scammers trying to steal from naïve buyers. Stone-Gross et al. (2009) monitored hackers in IRC chat rooms who had taken control of over 180,000 computers through the dissemination of a virus, enabling these researchers to understand how the hackers communicated with the infected computers, and how this could be prevented.

The third and final type of trace that can be gathered is known as leaks. Criminal markets are by nature competitive with participants fighting for illicit market share (Reuter, 1983). Given the impossibility of establishing public credibility or to advertise, offenders must use their reputation to find and attract new partners (Décary-Hétu, 2013). As reputation is one of the most prized assets of offenders (Anderson, 1999), it is often reputation itself that is the target of offenders who want to harm their competitors. One way to attack the reputation is to release some of their private information online. This practice, known as *doxing (Coleman, 2014)*, provides researchers with information about the identity of offenders when disclosed in this way. This information is often shared on text-sharing websites like Pastebin where the poster of the information can remain anonymous. Leaks can also target whole convergence settings that are hosted on discussion forums. In this case, discussion forum administrators try to poach participants from other convergence settings by anonymously stealing and releasing a database that contains all of the public and private messages as well as all of the administrative information (IP addresses of visitors,

promotions and rankings) of a competitor's forum. The leak leads the compromised forum participants to move to more secure settings, possibly that of the offenders who are responsible for the leak. Leaks are extremely useful traces as they provide information that would not normally be available publicly. They are however of unknown origin and it is often not possible to verify if the traces have been tampered with in any way. Leaks also tend to be taken down relatively rapidly and so must be downloaded as soon as they are published.

Motoyama, McCoy, Levchenko, Savage, and Voelker (2011) collected leaks from six different forums and measured their social network, market dynamics and regulation. They found that offenders who had a higher status, a good reputation and a large social network were more successful in selling illicit goods online. They also found that many participants were banned from forums, mainly for trying to create multiple accounts to scam others. The work of Afroz Afroz, Garg, McCoy, and Greenstadt (2013) is based on a similar dataset of traces and defines the characteristics of a successful convergence setting. These include a growing number of participants over time, effective official regulation by forum administrators and easy communication tools.

Collecting traces online on offenders provides researchers with new and innovative datasets that are free from the bias of official criminal justice derived data. In many cases, these traces offer a more representative picture of offending communities (see Décary-Hétu et al., 2014, p. for more details) and unbiased data on offenders who had no clue that their interactions would be studied at some point in the future. As valuable at it is however, this methodology requires skills that vew researchers possess. The next section will detail our own experience of developing a research project that collected traces of offenders on drug cryptomarkets. This section will showcase just how time-consuming and difficult it can be to set up a mirroring software even when the researchers have the necessary technical skills.

5.4 DATACRYPTO: A tool for the monitoring of online illicit marketplaces

Using the Internet as a source of data for academic research poses many challenges, even for researchers who are knowledgeable of new digital technologies. In this section, we will review our own experience of developing the DATACRYPTO software, a tool for monitoring the sale of illicit goods and services on cryptomarkets. The function of the DATACRYPTO tool was to automatically log in to these online marketplaces, download a copy of all of the web pages located there, and extract from these the listing and vendor information, alongside feedback posted by buyers.

The first challenge in such a project is to define the specifications of the tool (i.e. what data should be collected and how it should be presented to the researchers). Past research can provide an indication as to the type of data that would be useful to collect. In the case of cryptomarkets, past research either mirrored the web sites hosting the listings and vendor profiles (Aldridge & Décary-Hétu, 2014; Christin, 2013; Dolliver, 2015), or interviewed past and current customers (Barratt et al., 2014). It was important for us to have data on all the marketplace activities, which is a strength compared to interview approaches to looking at online drug sales, which can only access a tiny proportion of vendors who are willing participants. We decided to build on the approach we had previously taken, but this time monitoring multiple markets and merging the resulting data, providing a full snapshot of functioning cryptomarkets.

The first specification of the DATACRYPTO tool was therefore to be able to collect all of the listings, vendor profiles and feedbacks posted on cryptomarkets. The second specification was to limit as much as possible the manual and repetitive work that would be needed to collect this information. Christin (2012) and Dolliver (2015) both used the HTTrack software tool which needs to be configured and launched manually and which does not extract the information from the web pages it collects. We devised the DATACRYPTO

tool from the beginning to be able to work on any cryptomarket. To do so, the software would need some key information to start (ex: username and password to log onto the cryptomarket and the URL of the market) but would be able to adapt automatically to the various layout and structure of markets. The third specification of the DATACRYPTO tool was that it would allow the researchers to analyze the data it collected more rapidly and more efficiently. This meant first and foremost that queries could be run against the data from all cryptomarkets at the same time. This would allow us to quickly build a dataset of all vendors selling (say) cannabis during a period of time no matter what cryptomarket they were active on. Such a feature would allow us to describe and explain cryptomarkets in general and not just the dynamics of a specific cryptomarket. This was important for a number of reasons. First, with the profusion of markets since the closure of Silk Road 1, any one market is unlikely to be representative of all markets, with each marketplace having its own characteristics and features. A database of all marketplaces should allow us to draw conclusions about cryptomarkets in general, rather than produce findings only generalizable to one market. Additionally, cryptomarkets tend to compete with each other for sales of illicit drugs online, and as one closes, vendors tend to shift sales to alternative markets. The DATACRYPTO tool was therefore designed to mix and match data based on queries that take into account specific characteristics of vendors, listings and markets. The resulting database also had to be able to return queries for specific dates (e.g. all listings active in the last month or all listings that were active for at least three months over the past year). The fourth and last specification of the DATACRYPTO tool was to be able to export the output of the queries easily and rapidly. We therefore designed the tool so that it would offer links to comma-separated values (csv) files for each query. This type of data can be imported in most software packages like R, SPSS, Excel or Stata.

The design choices that went into the DATACRYPTO tool required us to plan ahead at least three or four years into our research programme. If DATACRYPTO was to be our main source of data on drug suppliers, it needed to be flexible enough to meet our needs for the foreseeable future. We therefore projected the type of data that we would be most likely to need in the coming years and incorporated it into the DATACRYPTO tool. We also immersed ourselves deeply into the cryptomarket setting to understand the current trends. Our goal was to predict the technological changes that were to come in the community and to design the DATACRYPTO tool in a way that would allow us to work around those changes. One of the early decisions we made was to focus on The Onion Router (TOR) network (Dingledine et al., 2004). This network is used by all of the cryptomarkets to hide the true location of their servers and to protect the identity of their participants. Early on, some cryptomarkets adopted a competing technology, the Invisible Internet Protocol (I2P) (see Zantout & Haraty, 2011 for more details). As both technologies were very different, it would have increased our costs to have the DATACRYPTO tool work on both TOR and I2P. After researching both technologies and following forum postings by cryptomarket participants we concluded that I2P adoption would be marginal for the foreseeable future. This also meant we could save programming costs by creating a tool to work solely on Tor.

By January 2015 the DATACRYPTO tool was completed and functional. The tool can log in to online illicit marketplaces and index all of the listings, the vendors and the feedbacks. If it loses its connection, it is able to log in again autonomously to the markets. It requires very little effort to adapt it when new markets are created. It provides many levels of quality assessment, which allow us to confirm that all of the markets are indexed and that the web pages we download contain what is intended. Summary pages allow us to monitor DATACRYPTO's work and to detect any problems rapidly. Even more importantly, it combines the data collected from all of the marketplaces into one central database. This allows us to query vendor data from multiple markets where they may be active or to draw a picture of the trade of specific drugs across multiple markets, giving us a much more representative view of the state of these markets.

5.4.1 Challenges in the development of the DATACRYPTO tool

Designing a tool like DATACRYPTO involves a series of decisions which all have an impact on the cost of development. For the vast majority of researchers, not accustomed to software development, preparing a budget that accurately costs the work can be a daunting task. Experts, acquaintances and colleagues can be of great help to accurately assess the budget. As we eventually learned (see below for more details), there is no science in the estimation of costs. As a reference point, the DATACRYPTO tool was initially estimated to take about 4 months' time to develop and cost around $13,000 USD.

To find a reliable developer, it is usual to put out a call for bids from developers. These mostly draw the attention of software firms who can charge upwards of $100 USD per hour for their time. Given the limited budget of most research projects, hiring a software firm is often too expensive. An alternative is to work with independent freelance developers who typically bill an hourly wage of $50 USD or less. freelancer.com, a website that manages the hiring of software developers, can be a good starting point. The web site allows someone seeking to hire a developer to post an English language description of their project and to receive bids from all over the world. Developers' profiles show a history of their projects as well as feedback about their previous projects from those who have hired them. Although websites like freelancer.com provide a good starting point for finding developers, in our experience the quality of the work evidenced on these sites varies considerably, and communication can sometimes be difficult given that many developers do not have English as a first language. Researchers can take advantage of the milestone feature of the site which allows those hiring to set deadlines for the different parts of a projects, releasing payment at intervals once milestones have been reached. Our experience with the development of the DATACRYPTO tool has shown us that should a developer miss a deadline, it is better to end the current contract and find another freelancer. Another good practice is to ask that the developer explain in their own words what is expected of them, given that developers may be keen to accept jobs they may not be equipped to deliver. Not all freelancers will be willing to work on the development of tools for researchers, particularly in criminology. Some developers may not have the necessary skill set to build tools that can access the dark net, the part of the Internet that is hosted on the Tor network. Others may fear that online offenders would somehow be able to retrace the developer of the tool and take online (and possibly offline) actions against them. Still, Motoyama et al. (2011) have demonstrated that there is no shortage of freelancers willing to work on projects that involve work on parts of the web where criminals operate. It is nevertheless important to make this clear up front.

Once hired, freelancers need to be managed on a day-to-day basis. Developers often have questions about the specification of the project, and researchers need to keep on top progress. Selecting a freelancer that in the same time zone as the researchers, therefore, can be critical to effective communication. Planning phone meetings and chats can be tricky when there is a large time difference between the researcher and the developer, with one or the other often needing communication to occur outside of typical 9-5 working hours, and therefore sometimes involving intrusion into late evenings or early mornings. This is an often overlooked but crucial issue that researchers need to keep in mind. The developer we hired was one we'd worked with successfully in the past, who had good reviews, and who was skilled in work on the dark net. However, the nine hour time difference between him and us made the kind of real time communication that we needed when we began to notice progress had slowed less feasible. It was only after delays and cursory email replies from him over a matter of weeks that we began to fear that work he was claiming to do was not actually being done. We were reluctant to pull the plug at this stage because of our investment in him and the project up to that point, although in retrospect we should have: his renewed promises to focus only on our project came to nothing, and a few weeks later, we were forced to fire him. Although we considered the possibility of taking legal action, the likelihood of success combined with the effort involved made this not worth our while. We found a local developer who was willing to work on the

project but negotiating the contract was made much more difficult since much of the budget had already been spent on the first developer. In the end we managed to agree on a contract but had to make the concession that the new developer would be allowed to start fresh and not use the previous developer's code. Picking up someone else's code is something that very few developers want to do as it is often more time consuming to learn how something was coded rather than just write it up from scratch. This taught us that a development project that is 70% complete is not very different from one that is 20% complete. In both instances, the software will not work and a new hire will likely have to start over the project. It is therefore essential to keep track of the project on a daily basis in order to make sure that should we need to change the developer, 20% of the funds are invested in the first failed developer and not 70%.

Another issue that researchers may face is the payment method for the developer. Most developers will ask that they be paid regularly (every week, every other week), especially when working on big projects. Researchers must make sure that the Finance Departments at their institutions are able to pay a developer on a weekly or bi-weekly basis. Our University could not accommodate this, and that too ended up being a problem for the project. Although at first only willing to pay on completion of the project, our University eventually ended up agreeing to payment in three parts. However, had we been able to tie progress to weekly payment (as the developer originally wanted), our losses to the project would not have been so great. The second developer delivered the DATACRYPTO tool although even this took twice as long as initially promised. In this case however, regular updates were sent to us and we could talk about the project on the phone.

5.5 Future challenges and conclusion

Online convergence settings offer significant opportunities for researchers to collect traces on offenders. The aim of this section of our report was to describe three ways in each these traces could be collected as well as share our own experience building a tool that could collect traces online. Even though we had extensive technological skills having coded a beta version of the DATACRYPTO tool ourselves, we still faced many issues and challenges during the coding process of the tool. Moving forward, we see three challenges that may limit the researchers' ability to take advantage of traces found in convergence settings.

First, researchers need to develop their understanding of the convergence settings they want to monitor. It is essential that they understand how these settings work and who the participants in these settings are to be able to select the right traces to collect. Each setting has its own characteristics. In the case of cryptomarkets for example, some markets keep all of the buyers' feedbacks while others only show the last 20 feedbacks, severely curtailing the utility of those markets in generating an understanding of transactions. Not understanding the feedback retention policy of a cryptomarket could seriously affect the quality of the analyses. It is also important that researchers develop their understanding of technology. If they are to hire freelancers and develop new tools that are customized for specific convergence settings, they must be able to understand what can and cannot be done and how to do it. It is not necessary here to learn programming languages per se but to understand how web crawling and web scraping works, the type of defences that convergence settings can put up and how they can be bypassed. In the case of cryptomarkets, the login page often includes a CAPTCHA, a series of fuzzy characters meant to block robots from logging in on to the site. Commercial services like DEATH BY CAPTCHA can be used to bypass these CAPTCHA. This service in particular charges as little as a penny to defeat the CAPTCHA system. To do so, it hires hundreds of workers who sit in front of computers, waiting for CAPTCHA to be submitted and solved by them. Understanding the subjects, the traces they leave and the technology they use will be essential moving forward.

The second challenge will be in managing the traces collected. In the case of cryptomarkets, three markets generated almost a 1,000,000 listings from 100,000 vendors over 2014[7]. Aggregating, sorting and manipulating such large datasets is very cumbersome and requires creative thinking. It is possible to break these datasets into smaller subsets but one of the advantages of online traces is that they provide a fuller and representative picture of criminal systems. In the case of copyright fraud for example, Décary-Hétu et al. (2014) demonstrated that it was possible to gather data on much of the fraud that had occurred over the past years. This macro level data allowed him to measure the impact of police operations on a level that had seldom been realized in the past. Part of the solution to this challenge is to invest in bigger computers who can handle this level of data. SPSS, a popular data analysis software package, can now handle tens of millions of rows without difficulty.

Finally, the third challenge will be for researchers to adapt to the constant innovation by offenders. Already we are seeing that convergence settings are becoming more and more difficult to locate using search engines like Google. Tens of financial fraud forums can be found on Google but the more private and elite convergence settings are increasingly accessible by invitation only, so access to these will involve researchers in deception, a contentious practice for researchers. We have also found Russian-speaking forums where the administrators ask prospective participants to answer cultural questions that only Russian-born individuals could answer. Offenders are also taking advantage of legitimate technology like CAPTCHAs and the anti-robot service of CloudFlare to protect themselves from researchers looking to crawl their forum. The CloudFlare service makes sure that humans are connecting to a forum using a series of tests that are difficult for robots to bypass. As more and more research is published using online traces, we can expect offenders to go deeper into the dark web and to become more difficult to monitor. Here again, an understanding of the technology used by offenders will be key to building new software packages that can skirt the hurdles put in place by the offenders. Human intelligence, as opposed to artificial intelligence, will also become more and more important. Very often, offenders will leave clues and links to the more elite or discreet convergence settings in discussion forums and online discussions. It is only by reading through their messages that it will be possible to identify and collect traces from these settings.

So far, researchers have only managed to collect a tiny fraction of all of the traces that offenders have left online. This source of data holds the promise to skirt many of the issues associated with official data or interview data, the main sources of data for criminologists. It also brings researchers much closer to their research subject and removes some of the intermediaries that affect data quality. Using traces brings us much closer to the beginnings of British and American sociology where direct interactions with offenders were valued (Tremblay, 2010). This will require important investments on the researchers' part but, just as our DATACRYPTO tool has, we believe that it is worth the time and effort to do so.

[7] These numbers were calculated by adding the number of listings and vendors active each week. If a listing was active for the whole year, it is therefore counted 52 times in these numbers.

REFERENCES

Afilipoaie, A., & Shortis, P. (2015). Operation Onymous: International law enforcement agencies target the Dark Net in November 2014 *GDPO Situation Analysis*. Swansea: Global Drug Policy Observatory.

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013). *Honor among thieves: A common's analysis of cybercrime economies.* Paper presented at the eCrime Researchers Summit (eCRS), 2013.

Aldridge, J., & Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket "Silk Road" as a Paradigm Shifting Criminal Innovation. *Available at SSRN*.

Aldridge, J., Measham, F., & Williams, L. (2011). *Illegal Leisure Revisited*. London: Routledge.

Anderson, E. (1999). *Code of the street : decency, violence, and the moral life of the inner city*. New York: W.W Norton.

Aron, J. (2014). What's wrong with Bitcoin? *New Scientist, 221*(2955), 19-20. doi: http://dx.doi.org/10.1016/S0262-4079(14)60271-2

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction, 107*(3), 683-683.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction, Early View Online Version*(12 Feb 2014). doi: 10.1111/add.12470

Bhattacharjee, Y. (2011). Why Does A Remote Town In Romania Have So Many Cybercriminals? Retrieved 1 April 2015, 2015, from http://connection.ebscohost.com/c/articles/58844948/why-does-remote-town-romania-have-so-many-cybercriminals

Blumstein, A. (1995). Youth violence, guns, and the illicit-drug industry. *Journal of Criminal Law and Criminology*, 10-36.

Boase, J., & Wellman, B. (2006). Personal relationships: On and off the Internet. *The Cambridge handbook of personal relationships*, 709-723.

Bouchard, M. (2007). A capture–recapture model to estimate the size of criminal populations and the risks of detection in a marijuana cultivation industry. *Journal of Quantitative Criminology, 23*(3), 221-241. doi: 10.1007/s10940-007-9027-1

Bouchard, M., & Tremblay, P. (2005). Risks of Arrest across Drug Markets: A Capture-Recapture Analysis of "Hidden" Dealer and User Populations. *Journal of Drug Issues, 35*(4), 733-754. doi: 10.1177/002204260503500404

Bourgois, P. I. (2003). *In Search of Respect: Selling Crack in El Barrio* (2nd ed.). Cambridge: Cambridge University Press.

Branwen, G. (2015a). 2014 in DNMs: by the numbers. Retrieved 14 March 2015, 2015, from http://www.reddit.com/r/DarkNetMarkets/comments/2r58vs/2014_in_dnms_by_the_numbers/

Branwen, G. (2015b). Tor Black-Market-Related Arrests: A listing of all known arrests and prosecutions connected to the Tor-Bitcoin drug black-markets 2015, from http://www.gwern.net/Black-market arrests

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. *Available at SSRN 2211842*.

Burton, R., Thomson, F., Visintin, C., & Wright, C. (2014). United Kingdom drug situation: Annual report to the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) 2014. London: United Kingdom Focal Point at Public Health England.

Buterin, V. (2014). Multisig: The Future of Bitcoin. Retrieved 1 April 2015, 2015, from https://bitcoinmagazine.com/11108/multisig-future-bitcoin/

Castells, M. (1996). The rise of the networked society: Cambridge, MA, and Oxford: Blackwell Publishers.

Caudevilla-Gálligo, F. (2015). Internet and Drug Markets: A health perspective: EMCDDA.
Caulkins, J., & Reuter, P. (2009). Towards a harm-reduction approach to enforcement. *Safer Communities, 8*(1), 9-23.
Chen, A. (2011). The underground website where you can buy any drug imaginable. *Gawker.* Retrieved 1 March 2014, from http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160
Chen, H. (2011). *Dark web: Exploring and data mining the dark side of the web* (Vol. 30): Springer Science & Business Media.
Chernova, Y. (2015). Bitcoin Mining Company KnCMiner Gets $15 Million Amid Lawsuits. Retrieved 1 April 2015, 2015, from http://blogs.wsj.com/venturecapital/2015/02/03/bitcoin-mining-company-kncminer-gets-15-million-amid-lawsuits/
Chiauzzi, E., DasMahapatra, P., Lobo, K., & Barratt, M. J. (2013). Participatory Research With an Online Drug Forum: A Survey of User Characteristics, Information Sharing, and Harm Reduction Views. *Substance use & misuse*.
Christin, N. (2013). *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Paper presented at the Proceedings of the 22nd International Conference on World Wide Web.
Christin, N. (2014). Commentary on Barratt et al.(2014): Steps towards characterizing online anonymous drug marketplace customers. *Addiction, 109*(5), 784-785.
Coleman, G. (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*: Verso Books.
Coomber, R., & Moyle, L. (2013). Beyond drug dealing: Developing and extending the concept of 'social supply'of illicit drugs to 'minimally commercial supply'. *Drugs: Education, Prevention and Policy, 21*(2), 157-164. doi: 10.3109/09687637.2013.798265
Darke, S., Ross, J., & Hall, W. (1996). Overdose among heroin users in Sydney, Australia: I. Prevalence and correlates of non-fatal overdose. *Addiction, 91*(3), 405-411.
de Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. S. (2014). Unique in the Shopping Mall: On the Re-identifiability of Credit Card Metadata. *High Impact Journal*.
Décary-Hétu, D. (2013). *Le capital virtuel: entre competition, survie et réputation.* (PhD), University of Montreal, Montreal.
Décary-Hétu, D., Dupont, B., & Fortin, F. (2014). Policing the Hackers by Hacking Them: Studying Online Deviants in IRC Chat Rooms *Networks and Network Analysis for Defence and Security* (pp. 63-82): Springer.
Department of Justice. (2014). Dozens of Online "Dark Markets" Seized Pursant to the Forfeiture Complaint Filed in Manhattan Federal Court in Conjumption with the Arrest of hte Operator of Silk Road 2.0. Retrieved 14 March 2015, from http://www.justice.gov/usao/nys/pressreleases/November14/DarkMarketTakedown.php
Dolliver, D. S. (2015). Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel. *International Journal of Drug Policy*.
Economist. (2012). Monetarists Anonymous. *Economist, 404*(8804), 80-80.
Edmunds, M., Hough, M., & Urquia, N. (1996). Tackling local drug markets *Crime detection and prevention series* (pp. 50): Home Office Police Research Group.
Electronic Frontier Foundation. (2015). NSA Spying on Americans. Retrieved 1 April 2015, 2015, from https://www.eff.org/nsa-spying
Elovici, Y., Fire, M., Herzberg, A., & Shulman, H. (2014). Ethical considerations when employing fake identities in online social networks for research. *Science and engineering ethics, 20*(4), 1027-1043.
Eyal, I., & Sirer, E. (2014). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In N. Christin & R. Safavi-Naini (Eds.), *Financial Cryptography and Data Security* (Vol. 8437, pp. 436-454): Springer Berlin Heidelberg.

Fallmann, H., Wondracek, G., & Platzer, C. (2010). Covertly probing underground economy marketplaces. In C. Kreibich & M. Jahnke (Eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 101-110). Berlin: Springer.

Franklin, J., Perrig, A., Paxson, V., & Savage, S. (2007). *An inquiry into the nature and causes of the wealth of internet miscreants.* Paper presented at the ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA.

Global Drugs Survey. (2013). Drug Prices. Retrieved 21 March 2014, from http://www.globaldrugsurvey.com/about/drug-prices

Holt, T., Soles, J., & Leslie, L. (2008). *Characterizing malware writers and computer attackers in their own words.* Paper presented at the The 3rd International Conference on Information Warfare and Security: Peter Kiewit Institute, University of Nabraska, Omaha USA: 24-25 April 2008.

Home Office. (2014). Drug Misuse: findings from the 2013/14 Crime Survey for England and Wales.

Horswell, J., & Fowler, C. (2004). Associative evidence–the Locard exchange principle *The Practice Of Crime Scene Investigation* (pp. 45).

Hughes, C. M., McElnay, J. C., & Fleming, G. F. (2001). Benefits and risks of self medication. *Drug safety, 24*(14), 1027-1037.

Johnson, B., Golub, A., & Dunlap, E. (2006). The rise and decline of hard drugs, drug markets, and violence in inner-city New York. In A. Blumstein & J. Wallman (Eds.), *The crime drop in America* (pp. 164-206). Cambridge: Cambridge University Press.

Krebs, V. E. (2002). Mapping networks of terrorist cells. *Connections, 24*(3), 43-52.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*: Palgrave Macmillan.

Lapachinske, S. F., Okai, G. G., dos Santos, A., de Bairros, A. V., & Yonamine, M. (2015). Analysis of cocaine and its adulterants in drugs for international trafficking seized by the Brazilian Federal Police. *Forensic Science International, 247*, 48-53.

Lavorgna, A. (2013). *Transit Crimes In The Internet Age: How New Online Criminal Opportunities Affect The Organization Of Offline Transit Crimes.* (PhD), University of Trento, Trento.

Lawn, W., Barratt, M., Williams, M., Horne, A., & Winstock, A. (2014). The NBOMe hallucinogenic drug series: Patterns of use, characteristics of users and self-reported effects in a large international sample. *Journal of Psychopharmacology, 28*(8), 780-788. doi: 10.1177/0269881114523866

Levitt, S. D., & Venkatesh, S. A. (2000). An economic analysis of a drug-selling gang's finances. *The Quarterly Journal of Economics, 115*(3), 755-789.

Lupton, R., Wilson, A., May, T., Warburton, H., & Turnbull, P. J. (2002). *A rock and a hard place: drug markets in deprived neighbourhoods*: Home Office.

Mack, E. (2013). The Bitcoin Pizza Purchase That's Worth $7 Million Today. Retrieved 1 April 2015, 2015, from http://www.forbes.com/sites/ericmack/2013/12/23/the-bitcoin-pizza-purchase-thats-worth-7-million-today/

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security, 2013*(6), 9-13.

Marill, J. L., Boyko, A., Ashenfelder, M., & Graham, L. (2004). *Tools and techniques for harvesting the World Wide Web.* Paper presented at the Proceedings of the 4th ACM/IEEE-CS joint conference on Digital libraries.

Martin, J. (2013). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice, October 7, 2013 1748895813505234*. doi: 10.1177/1748895813505234

Martin, J. (2014). *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs*: Palgrave Macmillan.

May, T., & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research and Theory, 12*(6), 549 - 563.

McCarthy, B., & Hagan, J. (2001). When crime pays: Capital, competence, and criminal success. *Social Forces, 79*(3), 1035-1060.
Melnik, M. I., & Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from eBay auctions. *The journal of industrial economics, 50*(3), 337-349.
Moeller, K., & Hesse, M. (2013). Drug market disruption and systemic violence: Cannabis markets in Copenhagen. *European Journal of Criminology, 10*(2), 206-221.
Morselli, C. (2001). Structuring Mr. Nice: entrepreneurial opportunities and brokerage positioning in the cannabis trade. *Crime, Law and Social Change, 35*(3), 203-244.
Morselli, C. (2009). *Inside Criminal Networks*. New York: Springer Science+ Business Media.
Morselli, C., Turcotte, M., & Tenti, V. (2010). The mobility of criminal groups. *Global Crime, 12*(3), 165-188.
Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). *An analysis of underground forums.* Paper presented at the Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.
Müller, C. P., & Schumann, G. (2011). Drugs as instruments: a new framework for non-addictive psychoactive drug use. *Behavioral and Brain Sciences, 34*(06), 293-310.
Oliveira, M. (2014). Canadians spending drastically more time online, comScore study shows. Retrieved 1 April 2015, 2015, from http://www.thestar.com/business/tech_news/2014/11/12/canadians_spending_drastically_more_time_online_comscore_study_shows.html
Olston, C., & Najork, M. (2010). Web crawling. *Foundations and Trends in Information Retrieval, 4*(3), 175-246.
Pangburn, D. (2013). Did One of the Silk Road's Successors Just Commit the Perfect Bitcoin Scam? Retrieved 30 March 2015, 2015, from http://motherboard.vice.com/blog/did-one-of-the-silk-roads-successors-just-commit-the-perfect-bitcoin-scam
Power, M. (2015). Why are pills so strong at the moment? Retrieved 1 April 2015, 2015, from http://www.mixmag.net/words/news/strong-pills
Reuter, P. (1983). *Disorganized crime: the economics of the visible hand*: MIT press Cambridge, MA.
Reuter, P. (2009). Systemic violence in drug markets. *Crime, Law and Social Change, 52*(3), 275-284.
Reuter, P., & Kleiman, M. A. (1986). Risks and prices: an economic analysis of drug enforcement. *Crime and Justice*, 289-340.
Salinas, M. (2014). Black credit. *SSRN*.
Sergi, A., & Lavorgna, A. (2012). Trade secrets: Italian mafia expands its illicit business. *Jane's Intelligence Review*, 44-47.
Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. *Social Networks, 13*(3), 251-274.
Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., . . . Vigna, G. (2009). *Your botnet is my botnet: analysis of a botnet takeover.* Paper presented at the Proceedings of the 16th ACM conference on Computer and communications security.
Thelwall, M., & Stuart, D. (2006). Web crawling ethics revisited: Cost, privacy, and denial of service. *Journal of the American Society for Information Science and Technology, 57*(13), 1771-1779.
Thornton, S. (1995). *Club Cultures: Music, Media and Subcultural Capital*. Cambridge: Polity Press.
Topalli, V., Wright, R., & Fornango, R. (2002). Drug dealers, robbery and retaliation. Vulnerability, deterrence and the contagion of violence. *British Journal of Criminology, 42*(2), 337-351. doi: 10.1093/bjc/42.2.337
Transform. (2009). After the War on Drugs: Blueprint for Regulation. Bristol: Transform Drug Policy Foundation.
Tremblay, P. (2010). Le délinquant idéal. *Performance, discipline, solidarité. Montréal: Liber*.

Tupper, K. W. (2008). The globalization of ayahuasca: harm reduction or benefit maximization? *Int J Drug Policy, 19*(4), 297-303. doi: 10.1016/j.drugpo.2006.11.001

Unnikrishnan, C., & Arathoon, M. (2008). Lax Regulation Sees India Becoming A Haven For Illegal Online Pharmacies. Retrieved 1 April 2015, 2015, from http://www.livemint.com/Home-Page/NFIWys7sX5w4TX7RzrqrKI/Lax-regulation-sees-India-becoming-a-haven-for-illegal-onlin.html

Van Hout, M. C., & Bingham, T. (2013). Responsible Vendors, Intelligent Consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*.

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

Wellman, B. (2002). Designing the Internet for a networked society. *Communications of the ACM, 45*(5), 91-96.

Werb, D., Rowell, G., Guyatt, G., Kerr, T., Montaner, J., & Wood, E. (2011). Effect of drug law enforcement on drug market violence: A systematic review. *International Journal of Drug Policy, 22*(2), 87-94.

Williams, L. (2012). *Changing lives, changing drug journeys*: Routledge.

Woolf, N. (2015). Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear With $12m. Retrieved 1 April 2015, 2015, from http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars

Zantout, B., & Haraty, R. (2011). *I2P data communication system.* Paper presented at the ICN 2011, The Tenth International Conference on Networks, St Maarten, Netherlands.