Crime, Law and Social Change (2023) 80:419–439
https://doi.org/10.1007/s10611-023-10093-y

Following the (DNM) Bible? A crime script analysis of darknet drug vending

Thomas Joyce[1]

Accepted: 22 March 2023 / Published online: 21 April 2023

Abstract

Darknet drug vending appears to be a multifaceted crime. Vendors use encrypted technologies to anonymously access cryptomarkets, engage buyers with effective advertising techniques, and employ stealth methods to send packages to buyers. What remains unclear is how these different methods come together in a single criminal process. This research addresses this gap by conducting a crime script analysis using 25 darknet drug vending 'how-to' guides. The developed crime script is then applied to 50 vendor arrest cases to test its application in practise. The results show that darknet drug vendors display a high degree effort in the completion of their crimes, and may be conceptualised, in partial contrast to traditional market drug dealers, as predominantly rational actors.

Keywords Darknet · Cryptomarket · Drugs · Vendors · Crime script analysis · Rational choice theory

Introduction

Darknet drug vending has been associated with a number of methods, such as anonymising technologies, customer service, and postal shipping. Yet most of these methods have merely been referenced in articles, rather than having been the focus of study themselves. For example, in Christin's now classic 2013 study, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, TOR, escrow, and Mt Gox are all mentioned in relation to the use of the Silk Road, but the article itself deals not with these methods, but with the website's measurement. Even after over 10 years of research into drug based cryptomarkets, research focusing purely on criminal methods appears to be relatively rare. There are some excep-

✉ Thomas Joyce
thomas.patrick.joyce@outlook.com

[1] Università Cattolica del Sacro Cuore, Largo Agostino Gemelli, 1, 20123 Milano, MI, Italy

tions: in 2014, van Hout and Bingham published *Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading*, which characterised the professionalism with which vendors generally treated buyers, and in 2017, Aldridge and Askew published *Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement*, which explored the methods vendors use at the delivery stage. Yet these studies focus on specific methods, rather than the methods used by vendors as a whole. Other studies on methods, such as the provision of free samples (Ladegaard, 2018), specialisation in business-to-business transactions (Aldridge & Décary-Hétu, 2014), and vendor branding (Craciunescu, 2021; Hämäläinen, 2015), while relevant, are even more niche. As these exceptions focus only on specific methods, and are few in number, the majority of methods vendors use to sell drugs on the darknet, and how these methods come together in a single process, remains under-researched. While methods might be studied individually, in reality they function as part of a series, and the totality of how they come together in a single movement has the potential to reveal much about the crime itself, and the criminals who perpetrate it.

Crime script analysis (CSA) (Cornish, 1994) can be a useful tool for conceptualising the process criminals follow to complete a given crime, and it has been employed to successful effect on a number of offences, such as drug production, human trafficking, environmental crime, and the online trafficking of illegal goods (Chiu et al., 2011; Lavorgna, 2014; Savona et al., 2013; Thompson & Chainey, 2011). In contrast to the much of the work conduced on drug based cryptomarkets, which tend to be grounded in quantitative research, particularly the study of market data (e.g. Broséus, et al., 2017; Christin, 2017; Rhumorbarbe et al., 2016; Tzanetakis, 2018; van Buskirk et al., 2016), CSA takes a qualitative approach. The use of qualitative sources, such as case files and how-to-guides, as might be useful for formulating a crime script, has thus far been non-existent in the field–with the exception of data drawn from small samples of interviewees in certain articles (e.g. van Hout & Bigham, 2014; Martin et al., 2020). Recent work also suggests that the fluidity of the methodological process for developing any script may result in scripts being developed in an intuitive manner, with potential for inaccuracies, and low replicability (Dehghanniri & Borrion, 2019). Thus this research was presented with quite a challenge: a lack of suitable data (at least judged by previous work in the field) and an increased empirical burden to develop and refine the CSA methodology in order to use it. Nevertheless, due to its particular capacity for conceptualising criminal behaviour, crime script analysis was still chosen as the methodological framework for this study.

In traditional drug market literature, dealers are rarely conceptualised as being purely rational offenders (e.g. Coomber, 2015; May & Hough, 2004; Reuter & Trautmann, 2009; Salinas, 2017). It has been shown that drug dealers may drift (Matza, 1964) into criminality, rather that decide upon it, and may be motivated by seductive factors (Katz, 1988) such as lifestyle, friendship, ideological belief, and social standing (Jacinto et al., 2008; Parker, 2000; Potter, 2009), in tandem with more economically grounded motivations. Cryptomarket actors have also been considered within a broad theoretical landscape, especially buyers. Notions of trust, harm reduction, conflict management, reputation dynamics, and professionalism have all received attention (Bancroft, 2017; Morselli et al., 2017; Nurmi et al., 2017; Kamphausen

& Werse, 2019; van Hout & Bingham, 2014). However, previous research which applied a cost-benefit framework to darknet drug vending has suggested that vendors are predominately economically motivated actors, who experience an expanded level of rationality beyond the constraints typical of traditional drug dealing (Aldridge & Askew, 2017; Martin et al., 2020). Given the implications of this suggestion for our understanding of vendor behaviour, it may be useful to consider it in light of the entirety of the criminal process; in particular one might question whether the complexity of the crime, the effort involved in its completion, and the skills required to utilise its methods, are indicative of enhanced, or predominantly rational acting.

This research aims to develop a crime script (Borrion, 2013; Cornish, 1994) for cryptomarket drug vending through an analysis of 25 how-to guides and 50 vendor arrest cases. By creating a schema which outlines the different stages which vendors must complete to conduct this crime, and the different events (scenes) and instruments (props) required to complete said stages, this research seeks to enhance our understanding of how vendors commit this crime. Through the use of novel data sources, and the implementation of a step-by-step process for developing a script, this research also intends to further the use of qualitative methods for understanding darknet drug vending. Ultimately, examining the entirety of vendor's criminal process should allow us to analyse possible to behavioural indicators of rationality, such as effort and skill, to determine whether vendor conduct can be considered predominantly rational.

Literature review

Avoiding costs

Anonymity is the driver which affects every aspect of the cryptomarket drug vending process. The internet server, website, vendor profile, monetary transaction, and delivery process are defined by this factor (Aldridge & Askew, 2017; Aldridge, 2019). The aspects of anonymity in relation to encryption (TOR, Tails, PGP etc.), and vendor profiles (the use of aliases, cryptocurrency wallets, etc.) have already been referenced in the literature (Christin, 2013; Martin, 2014b). Users use aliases to conceal their identity, and make purchases through the servers escrow system, making the 'money' difficult to trace (Martin, 2014b). It is especially interesting to note that cryptomarkets *require* these measures of anonymity (Aldridge, 2019). Vendors may even be blocked access to the server for neglecting to conceal their identity (Masson & Bancroft, 2018; Morselli et al., 2017).

Vendors take advantage of the postal services (national post, private courier companies etc.) to ship drugs both domestically and internationally. Their illicit products appear as just another parcel in the mail stream, and thus may go undetected by the authorities. This method eliminates the need for physical contact between the parties, and has the potential, in the case of certain drugs and certain vendors, to bypass the traditional drug market system; drugs being produced in-house and sent directly to buyers, negating drug producers, traffickers, and street sellers. This physical distance, combined with anonymity, also explains why the markets are reportedly non-violent (Aldridge, 2019; Martin, 2014a; Morselli et al. 2017).

Rather than violence being used to deal with conflict, management strategies such as tolerance, avoidance, ostracism, third-party intervention, negotiation, and threats, are employed, both by individual vendors, but also by the market as a whole, through its moderators and administrators who monitor unwanted behaviour (Bakken et al., 2018; Bancroft et al., 2019; Morselli et al., 2017). Each market has its own rules of conduct which must be followed by all users; else they face fines, the temporary freezing of their account, or expulsion from the market (Bakken et al., 2018). Instead of simply benefiting buyers, these rules also benefit vendors by helping to prevent scamming, and to ensure that transactions run smoothly.

Ultimately, even aside from any regulation by those running it, each market acts as a social space, which requires a common security orientation, supported by the mutual self-interest of all users, in order to flourish (Bancroft et al., 2019). By participating in a kind of informal voting, through the provision of feedback, the conducting of sales, and the communication on forums, darknet users signal the vendor behaviours of which they approve and disapprove (Bakken et al., 2018; Bancroft et al., 2019). As buyers select vendors based on established trust, efficiency, stealth, and the quality of their drugs, it behoves vendors to satisfy these requirements (van Hout & Bingham, 2013). In a 2017 study, Décary-Hétu and Quessy-Doré found that buyers make 60% of their total market purchases from the same vendor (Décary-Hétu & Quessy-Doré, 2017). This indicates that a vendor’s reputation: their ability to consistently deliver a high quality service over a prolonged period, is a key predictor of their success (Décary-Hétu & Quessy-Doré, 2017; Nurmi et al., 2017). While not all vendors employ this level of professionalism, it appears that only those that do are likely to achieve lasting and substantive gain.

Gaining benefits

Successful vendors tend to deliver a high-quality service; the drugs sent to buyers typically match the advertised substance and are usually of a high purity (Bhaskar et al., 2019; Caudevilla et al., 2016). The information vendors provide about shipping is also normally accurate (Rhumorbarbe et al., 2016). It may be for these, and similar reasons, that successful vendors are typically characterised as being professional and efficient: avoiding disputes, communicating frequently and politely, and dispatching products quickly (van Hout & Bingham, 2014). As such, it is unsurprising that the substantive portion of feedback given to vendors by buyers seems to be positive (Bhaskar et al., 2019).

In order to market their products successfully, vendors may employ a number of methods. Advertisements may be used to attract/maintain buyers and thereby increase sales, with successful vendors typically posting many listings on their profile pages and advertising their shop on multiple forums (Décary-Hétu & Quessy-Doré, 2017; Paquet-Clouston et al., 2018). Products are typically described in an attractive way, using buzz words and slogans (Zaunseder & Bancroft, 2020). Vendors may also give away free samples, make discounts, and provide offers in order to attract buyers, and promote the reception of positive feedback (Ladegaard, 2018; Zaunseder & Bancroft, 2020).

Vendor branding is also taken seriously. As a vendor's handle is used by buyers to identify vendors, and to review their products, it is intimately tied to their reputation, and is therefore a valuable asset (Hämäläinen, 2015). Different methods may be used by vendors to brand their handle, including icons taken from popular or drug-related culture, and the use of memorable usernames (Hämäläinen, 2015; Craciunescu, 2021). Vendors also tend to specialize by focusing on either a single type of drug, or a particular weight echelon, in order to target specific buyers (Christin, 2017). For instance, one such specialisation could be business to business transactions: supplying other vendors with drugs for resale (Aldridge & Décary-Hétu, 2014; Christin, 2017).

Gaps to be filled

The literature tends to address single points in the criminal process: encrypting technologies, shipping behaviours, or professional conduct (Aldridge & Askew, 2017; Martin, 2014b; van Hout & Bingham, 2013). Many methods are merely dealt with in passing, rather than given focused attention, with some methods, such as money laundering and crime management, not being explored at all. Most pressingly, the overall process of how these different methods come together in a cohesive process remains unclear.

Theoretical framework

Rational choice

In some sense, cryptomarket vendors take cue from the three distinct market levels of the traditional drug markets: upper, middle, and lower level distribution. The potentiality for production (Bakken et al., 2018), and for significant profits, appear to align with upper-level distribution, while the fluidity of roles/operations, and the evidence of business-to-business transactions, (Aldridge & Décary-Hétu, 2016; Christin & Thomas, 2019) may denote the middle-level range. However, due to the interaction between vendor to buyer, the information available to buyers (Bancroft & Reid, 2016), the frequency with which the buyer is also the consumer, the open channels of communication between the parties (Childs et al., 2020), the potentiality for repeat purchases (Bakken et al., 2018), and the typically small amounts purchased (Christin & Thomas, 2019), they may be most readily conceptualised as lower-level distribution markets (Demant et al., 2018). As such, it is unsurprising that the results of much of cryptomarket research have been analysed in light of traditional market drug dealing (e.g. Aldridge & Askew, 2017; Aldridge & Décary-Hétu, 2016; Décary-Hétu et al., 2016; Décary-Hétu & Giommoni, 2017; Demant et al., 2018; Paquet-Clouston et al., 2018).

Rational choice perspectives have been readily applied to traditional market dealing (Jacques & Reynald, 2012). Traditional market drug dealers may employ a number of techniques to avoid the attention of law enforcement, such as reducing their visibility in the public domain, employing clever means of stashing drugs, and using transactional mediation to exchange goods with buyers (Jacobs, 1996; Fader, 2016; Vannostrand & Tewksbury, 1999). Recent work has moved somewhat away from this conception however, considering that other cultural, personal, and institutional factors may play a key role in drug dealers behaviour (Coomber, 2015; May & Hough, 2004; Reuter & Trautmann, 2009; Salinas 2017). Whether they are selling drugs in an open market on the street, or in a closed market in their home, traditional drug dealers are limited by a number of critical factors: their supply of drugs, their access to buyers, and their geographical locality (Coomber, 2006; Reuter, 1983). As drug markets differ greatly from place to place, dealer behaviours cannot always be readily homogenised; techniques used by one dealer in one place to increase gains, may not be used by another elsewhere (Coomber, 2006), as the distinction between open and closed market dealing makes clear (Jacinto et al., 2008; Parker, 2000; Potter, 2009). Dealer rationality may also be bounded: dealers struggling to weigh up costs and benefits effectively due to the lack of information, or the impairing influence of certain personal and contextual factors (Akers, 1990; Cornish & Clarke, 1986; Jacobs & Wright, 2010). Actions may instead be driven by emotion and may be limited by the involvement of organised crime, violence between parties, and the attention of law enforcement. As such, when rational choice is applied to traditional drug dealing, it is seen as a limited force, one which may be used as a means of analysis in certain contexts, such as arrest avoidance, but which should not dominate the array of other factors which influence, restrict, and otherwise cause drug dealing behaviour.

It may be tempting to think, because of the product similarity between drug dealing and cryptomarket drug vending, that the latter can be understood along similar lines as the former. As previously mentioned, many articles on the topic of cryptomarket drug vending ground their analysis, at least partially, in traditional drug market literature (e.g. Aldridge & Askew, 2017; Aldridge & Décary-Hétu, 2016; Décary-Hétu et al., 2016; Décary-Hétu & Giommoni, 2017; Paquet-Clouston et al., 2018). However, the similarities between the two crimes may be overstated, or at the very least, our understanding of traditional drug dealing may be only somewhat applicable to cryptomarket drug vending. Though the methods vendors use have been mentioned in passing throughout the literature, few articles focus on these methods in detail. While it appears, from the variety of methods that are mentioned, to be a multifaceted crime, the extent of the complexity involved in its execution, the skills it demands, and the effort it requires, remain unclear. As such, it is difficult to determine the degree to which vendor behaviour is rational; is it that we can consider darknet drug vending as a quasi-rational crime, similar to its physical world predecessor, or is it that the level of cost-benefit analysis, available information, and event complexity, are sufficient to deem it distinct from its predecessor, and a predominantly rational crime?

Aldridge and Askew, in their 2017 article, *Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement* suggest that due to the data sharing capabilities of darknet vendors, who on forums can freely exchange data about anonymising technologies and stealth techniques, darknet drug vendors are capable of achieving an expanded rationality–one which develops not merely from the experience of the individual, but the multitude (Aldridge & Askew, 2017). This information sharing is formalised, and in some sense, reaches a new height, in the form of how-to guides, in which vendors exchange complete best practises for stages of the crime, or for the crime in its entirety. Recently, Martin et al. explored the differentiated pathways, risks, and rewards of darknet drug vendors by interviewing a sample of 18 vendors, finding that though vendors were in small part affected by the seductions of crime, and conceptualisations of drift, they largely self-reported as being economically motivated (Martin et al., 2020).

This research builds on such considerations by taking a close look at the entire criminal process of vendors, to examine the amount of effort involved in its completion, and the degree to which the skills required therein are indicative of rational offending. In so doing, it questions the possibility of a third argument in favour of conceptualising darknet drug vendors as predominately rational actors: that the knowledge and skills required for this crime are so varied and complex that they mandate a particularly rational approach, causing vendors to closely mediate the space between cost and benefits.

Crime script analysis

Crime Script Analysis (CSA) is useful for determining the procedures that criminals follow to commit a given crime. By outlining all of the actions required for the preparation, execution, and completion of a crime, the given crime can be more easily deconstructed, compartmentalised, and understood (Borrion, 2013; Cornish, 1994). Taking the terminology from the dramatic arts, a script is played out an individual *actor* (the criminal) who uses *props* (the instruments and materials the criminal uses) to commit the crime, which takes place in a series of *scenes* (the activities or events completed by the criminal) (Cornish, 1994).

There is no single categorisation for the scenes of a crime script, and while the original conception of CSA was based on a structured series of conditions and instruments, multiple variations have since arisen, typically devised as suited to the given research aims (e.g. Chiu et al., 2011; Lavorgna, 2014; Savona et al., 2013; Thompson & Chainey, 2011). In relation to drug crime, there have been several script analyses conducted in recent years. In *Script Analysis of Open-air Drug Selling* Sytsma and Piza present a three stage crime script consisting of (1) the pretransactional act (loitering in an area, making contact between buyer and seller, seller giving the buyer a chance to inspect the drugs), (2) the transactional act (greeting, exchanging money for drugs-potentially in different locations), and (3) the posttransactional act (mobility-leaving the scene, to make a deal elsewhere or make purchases with earned cash) (Sytsma & Piza, 2018). In *Drug Dealing: Amsterdam's Red Light District* Jacques and Bernasco relatedly present three facilitating stages, which may be completed depending on the situation: (1) search for a customer (e.g. loiter in a known hotspot and communicate drug dealing signals), (2) solicit the customer (e.g. present drug offer discretely such as by saying the name of the drug softly in the presence of a potential buyer), (3) agree on and go to trade locale (e.g. speak to the buyer and arrange a more discrete time and place to exchange drugs for cash), and two necessary stages, which must be completed for the crime to be executed: (1) agree on trade terms (e.g. agree to sell one customer a certain quantity of a certain drug for a certain price), and (2) make an exchange (e.g. exchange with a customer the agreed upon drugs–potentially committing a minor fraud, such a delivering a smaller than requested amount, to increase profits) (Jacques & Bernasco, 2013). Finally, in 2021, Eric Jardine developed a crime script which outlined the four stages: informational accumulation, account formation, market exchange, and receipt, that buyers must follow to purchase drugs on the darknet (Jardine, 2021). While focused on buyers, this script highlighted several key behavioural factors relevant to all darknet drug market users: the need to learn how to conduct the criminal activity, the development and maintenance of an online profile, the effective understanding and use of market dynamics, and the basic level requirement that the crime must shift from the digital to the physical, with the drugs being delivered from vendor to buyer by post. In some sense, the research at hand is a continuation of these works, but in another, these scripts provide an interesting point of contrast through which the complexity of darknet drug vending can be better understood.

In terms of data sourcing, previous scripts have tended towards interviews and case files, though more contemporary efforts have been able to take advantage of tutorials, guides, and other criminal materials available on the internet (Holt & Lee, 2020; Hutchings & Holt, 2014; Lavorgna, 2014; van Hardeveld et al., 2016). This has proven to be an especially useful method in relation to cybercrime. In 2016, van Hardeveld et al. developed a crime script to describe the process carders use to trade stolen data, using 25 tutorials in which carders teach prospective carders their process (van Hardeveld et al., 2016). Even more recently, in 2020, Holt and Lee developed a three-stage crime script for the sale of counterfeit identify documents using an analysis of 19 specific vendor profiles (Holt & Lee, 2020). The research at hand takes a similar approach by studying the how-to guides and vendor arrest cases to formulate a crime script for cryptomarket drug vending; yet it also seeks to build upon them by advancing the process by which crimes may be scripted.

In their recent study, *Crime Scripting: A Systematic Review*, Dehghanniri and Borrion found that most crime scripts have been generated intuitively, without adherence to a strict methodological process (Dehghanniri & Borrion, 2019). While this may allow for a significant amount of flexibility in the formulation of scripts, this loose approach may result in inaccuracies, and a lack of replicability: there not being sufficient information provided to reproduce the given script. While conceding that scripting methodologies must not be too complex as to become inaccessible and must still be tailored to each crime on the basis of the information available, Dehghanniri and Borrion call for an overall greater methodological clarity in the production of scripts, as this will ultimately lead to higher rates of assurance in the use of crime scripting for understanding crimes (Dehghanniri & Borrion, 2019).

It is as such that this research seeks to create a crime script using sources similar to those previously used in cybercrime research, but which are novel for the study of darknet drug markets, and to follow a step-by-step empirical process in the development of said script, in service of more readily identifiable accuracy and replicability, achieved by using a two part methodology: first developing the script, and then verifying its effectiveness.

Data and methodology

How-to guides

300 guides were downloaded in sets from darknet forums. 115 of these guides were removed from the sample, as they focused on topics which were not relevant to the research, such as social engineering. This left 185 guides that dealt with the sale of drugs on the darknet, which fell into two categories:

1. General guides (3). These guides provided a step-by-step account of the drug vending process in full (e.g. *The Darknet Market Vendor Bible*) and were thereby deemed to be *general* in their nature.
2. Specific guides (182). These guides provided an account of one particular method used to commit this crime (e.g. *Guide to Safe Postal Shipping*) and were thereby deemed to be *specific* in their nature.

160 of the specific guides focused on the growth, manufacturing, or synthesis of drugs. These were also removed from the sample, as they only related to one specific aspect of the crime, which may not apply to all vendors. 22 guides remained, focusing on setting-up anonymising technologies (9), shipping and packing (10), and money laundering (4), which when added to the general guides made for a total of 25. For those guides in which the date of publication was given, the timeframe ranged between 2014 and 2019. Though the guides were all presented in English, they were distinctly international in their authorship, making reference to authorship or the cultural context of the United States of America, the United Kingdom, Canada, the Netherlands, and Denmark. Some of the long form guides, such as *The Darknet Market Vendor Bible*, had a collaborative authorship, from vendors from a variety of European and North American contexts.

In order to determine the preliminary crime script, a thematic analysis of the general guides was conducted. They were read through in full, and their chapter headings and key words, determined on the basis of cryptomarket related proper nouns previously established by the literature (TOR, Tails, PGP, Bitcoin, DNA, Cannabis, Laptop, etc.), were marked. These different terms were then recorded in an excel file, consolidated based on common synonyms (e.g. Bitcoin and Monero being recorded as cryptocurrency) and counted on the basis of mentions/references in each guide. These terms were then used as the basis for the development of the script's stages (e.g. all the guides referenced mail, post, packages, stamps, etc., providing support for the formulation of a stage dedicated to postal shipping). Through this process, six stages emerged: gathering material resources, setting-up software technologies, conducting sales, shipping products, laundering proceeds, and managing operations. These stages were then filled in with methods based on events mentioned in the guides (scenes) and materials referenced as necessary to complete those events (props).

The specific guides were then used to enrich this preliminary crime script. The different methods used to complete each event in the criminal process (pathways) listed in the guides were included in the script, and the further information about different scenes and props were added. These results were then combined with a content analysis of all guides, and an overall understanding garnered about the phenomenon from the literature, to formulate the crime script.

Vendor arrest cases

In order to confirm the validity of the crime script, its use was tested against the recorded events and materials employed by arrested darknet vendors in the completion of their crimes. At the time of research, on the website www.darknetlive.com 154 arrest cases were listed, ranging from 2013 to 2021. In order to be included in the research these cases had to:

1. Deal with a drug vendor; sellers of weapons, counterfeit money, pornography, and other illegal services were omitted.
2. Be verifiable; supported by an official documentation from a judicial or law enforcement body.
3. Be available; accessible as downloadable case files from www.pacermonitor.com.

Once these exclusionary criteria were applied 50 cases remained, and were collected, for the research. Pacermonitor was used as an access point for case files as the majority of vendors listed on Darknetlive were American, and it allows open access on case files which, in many other jurisdictions, would be redacted or confidential. While this did create a strong bias towards American vendors, not all of the arrested vendors were based in America, some had been extradited or were merely arrested there.

In order to proceed with the analysis, the 50 downloaded cases were read through in detail. A tabled version of the crime script (which contained individual cells, each of which denoted a single scene, and its related props) was used to check and record the reference to relevant information in the arrest cases. When a key word denoting a particular prop, or information pertaining to a particular scene (such as photographs, descriptions, and other evidence) were presented in a given arrest case, a value increase of 1 was denoted in the relevant section of the tabled script. By this measure, the frequency with which the criminal process described in the cases reflected that of the crime script was determined.

Results

The following crime script for darknet cryptomarket drug vending was produced (Fig. 1).

As is apparent from the above figure, this crime script featured six stages which must be completed in order to sell drugs on darknet cryptomarkets.

First, the vendor must gather the necessary resources. This stage relates to the gathering, and subsequent use, of the hardware and materials necessary to commit the crime. Vendors must have a laptop or computer device to access the darknet; a means of creating address labels, preferably a printer; access to drugs, be they sourced, manufactured, or grown; access to an anonymised Wi-Fi connection (one which is

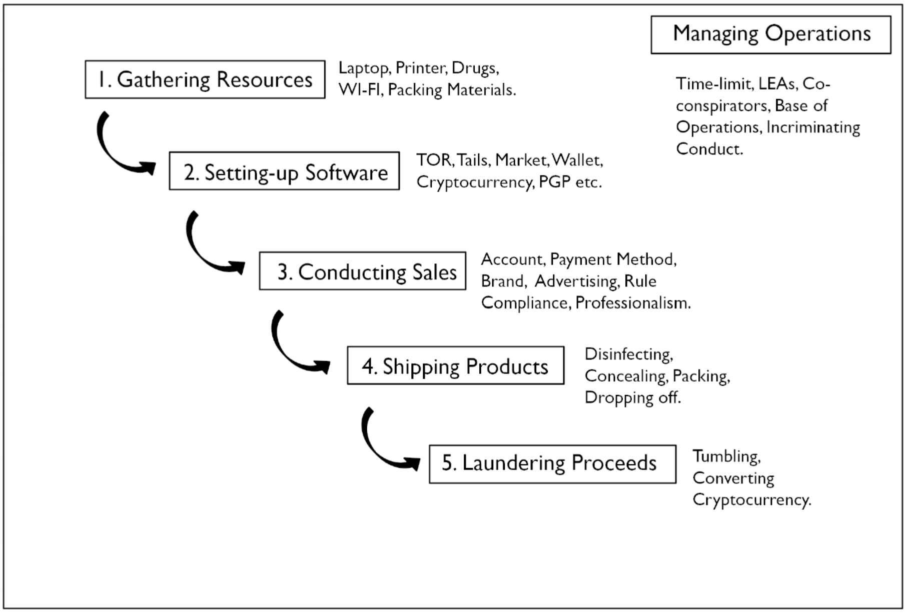
Managing Operations
Time-limit, LEAs, Co-conspirators, Base of Operations, Incriminating Conduct.
1. Gathering Resources
Laptop, Printer, Drugs, WI-FI, Packing Materials.
2. Setting-up Software
TOR, Tails, Market, Wallet, Cryptocurrency, PGP etc.
3. Conducting Sales
Account, Payment Method, Brand, Advertising, Rule Compliance, Professionalism.
4. Shipping Products
Disinfecting, Concealing, Packing, Dropping off.
5. Laundering Proceeds
Tumbling, Converting Cryptocurrency.

Fig. 1 Crime Script for Darknet Cryptomarket Drug Selling

not connected to their personal identity), and the packing materials necessary for the shipping stage of the crime.

Second, the vendor must set up their software technologies. This stage relates to the gathering, and subsequent use, of the software necessary to commit the crime. Vendors use an anonymous internet browser (such as TOR) to access the darknet; encrypted operating systems (such as Tails) to protect their anonymity; a cryptomarket to sell their product; a cryptocurrency wallet; and encrypted communication software (such as PGP).

Third, the vendor must conduct sales of their product. This stage relates to the technical and commercial considerations vendors account for in order to make sales and profits. Vendors set up and use a cryptomarket account; use a payment method (such as escrow) to complete transactions; create a brand for their account to attract buyers; advertise their products through appropriate language, relevant information, pictures, and offers; follow the market rules and regulations; and engage in quality customer service, seeking to appear polite and reliable in order to maintain their customer base.

Fourth, they must ship their products to buyers. This stage relates to the packing and dropping off of drug parcels. Vendors pack parcels using precautionary materials (such as latex gloves and rubbing alcohol) to ensure that their DNA and/or fingerprints do not get on the parcel or its contents; use special materials (such as vacuum sealed bags and mylar) to impede the use of scans and sniffer dogs to detect drugs inside the parcel; employ decoys (such as food items or children's toys) to conceal the drugs when shipping their products internationally; ensure that the exterior of the package appears professional (such as through the use of a legitimate return address and printed labels); and drop their parcels off at postal services in a manner which is not easily traceable, and does not arouse suspicion (such as by using postal mail bins at night).

Fifth, they must launder their proceeds. This stage relates to cleaning of illicitly earned cryptocurrency so that it can be saved or used without arousing suspicion. Vendors tumble their cryptocurrency (using online applications such as Bitquick or methods such as peer-to-peer mixing), and then convert it into fiat currency (using methods such as Bitcoin ATMs or Crypto debit cards).

Sixth, vendors must manage their operation. This stage is an overall step, observed throughout the entire process, to ensure the smooth completion of the crime. Vendors are recommended to keep to a particular vending time-limit; plan how to deal with law enforcement; work with co-conspirators in certain cases; manage their base of operations; and avoid incriminating conduct such as committing other crimes or making obvious displays of wealth.

The six stages of this crime script were validated against the vendor arrest cases using a tablet version of the crime script (Table 1).

Studying the table, we can clearly see that most of the methods from the crime script were frequently mentioned in the cases. Of the different stages presented here, it appears that Gathering Material Resources and Setting-up Software Technologies proved the most relevant. Most of the arrest cases began by describing the context of the darknet and cryptomarkets, in which many of these components, including cryptomarkets, drugs, the internet, and cryptocurrencies were almost always mentioned, as integral to the crime. The latter stages, such as shipping and money laundering, were generally only mentioned when these methods were relevant to the given case,

Table 1 Table version of the crime script including the stages and scenes

Stages	1. Gathering Material Resources 100%	2. Setting-up Software Technologies 100%	3. Conducting Sales 62%	4. Shipping Products 80%	5. Laundering Proceeds 72%	6. Managing Operations 100%
Scenes	Using a laptop 58%	Using an anonymous internet browser 80%	Running a vendor account – technical 42%	Packing – inside the parcel 56%	Tumbling cryptocurrency 30%	Keeping to the vending time-limit 30%
	Using a printer 36%	Using encrypted technologies 14%	Running a vendor account – commercial 52%	Packing – outside the parcel 70%	Converting cryptocurrency 68%	Dealing with law enforcement 100%
	Accessing Wi-Fi 92%	Choosing a cryptomarket 92%		Dropping off parcels 64%		Working with co-conspirators 40%
	Getting drugs 100%	Using cryptocurrency 86%				Managing base of operations 74%
		Using encrypted communication 42%				Avoiding incriminating conduct 34%

namely when their use/non-use could be used to build the case against the vendor. This may point to the distinction between digital and physical aspects of the crime; the physical aspects being more frequently mentioned in relation to specific arrests, as it is through them that vendors are most vulnerable to error and identification. Nevertheless, from the broad reference of the stages across all cases, it is clear that vendors followed this crime script.

Interestingly, while all vendors engage in the six stages of this script in order to sell drugs on the darknet, the manner in which they complete these stages may vary substantially from vendor to vendor. While certain pathways appeared to be widely universal, such as the use of TOR for the completion of the Using an Anonymous Internet Browser scene, many were subject to variation, such as the Converting Cryptocurrency stage, which could be completed through a number of online (e.g. applications like Bitquick) and offline (e.g. Bitcoin ATMs) means listed in the guides, and in the cases. Differences in the nature of operations were also apparent; the majority of vendors in the case sample were solo operators (60%), while the remainder worked in teams (40%), two different criminal structures, which presented two differing approaches as the Management of Operations stage, one involving co-conspirators, the other not, one implying a significant, and potentially more complex base of operations, the other not.

Across all scenes, and all potential pathways, the wide variety of props required by vendors for the completion of the script was apparent. The necessary physical resources including items such as a laptop or computer, a printer, an internet source, a base of operations, packages, baggies, mylar, decoys (such as teddy bears or sweets), disinfectant, latex gloves, face masks, stamps, tracking labels etc.; the necessary digital resources including TOR, Tails, cryptomarkets, cryptocurrencies (generally Bitcoin), communication software (such as PGP, Jabber, or Telegram), tumblers, convertors, postal packing websites, etc. The guides and the cases both revealed the importance of these props, and how vendors, in order to be successful, must employ them effectively.

Discussion

Through examining the cryptomarket drug vending process as a whole, we gain new insights into the rationality of drug vendors. Whether in a closed or open market, traditional market dealing is generally an uncomplicated crime; the dealer purchases the drugs from a wholesale source, divides them into smaller quantities, and sells them to customers. Crime scripts of traditional market dealing indicate that the act takes place within a single point in time and space, involves no specific materials/devices/technology other than drugs and money, and involves no activities other than those consolidated to that moment: making contact, allowing for drug inspection, and exchanging drugs for cash (Jacques & Bernasco, 2013; Sytsma & Piza, 2018). Of course, there may be other relevant drug dealing aspects not accounted for therein: purchasing drugs in bulk, weighing and bagging drugs for resale, taking steps to avoid law enforcement, moderating/responding to violence and/or theft, and (potentially) liaising with co-conspirators. Other variations may depend on the form of market (open vs. closed) and the cultural/geographical/social context in which the given dealer operates. Nevertheless, even with these considerations, it is clear that darknet drug vending is significantly more complex. Vendors engage in a crime that takes place across time and space, and that involves a host of different materials/devices/technology in order to be completed. Almost all of the methods, with the exception of bagging drugs and avoiding violence, employed by traditional market dealers percolate around the drug transaction itself. This stands in sharp contrast to darknet drug vendors, who not only employ a variety of hardware and software technologies to commit their crimes, but may produce their own drugs, advertise and market not merely their products, but their own personal brand, engage in high-quality, professional customer service, package and ship their products, launder their money, and manage their entire operation, which may involve multiple co-conspirators employed in different specialised tasks.

Relatedly, the skillset required for darknet drug vending is much broader. As opposed to a situation where a traditional market dealer's success may be dependent on their friendliness, the perceived consistency of their drug supply, and techniques for evading law enforcement, darknet drug vendors require a variety of different skills, which must be employed in different ways, and in different offline and online spaces. They must have the computer skills to use anonymising technologies, the business skills to sell their products, the packing skills to send drugs by post, the money laundering skills to convert their earnings, and the management skills to run their operation smoothly. Thus we can observe somewhat of an emancipation from traditional market dealing, in that the cryptomarket iteration involves the use of more varied methods. For traditional market drug dealers, transactions tend to happen within a short space of time, within a limited geographical range (Jacques & Bernasco, 2013; Sytsma & Piza, 2018). Darknet drug vending, in contrast, requires much more time and effort: while a buyer might order and pay for drugs quickly, the packing and shipping of drugs, the release of the funds from escrow to the vendor, and the laundering of the proceeds, might take several days, even weeks. While multiple orders might be taken, their payments released, and their proceeds laundered simultaneously, each will still need to be packaged individually, and any problems with an order handled specifically, and in a professional manner. The contrast in set-up time between the two forms of dealing is even more pronounced. Once traditional market drug dealers gain access to supply, they may start selling drugs in public to strangers, or privately to friends quite immediately. Though it varies from dealer to dealer, and context to context, the potential investment of time required to start dealing is minimal. Darknet drug vendors, however, must purchase a variety of different materials to commit the crime, and set-up a variety of different software technologies which, when it comes to purchasing the materials, and installing and learning to use the software, could plausibly take several weeks, depending on the given vendor and their pre-existing material stores or computer knowledge. This point should stand regardless of how successful a given vendor is, as though there may be a significant degree of variability in the quality, efficiency, and fastidiousness in which the methods used to sell drugs on the darknet are applied by vendors, the steps which frame these methods must be followed to commit the crime. Even by virtue of vendors having to organise hardware, use software, deal with customers, ship drugs, launder money, and manage their operations, regardless of how well they complete these steps, by virtue of these steps alone, this crime can be marked as clearly distinct from its traditional iteration.

Darknet drug vendors also manage costs and benefits differently. Traditional market dealers engage in methods, such as stashing and transactional mediation, to avoid arrest (Jacobs, 1996; Fader, 2016; Vannostrand & Tewksbury, 1999). While the digital aspect of the crime provides vendors with the significant benefit of anonymity and distance from law enforcement, reducing or even eliminating the need for traditional market methods, it also provides an additional cost. If vendors make an error during the cyber stages of the crime, this error may be inscribed permanently onto their personal hardware, the online records of legitimate companies who services were used in the process, or the potentially take-down/hack accessible records of the cryptomarket. In the arrest cases, data from these different sources were used as contributory evidence in the case against the vendors; something which, given the purely physical nature of traditional drug dealing, would be unlikely in standard drug dealing cases, with the exception of mobile phone data. Cryptomarket vendors also have much greater capacities for success. While the average earnings from both lower-level traditional market dealing and darknet drug vending have been found to be generally comparable (Demant et al., 2018) no literature on traditional market dealing has shown anything near the *potential* capacity for top-rated vendors to make earnings which, in the traditional market, would be purely the reserve of upper-level, and/or potentially mid-level distributors. It is these high earning vendors which seem to be more likely to be the target of law enforcement intervention, and thus it may be that darknet drug vendors of different earning capacities have to deal with costs and benefits in different ways. Darknet drug vendors also have far more pathways to choose from when committing their crime. While traditional market dealers may operate in public or private spaces, and may signal, attract, and exchange drugs with buyers in different ways, the number of tasks involved limits the means by which the crime can be committed (May & Hough, 2004; Jacques & Bernasco, 2013; Sytsma & Piza, 2018). In contrast, each stage of the cryptomarket crime script presents a variety of pathways to the vendor: which encrypting technologies to use, which market to access, how to cash-out etc. The sheer extent of choice mandates a closer consideration of costs and benefits than that of actors who are closely limited by the opportunities their limited context provides.

Costs and benefits may be managed differently depending on the country in which the vendor operates. While the stages of the script in different countries should remain the same, as each is necessary for the full completion of the crime, the means by which these stages are executed could vary significantly. One point of variation is the availability of methods. The accessibility of high-speed internet, postal service standards, and local money laundering services may all be country dependant, closing off vendors from certain pathways, and encouraging the use of other ones. For example, while there are many pathways open to vendors to launder their illicit proceeds outlined in the script, this list might be limited by a vendor's location; if they live in a country where there are no bitcoin ATMs, crypto debit cards are not issued/accepted, and crypto-for-cash trades are uncommon, their money laundering activities will be limited to online services. A second point of variation relates of the differences between the legal, political, and social structures of countries. The use of anonymising technologies, drug sourcing materials/knowledge, and shipping practises may be subject to different legal restrictions and law enforcement practises to which vendors must adopt their methods accordingly. For example, in certain countries, postal mail of a certain size and weight may not be openable without a warrant, limiting the likelihood of interception in those countries, and thus reducing the need for fastidious shipping methods for vendors shipping to them. It is thus that the script has a certain level of flexibility, with a number of different pathways being employed, and executed with differing levels of caution and expertise, depending on the context.

It should be noted however that darknet drug vendors have a clear environmental advantage over traditional market dealers. While traditional market dealers must rely largely on their wits, the drugs which they have access to, and their drug dealing context to buffer them from detection by law enforcement, darknet drug vendors take advantage of a variety of technological applications and services to execute their crimes. Both the anonymising technologies they use: TOR, Tails, Bitcoin, Ethereum, Telegram, Bitquick etc. and their means of shipping: national postal services and private couriers, exist, and are maintained, by independent external sources. By relying on these services, vendors can execute their crimes effectively, reducing the cost of detection by improving their anonymity, and increasing the benefit of profits by making sales transactions more convenient for buyers. As such, the study of cryptomarket drug vending methods hints at the parallel between vendor behaviour and the markets on which they operate; cryptomarkets all at once making darknet drug vending a more complicated, yet more effective, crime.

Limitations

Firstly, it should be noted that, in many ways, the work at hand is a preliminary study. While there has been a lot of research conducted on the sales of drugs online; particularly in relation to the functioning of the markets as a whole, and the interaction between vendors and their customers, this is the first work which encompasses the entire process from beginning to end. However, the broad scope of this approach meant that the technical aspects of how these different methods are employed in practise were not provided. Even with the previous work in this area, it is likely that a more complete examination of these methods will be needed on a single method level, especially as their use evolves over time.

Secondly, there was an issue with the parameters of the data–specifically its anglophonic focus. Though the guides were written by vendors from many different countries, most of the focus was still on the Anglosphere. Similarly, while there were some foreign vendors in the sample, the vast majority of arrested vendors were from the United States. It could be interesting for future research to investigate the application of this crime script in reference to specific cultural contexts, in order to better account for potential differences in the physical world aspects of the crime between vendors, such as whether practises for posting drugs differ in countries where there is limited law enforcement attention given to cryptomarket drug vending.

Thirdly, this research deals with particularly sensitive, and ultimately criminal information. It might even be suggested that this crime script could help a criminal to sell drugs on the darknet. While this is certainly a valid concern, it should be noted that all the data used in this research was drawn from the public domain: the how-to guides and arrest cases being sourced openly though the internet. This research merely took data ostensibly accessible to vendors and inserted it into a criminological context (Christin & Martin, 2016). Of course, the analysis and processing of data does alter the nature of this information, but any harm in presenting it should be outweighed by the benefit provided to criminologists seeking to better understand this crime (van de Laarschot & van Wegberg, 2021).

Fourth, the use of case studies comes with certain limitations. All the vendors sampled failed to maintain their anonymity, and thus, in some sense, were not successful criminals. However, this is at least partially balanced by the focus of law enforcement on the arrest of financially successful vendors; while all the vendors in the sample were arrested, they were typically sought for arrest precisely because they were successful. Of the cases in which the estimated earnings of the vendors were stated, most ran into the high hundred thousands, with several vendors reported to have earned millions. Furthermore, because the cases are presented from the perspective of law enforcement, they may be limited by their provision of information pertaining to the specific case, and to the interest of the authorities, as opposed to the actual vendor's conduct. Yet what was apparent from the study of the cases was that the information provided was extensive: typically giving a full background on the mandatory, technologically driven aspects of the crime, as well as most aspects of the routine process of the criminal in question, their communication with buyers, postal shipping methods, and money laundering techniques being frequently referenced as evidence. It should also be noted that, despite this limitation, case files provide a rich and varied source of qualitative data, one which can be used to enhance findings in the literature derived from quantitative sources.

Conclusion

Before this research was undertaken, we knew quite a lot about the crime of cryptomarket drug dealing (Barratt & Aldridge, 2016). There had been a lot of significant works published on the issue, which had developed our understanding of specific components of the crime, especially in relation to buyer-vendor interactions, market statistics, and user dynamics (e.g. Aldridge & Décary-Hétu, 2014; Morselli et al., 2017; Tzanetakis, 2018; Zaunseder & Bancroft, 2020). However, it remained unclear how all the different aspects of this crime came together in a single, comprehensive process. Moreover, several key methods used by cryptomarket drug vendors, such as money laundering, and the management of operations, had not yet been explored. Though vendors were frequently assumed to be rational actors, few studies had examined the theory in detail, and considered the extent to which vendors may be so conceptualised.

We now know that there is a clearly delineated process which all cryptomarket vendors must follow in order to complete this crime. The processes by which vendors launder their illicit proceeds and manage their operations have been illuminated, and we have gained a better understanding of the different pathways open to vendors for the completion of these aspects of the crime. Finally, in fresh consideration of the entirety of the criminal process of cryptomarket drug vending, we observe that cryptomarket drug vendors contrast significantly with their traditional market counterparts, and for all of the time, effort, and skills involved in the commission of their crime, may be conceptualised as being predominately rational.

Author contribution The solo author completed all sections of the research and the manuscript alone.

Funding No external funding was provided for this research.

Data Availability The first dataset (how-to guides) generated during and/or analysed during the current study are not publiclyavailable as they were accessed predominantly through darknet forums, but they are available from the corresponding author on reasonable request.
The second dataset (case files) generated during and/or analysed during the current study are publicly available through the United States repository of criminal cases accessible through https://www.pacermonitor.com. A full list of the cases used in this study can be made available by the corresponding author on reasonable request.

Declarations

Ethical approval Granted internally by the research centre Transcrime attached to UCSC.

Informed consent Not required as no participants took part in this research.

Statement Regarding Research Involving Human Participants and/or Animals Not applicable.

Conflict of interest There are no known competing interests.

References

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *The Journal of Criminal Law and Criminology*, *81*(3), 653–676. https://doi.org/10.2307/1143850

Aldridge, J. (2019). Does online anonymity boost illegal market trading? *Media Culture and Society*, *41*, 578–583. https://doi.org/10.1177/0163443719842075

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, *41*, 101–109. https://doi.org/10.1016/j.drugpo.2016.10.010

Aldridge, J., & Décary-Hétu, D. (2014). Not an “eBay for drugs”: The cryptomarket “silk road” as a paradigm shifting criminal innovation. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2436643

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

Bakken, S. A., Moeller, K., & Sandberg, S. (2018). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology*, *15*(4), 442–460. https://doi.org/10.1177/1477370817749177

Bancroft, A. (2017). Responsible use to responsible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket. *Health Risk and Society*, *19*(7–8), 336–350. https://doi.org/10.1080/13698575.2017.1415304

Bancroft, A., & Reid, P.S. (2016). Concepts of illicit drug quality among darknet market users: Purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy*, *35*, 42–49. https://doi.org/10.1016/j.drugpo.2015.11.008

Bancroft, A., Squirrell, T., Zaunseder, A., & Rafanell, I. (2019). *Producing Trust among Illicit Actors: A Techno-Social Approach to an online Illicit Market* (pp. 456–472). 25 – 3: Sociological Research Online. https://doi.org/10.1177/1360780419881158

Barratt, M. J., & Aldridge, J. (2016). Everything You Always wanted to know about drug Cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, *35*, 1–6. https://doi.org/10.1016/j.drugpo.2016.07.005

Bhaskar, V., Linacre, R., & Machin, S. (2019). The economic functioning of online drugs markets. *Journal of Economic Behaviour and Organization*, *159*, 426–441. https://ideas.repec.org/a/eee/jeborg/v159y2019icp426-441.html. Retrieved: 24/11/21.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, *2*, 6. https://doi.org/10.1186/2193-7680-2-6

Broséus, J., Rhumorbarbea, D., Morelatob, M., Staehlia, L., & Rossy, Q. (2017). A geographical analysis of trafficking on a popular darknet market. *Forensic Science International*, *277*, 88102. https://doi.org/10.1016/j.forsciint.2017.05.021

Caudevilla, F., Ventura, M., Fornis, Barratt, I., Vidal, M. J., Iladanosa, C., Quintana, C. G., Munoz, P., & Calzada, A., N (2016). Results of an international drug testing service for cryptomarket users. *International Journal of Drug Policy*, *35*, 38–41. https://doi.org/10.1016/j.drugpo.2016.04.017

Childs, A., Coomber, R., Bull, M., & Barratt, M.J. (2020). Evolving and diversifying selling practices on drug cryptomarkets: An exploration of off-platform "direct dealing". *Journal of Drug Issues*, *50*(2), 173–190. https://doi.org/10.1177/0091450920934186

Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of Drug Manufacturing in Clandestine Laboratories: Implications for Prevention. *British Journal of Criminology*, *51*, 355–374. https://doi.org/10.1093/bjc/azr005

Christin, N. (2013). Traveling the silk road: A measurement analysis of a large anonymous online marketplace. In: Proceedings of the 22nd International Conference on World Wide Web - WWW '13, Press, Rio de Janeiro, Brazil, 213–224. https://doi.org/10.1145/2488388.2488408

Christin, N. (2017). An EU-focused analysis of drug supply on the AlphaBay marketplace. Retrieved: 24/11/21 https://www.emcdda.europa.eu/system/files/attachments/6622/AlphaBay-final-paper.pdf

Christin, N., & Thomas, J. (2019). Analysis of the supply of drugs and new psychoactive substances by Europe-based vendors via darknet markets in 2017–18. *EMCDDA*. Retrieved April 11, 2023, from https://www.emcdda.europa.eu/system/files/media/attachments/documents/12104/EDMR2019_BackgroundReport_Darknet.pdf

Coomber, R. (2006). *Pusher myths: Re-situating the drug dealer*. Free Association.

Coomber, R. (2015). A tale of two cities understanding differences in levels of heroin/crack market-related violence—A two city comparison. *Criminal Justice Review*, *40*, 7–31. https://doi.org/10.1177/0734016814565817

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R. V. Clarke (Ed.), *Crime prevention studies* (pp. 151–196). Willow Tree Press.

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending - criminal law and criminal justice book reviews*. Springer-Verlag.

Craciunescu, N. E. (2021). Drugs, brands and consumer culture: The sign-value of the products sold on the darknet marketplaces. *Drugs and Alcohol*, *21*(2), 124–134. https://doi.org/10.1108/DAT-12-2019-0048

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

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

Décary-Hétu, D., & Quessy-Doré, O. (2017). Are repeat buyers in Cryptomarkets Loyal customers? Repeat business between dyads of Cryptomarket vendors and users. *American Behavioral Scientist*, *61*, 1341–1357. https://doi.org/10.1177/0002764217734265

Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology*, *18*(4), 504–525. https://doi.org/10.1177/1477370819850943

Demant, J., Munksgaard, R., & Houborg, E. (2018). Personal use, social supply or redistribution? cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime*, *21*, 42–61 https://doi.org/10.1007/s12117-016-9281-4

Fader, J.J. (2016). Selling smarter, not harder: Life course effects on drug sellers' risk perceptions and management. *International Journal of Drug Policy*, *36*, 120–129.https://doi.org/10.1016/j.drugpo.2016.04.011

Hämäläinen, L. (2015). Usernames of illegal drug vendors on a darknet cryptomarket. *Onoma*, *50*, 45–71. https://doi.org/10.34158/ONOMA.50/2015/2

Holt, T. J., & Lee, J. R. (2020). A crime script analysis of Counterfeit identity document procurement online. *Deviant Behavior*, 1–18. https://doi.org/10.1080/01639625.2020.1825915

Hutchings, A., & Holt, J., T (2014). A crime script analysis of the online Stolen Data Market. *British Journal of Criminology*, *55*, 596–614. https://doi.org/10.1093/bjc/azu106

Jacinto, C., Duterte, M., Sales, P., & Murphy, S. (2008). "I'm not a real dealer": The identity process of ecstasy sellers. *Journal of Drug Issues*, *38*, 419–444. https://doi.org/10.1177/002204260803800203

Jacobs, B.A. (1996). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly*, *13*, 359–381. https://doi.org/10.1080/07418829600093011

Jacobs, B.A & Wright, R. (2010). Bounded rationality, retaliation, and the spread of urban violence. *Journal of Interpersonal Violence*, *25*(10), 1739–1766. https://doi.org/10.1177/0886260509354502

Jacques, S., & Bernasco., W. (2013). Drug dealing: Amsterdam's Red Light District. In R. Wortley & B. Leclerc (Eds.), *Cognition and crime: Offender decision making and script analyses* (pp. 120–139). Routledge.

Jacques, S., & Reynald, D. M. (2012). The offenders' perspective on prevention: Guarding against victimization and law enforcement. *Journal of Research in Crime and Delinquency*, *49*(2), 269–294. https://doi.org/10.1177/0022427811408433

Jardine, E. (2021). Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention. *American Journal of Criminal Justice*, *46*, 980–1005. https://doi.org/10.1007/s12103-021-09656-3

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, *73*, 281–287. https://doi.org/10.1016/j.drugpo.2019.04.011

Katz, J. (1988). *Seductions of crime: Moral and sensual attractions of doing evil*. Basic Books.

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

Lavorgna, A. (2014). Internet-mediated drug trafficking: Towards a better understanding of new criminal dynamics. *Trends in Organised Crime*, *17*, 250–270. https://doi.org/10.1007/s12117-014-9226-8

Martin, J. (2014a). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Palgrave Macmillan.https://doi.org/10.1057/9781137399052

Martin, J. (2014b). Lost on the silk road: Online drug distribution and the 'cryptomarket'. *Criminology and Criminal Justice*, *14*, 351–367. https://doi.org/10.1177/1748895813505234

Martin, J., & Christin, N. (2016). Ethics in cryptomarket research. *International Journal of Drug Policy*, *35*, 84–91. https://doi.org/10.1016/j.drugpo.2016.05.006

Martin, J., Munksgaard, R., Coomber, R., Demant, J., & Barratt, M. J. (2020). Selling drugs on Darknet Cryptomarkets: Differentiated pathways, risks and rewards. *The British Journal of Criminology 60 – 3*, 559–578. https://doi.org/10.1093/bjc/azz075

Masson, K., & Bancroft, A. (2018). Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy*, *58*, 78–84. https://doi.org/10.1016/j.drugpo.2018.05.008

Matza, D. (1964). *Delinquency and drift*. John Wiley.

May, T., & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research & Theory*, *12*, 549–563. https://doi.org/10.1080/16066350412331323119

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. *International Criminal Justice Review*, *27*, 237–254. https://doi.org/10.1177/1057567717709498

Nurmi, J., Kaskela, T., Perälä, J., & Oksanen, A. (2017). Seller's reputation and capacity on the illicit drug markets: 11-month study on the finnish version of the Silk Road. *Drug and Alcohol Dependence*, *178*, 201–207. https://doi.org/10.1016/j.drugalcdep.2017.05.018

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

Parker, H. (2000). How young Britons obtain their drugs: Drugs transactions at the point of consumption. Crime Prevention Studies, 11. In M. Natarjan, & M. Hough (Eds.), *Illegal drug markets: From research to Prevention Policy*. Willow Tree Press.

Potter, G. (2009). Exploring retail-level drug distribution: Social supply, "real" dealers and the user/dealer interface. In Z. Demetrovics, J. Fountain, & L. Kraus (Eds.), Old and new policies, theories, research methods and drug users across Europe, ed. Demetrovics, Z., Fountain, J., Kraus., L., PABST, Germany.

Reuter, P. (1983). *Disorganised crime*. The MIT Press.

Reuter, P., & Trautmann, F. (Eds.). (Eds., 2009). Report on Global Illicit Drug Markets 1998–2007. Brussels: European Commission. Retrieved: 24/11/21 https://www.drugsandalcohol.ie/12757/

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q., & Esseiva, P. (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical, and chemical data. *Forensic Science International*, *267*, 173–182. https://doi.org/10.1016/j.forsciint.2016.08.032

Salinas, M. (2017). The unusual suspects: An educated, legitimately employed drug dealing network. *International Criminal Justice Review*, *28*(3), 226–242. https://doi.org/10.1177/1057567717745583

Savona, E. U., Giommoni, L., & Mancuso, M. (2013). Human trafficking for sexual Exploitation in Italy. In B. Leclerc, & Wortley (Eds.), *Cognition and crime*. R. Routledge.

Sytsma, V.A., & Piza, E.L. (2018) Script analysis of open-air drug selling: A systematic social observation of CCTV footage. *Journal of Research in Crime and Delinquency*, *55*(1), 78–102. https://doi.org/10.1177/0022427817709502

Thompson, L., & Chainey, S. (2011). Profiling illegal Waste activity: Using crime scripts as a Data Collection and Analytical Strategy. *European Journal on Criminal Policy and Research*, *17*, 179. https://doi.org/10.1007/s10610-011-9146-y

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy*, *56*, 17–186. https://doi.org/10.1016/j.drugpo.2018.01.022

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

van de Laarschot, J., & van Wegberg, R. (2021). Risky Business? Investigating the Security Practises of Vendors on an Online Anonymous Market using Ground-Truth Data, 30th USENIX Security Symposium. Retrieved: 25/11/21 https://www.usenix.org/system/files/Sect. 21-van-de-laarschot.pdf

van Hardeveld, G. J., Webber, C., & O'Hara, K. (2016). Discovering credit card fraud methods in online tutorials. *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention*. https://doi.org/10.1145/2915368.2915369

van Hout, M. C., & Bingham, T. (2013). 'Surfing the silk road': A study of users' experiences. *International Journal of Drug Policy*, *24*, 524–529. https://doi.org/10.1016/j.drugpo.2013.08.011

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*, 183–189. https://doi.org/10.1016/j.drugpo.2013.10.009

Vannostrand, L.-M., & Tewksbury, R. (1999). The motives and mechanics of operating an illegal drug enterprise. *Deviant Behavior*, *20*, 57–83. https://doi.org/10.1080/016396299266597

Zaunseder, A., & Bancroft, A. (2020). Pricing of illicit drugs on darknet markets: A conceptual exploration. *Drugs and Alcohol Today 21 – 2*, 135–145. https://doi.org/10.1108/DAT-12-2019