American Journal of Criminal Justice
https://doi.org/10.1007/s12103-021-09656-3

Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention

Eric Jardine[1]

Received: 14 January 2021 / Accepted: 24 June 2021

Abstract

Darknet drug market participants must complete a distinct cybercrime script if they are to successfully procure illicit substances online. This paper details the four generic stages (i.e. Informational Accumulation; Account Formation; Market Exchange; Delivery/Receipt) of a novel cybercrime script for Darknet drug markets. It also presents vignette examples of known law enforcement interventions that have effectively targeted each stage of the script to reduce usage of these marketplaces. While law enforcement interventions to close specific Darknet markets tend to have only short-lived effects on levels of illicit activity, the lens of the cryptomarket crime script highlights numerous additional steps beyond closure that law enforcement can effectively undertake to reduce use of these platforms.

Keywords Cryptomarkets · Policing · Darknet · Dark Web · Cybercrime · Crime script · Silk road

In February 2011, a new e-commerce site emerged on an anonymized portion of the Internet known as the Tor Darknet. Silk Road, as this budding cryptomarket was called, combined the trust features of traditional e-commerce sites such as eBay or Amazon with a sophisticated escrow function and a transactional payment system based around a pseudonymous cryptocurrency known as Bitcoin (Lorenzo-Dus & Di Cristofaro, 2018; Martin, 2014b). The Silk Road market, like its successors, was primarily a market for drugs (Christin, 2013; Soska & Christin, 2015), with customers and vendors in the United States, Netherlands, Finland, the UK, Australia, Canada, and a host of other jurisdictions (Barratt et al., 2014; Van Buskirk et al., 2016).

Silk Road began as a small market with few listings, vendors, or customers. It grew rapidly, however, and splashed into the mainstream following an article in Gawker, which began by summarizing some of the harsh realities of offline drug procurement and the available possibilities on Silk Road. "Making small talk with

✉ Eric Jardine
ejardine@vt.edu

[1] Virginia Tech, Blacksburg, VA 24061, USA

Published online: 19 November 2021

your pot dealer sucks. Buying cocaine can get you shot," wrote journalist Adrian Chen. "What if you could buy and sell drugs online like books or light bulbs? Now you can: Welcome to Silk Road" (Chen, 2011).

Silk Road's new stint in the limelight caught the attention of US Senator Chuck Schumer. Days after the initial Gawker article, Senator Schumer held a Sunday press conference to pressure law enforcement to shut down the Silk Road cryptomarket. During his remarks, he highlighted how the forum "allows buyers and users to sell illegal drugs online, including heroin, cocaine, and meth … by hiding their identities through a program that makes them virtually untraceable. It's a certifiable one-stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen. It's more brazen than anything else by lightyears" (cited in York, 2011).

In October 2013, law enforcement eventually did succeed in shutting down Silk Road and arresting its main administrator, the infamous Dread Pirate Roberts. Silk Road's closure was the first of many such closures. Even though the cryptomarket ecosystem has proven to be remarkably resilient to takedowns (Décary-Hétu & Giommoni, 2017; Duxbury & Haynie, 2018; ElBahrawy et al., 2020; Van Buskirk et al., 2017), continues to expand over time (Dolliver, 2015; Paquet-Clouston et al., 2018; Soska & Christin, 2015), and exhibits high levels of adaptability in response to policing efforts (Horton-Eddison & Di Cristofaro, 2017), law enforcement has shown that it can police this online space as it does the offline world. Policing efforts, in this context, refer to interventions that either leverage aspects of the cybercrime script to identify and arrest cryptomarket participants or intervene preventively to reduce the likelihood that prospective participants can effectively complete the script.

To understand better what law enforcement does to police Darknet drug markets, this paper first presents a novel cybercrime script that details the steps through which cryptomarket users need to pass if they are to move from an initial learning phase to picking up illicit drugs at their mail boxes. Secondly, the paper details the litany of known police operations and procedures that leverage vulnerable points at each stage in the cryptomarket crime script. Overall, the analysis suggest that cryptomarket drug crimes follow a known pattern and each stage of this cycle is susceptible to effective law enforcement intervention.

The next section summarizes known activities in the Tor cryptomarket ecosystem, with a particular emphasis on site feature and how vendors and consumers use these platforms. This discussion leads to the next section, which presents a generalized novel cybercrime script for Darknet drug exchange using Tor cryptomarkets. The sections following unpack the details of each stage of the cryptomarket crime script and present known law enforcement tactics that target each step.

Darknet Cryptomarkets and Drugs

This section provides a brief summary of the Tor Darknet ecosystem, with an emphasis on three facets of the wider cryptomarket space (i.e. a market on Tor "defined as an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities" (Martin, 2014b, p. 356)). First, these marketplaces, while offering some other goods and services for sale, are heavily weighted toward drug exchange. Second, these platforms are built around e-commerce features such as customer feedback, product and vendor listing metrics, and market-based dispute resolution systems that both ameliorate potential trust deficits in the system and act as useful informational cues in customer purchasing decisions. And, finally, once a product and vendor have been selected and money has exchanged hands (potentially with recourse to a market escrow system), packages are then shipped either domestically or internationally, often via regular postal services.

Darknet cryptomarkets for drugs and other illegal content have both supply- and demand-side components, with market participants often vacillating between the two roles (Jardine, 2019b). Supply-side indicators reveal how many vendors are in operation and what those vendors tend to be selling. For instance, an early investigation into the first Silk Road marketplace tracked available products on offer as a way to determine what was for sale, concluding that the cryptomarket was "mostly a drug store, even though it also caters some other products" (Christin, 2013, p. 8). In particular, the top four product listing were for drugs, as were 90 percent of the top 10 listings and 16 of the top 20 product offerings. Across multiple cryptomarkets, cannabis, MDMA, and LSD consistently rank as the most frequently listed drugs on offer (Barratt et al., 2016a; Christin, 2013; Dolliver, 2015; Rhumorbarbe et al., 2016; Soska & Christin, 2015; Van Buskirk et al., 2016; Van Buskirk et al., 2013; Van Buskirk et al., 2014).

Vendors offer individual drug listings. Repeated iterations of *Drugs and the Internet* have tracked the increase in sellers on Silk Road 1.0 from 282 during the first observation period to 579 in October 2013, the month it was taken offline by the FBI (Van Buskirk et al., 2013; Van Buskirk et al., 2014). The Agora cryptomarket, which ran from 2013 until 2015, had 867 vendors peddling their wares in its last year of operation (Van Buskirk et al., 2016). Evolution, another cryptomarket in operation until its administrators absconded with user funds in 2015, had around 2,700 vendors from 70 countries (Rhumorbarbe et al., 2016). In 2016, AlphaBay had some 1,582 vendors, with 25,395 cumulative drug listings and evidence of 153,331 sales as measured by customer feedback entries (Paquet-Clouston et al., 2018). More broadly, systematic investigation of 35 distinct Darknet marketplaces records a generally increasing number of cryptomarket vendors over time (Soska & Christin, 2015). These increasing numbers suggest a gradual, but consistent, adoption of cryptomarkets as a source of drug procurement and sale, as well as the potential migration of offline drug-related illicit activities onto the Darknet.

In contrast to such supply-side indicators, demand-side measures can reveal how Darknet cryptomarkets are being used by both vendors and consumers (Jardine, 2019b). On cryptomarkets, these indicators include seller feedback ratings, comments, and vendor profile satisfaction scores. Collectively, these trust-features used to overcome the perils of e-commerce can also provide a sense of cryptomarket sales volume, how much money vendors are making, the proportion of sales that are nominally retail or wholesale, and how satisfied customers are with Darknet cryptomarket products. Leveraging customer feedback information, for example, can allow for a clear estimation of sales volume on both a single market (Aldridge & Décary-Hétu, 2014, 2016; Christin, 2013) and multiple marketplaces (Soska & Christin, 2015). In early 2013, Silk Road 1.0 was likely grossing sales in the range of $300,000 per day, which annualizes to about $110 million per year (Soska & Christin, 2015). Sales revenue on cryptomarkets have increased significantly since this time.

Broadly speaking, total cryptomarket sales revenue includes two separate modalities of drug exchange. Some portion of total sales revenue comes from individuals engaged in retail purchases for largely personal consumption. Another portion of sales volume is composed of wholesale transactions intended for social supply or local redistribution. The relative procurement picture along these lines is mixed. Silk Road 2.0 was likely best characterized as predominantly a retail site. No vendor listed more than 17 active drug categories and few advertised much in the way of cross-border delivery, which could be feasibly accomplished through traditional mail services (Dolliver, 2015). Sales of cocaine and heroin on the Agora marketplace also fit a pattern of retail sales (Dolliver et al., 2018). In contrast, looking at sale numbers from the first iteration of Silk Road depicts a somewhat different picture. Here, just short of half of all drug listings were for retail-sized portions of illegal drugs valued at less than $100. However, sales of this kind accounted for only around 17% of the cryptomarkets total volume. In contrast, large wholesale transactions (above $1,000) accounted for 26% of total market sales. In short, current cryptomarkets are likely predominately oriented toward retail sales, but there is mounting evidence to suggest some wholesale market throughput. These findings can mean either that individuals with access to cryptomarkets start to act as local drug distributors, a behavior which some individual customers from Silk Road 1.0 reported engaging in (Barratt et al., 2016b), or potentially that larger drug distribution networks are sourcing supply or selling via Darknet cryptomarkets.

While Darknet cryptomarkets, in line with offline illicit markets (Reuter, 1986), tend to have high levels of competitiveness (Paquet-Clouston et al., 2018), aggregate cryptomarket sales (be they retail or wholesale) are not evenly distributed across vendors. Similar to processes on clear web platforms (Barabási, 2014; Jardine, 2017), mechanisms of preferential attachment tend to emerge on Darknet cryptomarkets (Duxbury & Haynie, 2018). Customers in their search for trustworthy products and vendors tend to gravitate toward listings that are widely used by others, generating huge clusters of activity. As one vendor on Silk Road 1.0 put it, "keeping prices low as possible, shipping promptly and using good stealth techniques gets you good reviews on the forum, so more customers come to you" (Van Hout & Bingham, 2014).

These processes of preferential attachment create clusters of customers on particular sites and draw users toward particular vendors. On Silk Road 1.0, no vendor listed more than 1.5% of the available products, suggesting a fairly flat distribution of goods on offer (Christin, 2013). However, the top 100 vendors had 60 percent of the total sales volume, as measured by customer feedback entries. The top 200 vendors accounted for roughly 80% of all sales (Christin, 2013). These numbers from a single market are demonstrative of a highly unequal distribution of customers across content. They are also in line with the results of more far-reaching investigation into multiple cryptomarkets, where the top 1% of vendors across 35 Darknet platforms accounted for a majority (51.5 %) of sales (Soska & Christin, 2015).

These clusters of users emerge in part due to the e-commerce trappings of these sites, for example, customer feedback mechanisms, site-based escrow payment systems, and defined dispute resolution tools, which tend to result in fairly high levels of customer satisfaction. On the Finnish version of Silk Road, for example, both vendor reputation and capacity are positively associated with increased patronage by consumers (Nurmi et al., 2017). Ethnographic and single-case investigations of customer satisfaction with Silk Road 1.0 indicate that users tend to find that drug purchases on cryptomarkets are safer than the real world and provide higher quality (Barratt et al., 2014, 2016b; Hout & Bingham, 2013a, 2013b). Likewise, vendors on Silk Road 1.0 tended to be happy with the site's functionality and the protections that it provided, particularly compared to the prospect of street vending (Van Hout & Bingham, 2014). The satisfaction of both consumers and vendors is also largely reinforced by a widespread engagement with messaging forums and discussion boards, which propagate a techno-libertarian world view (Maddox et al., 2016) and share information on how to use cryptomarkets effectively (Aldridge & Askew, 2017; Smith & Frank, 2020)

Happy vendors and customers help to create a sustained market ecosystem, even as particular marketplaces are subject to law enforcement takedowns (Décary-Hétu & Giommoni, 2017; Soska & Christin, 2015; Van Buskirk et al., 2017). The persistence of cryptomarkets potentially increases the range and volume of drugs available for consumers (Aldridge et al., 2018). Given the inherent cross-border nature of both the Internet and the Tor overlay network, such forums also promise to potentially influence the geographical spread of illicit drugs as packages are shipped via state postal systems both domestically and internationally (Matthews et al., 2020). Consistent evidence suggests that countries have variable quantities and types of listed drugs on Darknet cryptomarkets (Dolliver, 2015; Van Buskirk et al., 2016), but a nested set of factors, ranging from the product and the vendor's profile to the vendor's likely location, also affect the likelihood that goods will be shipped internationally. For example, lighter products are more likely to be shipped across international borders. Vendors with higher ratings are less likely to engage in international distribution and merchants with more product listings are more likely to cross boundaries. Lastly, if the vendor's country has high policing capacity and a large domestic pool of consumers, then vendors are much less likely to engage in international diffusion of illegal drugs (Décary-Hétu et al., 2016). Ironically, perhaps, given the techno-libertarianism that heavily surrounded the early cryptomarket ecosystem (Munksgaard & Demant, 2016), most Darknet drug market sales get distributed by state-based postal systems such as USPS.

This summary of features, trends, and activity on Darknet drug markets suggests routine patterns of activity that can be effectively generalized into a cybercrime script for cryptomarket drug activity.

A Novel Cryptomarket Crime Script

The summary of site functions and the uses of Darknet markets detailed above can be generalized into a multistage novel cryptomarket cybercrime script through which buyers and sellers need to navigate. Crime scripts are schemata that organize the meaningful steps through which a potentially motivated offender needs to move in order to successfully complete an illicit/illegal activity (Cornish, 1994). While scripts are generally non-deterministic (therefore allowing for criminogenic innovation), they also aim at being fairly generalizable and exhaustive across actor type and context. Crime scripts are useful in that they allow for highly targeted law enforcement interventions, and are an increasingly common way of understanding the commission of crime across a number of crime types (Chiu et al., 2011; Cornish, 1994; Dehghanniri & Borrion, 2021; Hutchings & Holt, 2014).

At the most aggregated view and assuming the operation of a market run by administrators (which might be its own partially overlapping script), the cryptomarket crime script contains four stages: 1) informational accumulation; 2) account formation; 3) market use; and 4) delivery/receipt. This script is summarized in Fig. 1.

The generic stages start with a process of informational accumulation, where budding users become familiar with the Darknet, Tor, cryptocurrencies and particular cryptomarkets. Prospective users can then establish accounts, including both cryptocurrency wallets and customer or vendor accounts on individual or multiple cryptomarkets of choice. The market use phase includes divergent script steps for vendors or buyers. For buyers, users engage in a product search to locate the item, vendor and geographical “ship from/ship to” details that fit their needs. Vendors post profile details and product descriptions and manage their online identities in an effort to attract customers. Once a customer has selected a product listing, they would then exchange mailing details and funds with the selected vendor, potentially moderated by the cryptomarket via an escrow service. The vendor would then package the purchased product and ship it to the buyer, often via regular postal services. As a final action in the cryptomarket crime script, a buyer would then venture to the provided mailing address to take receipt of the product before finalizing the sale via the cryptomarket.

The generic four-stage cryptomarket crime script details the process through which vendors and buyers need to pass if they are to use a preexisting Darknet market. This generic four-stage script includes a number of subsidiary steps per stage. The next four sections detail the steps undertaken by buyers and sellers at each stage, and known law enforcement interventions targeting each phase of the cryptomarket script.

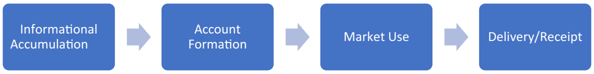


Fig. 1 A Generic Cryptomarket Crime Script

Stage 1: Informational Accumulation

Informational Accumulation: Detailed Script Steps

The first step in the cryptomarket crime script involves a process of informational accumulation, which happens through some combination of deliberate search and indirect exposure (See Figure 2 for detailed steps). Two common pathways of exposure are web search (such as via Google) and social media exposure (via Reddit or 4Chan, for example). These mediums of informational accumulation can be more or less targeted, often depending on whether the motivated offender is in the early or later stages of this step of the cryptomarket crime script.

Indirect exposure initiates the process of informational accumulation. Since active search usually requires knowledge of key terms or topics that can be entered into a search bar, indirect or unintentional exposure to the Darknet, Tor, or cryptomarkets on social media sites is likely to be a common initial catalyst of movement through the crime script for a potential motivated offender. For example, various social media platforms, such as Reddit, 4Chan, and numerous others, host active discussion threads for Darknet and cryptomarket related news. These threads could be ranked and displayed on a person's newsfeed without any active search on the part of the user, and so catalyze the initial informational accumulation process. Offline exposure can also initiate the informational accumulation stage of the cryptomarket script, through peer networks, television, news, or video games.

Once some basic knowledge of the Darknet as a conceptual ground is established, a prospective user could then begin a somewhat non-linear process of more targeted searches. A user, for example, could search for "Dark Web," "Darknet", or "Tor" on Google to begin a more deliberate process of learning about these systems, how they work, and how to access the anonymized Tor Darknet—or alternatives such as I2P or Freenet. Figure 3 plots the relative search frequency of these terms within the United States from the start of 2011, when Silk Road initiated the modern cryptomarket era, to the end of 2020. Searches for "Tor" are most common, but the term "Dark Web" has grown steadily in relative popularity over time. "Darknet" is evidently not a widely used term within the United States. A similar informational search process would unfold for cryptocurrencies, with

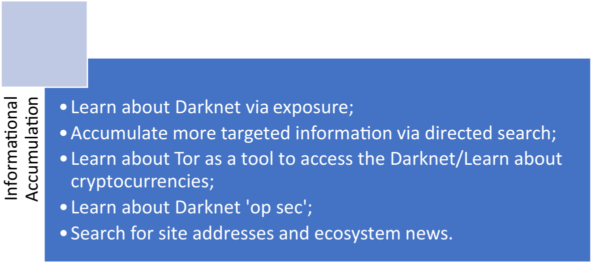
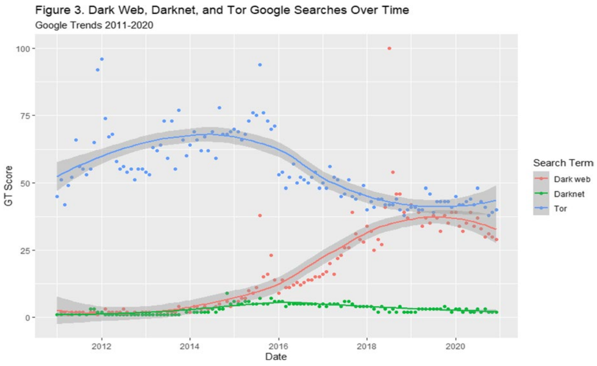

Informational Accumulation
• Learn about Darknet via exposure;
• Accumulate more targeted information via directed search;
• Learn about Tor as a tool to access the Darknet/Learn about cryptocurrencies;
• Learn about Darknet 'op sec';
• Search for site addresses and ecosystem news.

Fig. 2 Stage 1: Informational Accumulation

Fig. 3 Dark Web, Darknet, and Tor Google Searches Over Time



searches for specific coins (e.g. Bitcoin), modalities of exchange (e.g. Coinbase), and news (e.g. www.news.bitcoin.com) being potential search queries.

Once a prospective user has accumulated information about the Tor Darknet to the point where they feel comfortable attempting to access the system, their next step would be to use a regular web browser to visit the Tor Project website. From here, a person can easily download the Tor browser, which is preconfigured to leverage Tor's overlay network and to mask a user's Internet traffic by disassociating their IP address at the point at which they enter the network from the IP address seen by the administrators of the websites that they visit. Since the Tor browser can be used to access many Clear web sites, informational accumulation can continue via this channel, once a user has installed the Tor browser package. Users might also begin to employ virtual private networks (VPNs) at any stage of this step.

In a potentially concurrent process of informational accumulation, users who intend to navigate the Darknet market crime script effectively will also need to learn operational security ("op sec") techniques. Such techniques could include using VPNs and the Tor browser simultaneously, deploying encryption, and potentially running the operating system Tails, which boots from a USB, wipes session information once closed, and encrypts selected persistent files on the initiating USB drive. In summarizing the informational accumulation steps needed to securely engage with the Darknet cryptomarket ecosystem, one ethnographic study participant noted: "I did a lot of research on how encryption works, how PGP keys worked. That took me about two or three days to understand. I got set up. Got a clean laptop. Used TAILS, very secure, fresh, operating system, installed Tor" (Cited in Kowalski et al., 2019, p. 4). Often, in a grander sense, the employment (embodiment) of these techniques can induct users into a wider cryptomarket community, which places very high regard on the use and acting out of various "op sec" techniques (Bancroft & Scott Reid, 2017; Gehl, 2018).

The final step in the informational accumulation stage of the cryptomarket crime script involves locating specific Darknet .onion site addresses. Onion/Hidden Services are Darknet sites running standard web technologies (html, etc.) (Gehl, 2018) and include a number of different possible site types, ranging from Facebook's .onion version of its popular social media service to child abuse imagery forums (Jardine et al., 2020; Owen & Savage, 2015). Dot onion addresses are a minimum of

16 alphanumeric characters, chosen largely at random. This address structure makes .onion URLs hard to recall and nearly impossible to guess thematically, as one might with something like theweathernetwork.com. While search engines do exist for the Tor Darknet (e.g. NotEvil), their effectiveness is somewhat limited.

A very common informational accumulation practice, as a result, is for users to pursue knowledge of specific markets and .onion addresses by visiting so-called wiki sites, such as www.darknetstats.com, or the now closed DeepDotWeb. These wiki services aggregate news about the Darknet market ecosystem and also curate cryptomarket .onion addresses. From these sites, prospective cryptomarket users can complete the information accumulation step of the cryptomarket crime script by discovering a precise .onion address for the site they wish to visit. This address can then be copied and pasted into the search bar of the Tor browser. Assuming the selected site is up (DDoS attacks on cryptomarkets are common on the Darknet, often necessitating a site mirroring process), the prospective user has successfully completed the first phase of the script and is now viewing the login page of their selected market.

Informational Accumulation: Known Law Enforcement Interventions

The informational accumulation stage of the cryptomarket crime script presents a number of vulnerable points that law enforcement has leveraged effectively during the course of their publicly known investigations. Broadly, law enforcement actions targeting this stage of the script can be categorized as either largely 1) preventive or 2) investigatory. As the short cases below highlight, preventive strategies try to limit the effective accumulation of information by motivated offenders, making the completion of the first stage of the cryptomarket script harder to accomplish. Investigatory strategies leverage "digital traces" that new and current users leave online to identify suspects (Décary-Hétu & Aldridge, 2015). Oftentimes, current users of Darknet markets will share information via regular web platforms in order to support the informational accumulation of new users. These efforts are prone to intervention by law enforcement.

It is important to note that at some point in the informational accumulation stage of the cryptomarket crime script, users can choose to switch to the Tor browser and leverage the anonymity of the system to mask their IP address information. Prior to this eventual possibility, however, a series of searches and posts are likely to be done via more traditional web browsers. These search and exposure steps can provide a host of "digital traces" which can be leveraged in the course of an investigation (Décary-Hétu & Aldridge, 2015). While lacking the precision needed to investigate specific crimes, Google searches, for example, can be used as a proxy for activity in the initial stage of the cryptomarket crime script and do indeed correlate with self-declared cannabis consumption patterns within US states (Jardine & Lindner, 2020) and can predict the use of novel drugs (Perdue et al., 2018).

A few vignettes further illustrate the range of potential techniques used by law enforcement to exploit the informational accumulation stage of the script. One example of a preventive operation designed to increase the costs of completing the first stage of the cryptomarket crime script is the takedown of the link aggregation site (i.e. wiki) DeepDotWeb in 2019. Prior to its closure, DeepDotWeb was likely one of the most popular Darknet news and link aggregation sites, making it an integral initial point of departure for the cryptomarket crime script. In cooperation with European and Israeli law enforcement, the site was eventually seized by the Federal Bureau of Investigation (FBI) pursuant to 18 USC 1956(h), 981, 982. Two individuals in Israel were arrested, along with others in France, the Netherlands, Germany, and Brazil. Those arrested were charged with profiting from a criminal enterprise, because they were allegedly taking money to curate links to cryptomarkets that could be used to direct users toward illegal products (Lecher, 2019). In March of 2021, Tal Prihar, one of the co-operators of the site, pled guilty to conspiracy to commit money laundering, and agreed to forfeit the upward of eight million dollars in Bitcoin he had received from the operators of various Darknet market sites (United States. Department of Justice, 2021).

Beyond the immediate administration of justice in this case, the seizure of this site made the completion of the information accumulation stage of the crime script more challenging, at least until the ecosystem generated new wiki sites such as Darknetstats. Closure of r/darknetmarkets by Reddit in 2018 would have a similar effect of complicating the successful completion of the first stage of the cryptomarket crime script and should therefore reduce Darknet market activity in some measure. In simple terms, if a user cannot learn of the .onion address for the market they want to visit, then they cannot easily venture to the site, given the alphanumeric address structure of Onion/Hidden Services. Indeed, extrapolating from individual experiences with the information accumulation process, the rate of expansion of the Darknet market ecosystem might be at least partially limited by the high costs associated with this accrual of how-to knowledge, even absent efforts by law enforcement to complicate the completion of this stage of the script (Kowalski et al., 2019).

Law enforcement can also leverage digital identifiers on Clear Web platforms to de-anonymize individuals who might be engaged in online discussion about cryptomarkets. Such individuals could include prospective users who are engaging in the informational accumulation stage of the script and current market participants who are attempting to facilitate the movement of others through this stage via greater information sharing. One example is a 2015 investigation of r/darknetmarkets. Reddit is a popular social networking forum for discussion of Darknet drug market related activities, with subreddits such as darknetmarkets acting as a focal point (at least before it was closed down in 2018). In many cases, the discussion on these threads is remarkably specific, with individuals claiming to be staff at various cryptomarkets or alleging that they hold information about the identities of site administrators (Greenberg, 2015). In this case, the Baltimore branch of the Department of Homeland Security sent Reddit a subpoena requesting IP addresses, account information, and site activity of five individuals who had been active on the subreddit. Reddit initially contested the subpoena but eventually complied (Jardine, 2019a). According to Reddit's privacy policy, IP address information of posters is kept for 90 days, with the possibility of more extended storage should the company be required to do so. Since IP addresses (absent the use of a masking technology such as a VPN or Tor) typically resolve back to a specific autonomous systems number (ASN) and Internet Service Provider (ISP), they can often be used to associate posts and online activity with unique physical world addresses, as was the intention in this case.

Investigation into Clear web sites can also focus on other digital identifiers beyond IP address information. In an infamous example, the Dread Pirate Roberts, who launched Silk Road, was identified via a search of a Clear Web bitcoin news site called bitcointalk.org. In this instance, IRS Special Agent (SA) Gary Alfred recognized that eventual Darknet users must start by accumulating information on the Clear Web and then work their way down to particular markets. As he indicated in his testimony during Ross Ulbritch's trial, "I figured it [Silk Road] had to be [marketed] on the regular Internet so someone could tell you where to go" (Mullin, 2015).

SA Alfred was able to find the bitcointalk.org post by simply Googling "Silk Road" and ".onion". This procedure led to a post publicizing Silk Road by a person using the screenname "Altoid". Once SA Alfred had identified the Altoid screenname as an account of interest with links to Silk Road, he then searched the forum for all posts by this handle. Doing so led to a separate post asking to hire an IT specialist that also included a Gmail address linking the Altoid screenname to a real-name person. The full Altoid post read:

> "Hello, sorry if there is another thread for this kind of post, but I couldn't find one. I'm looking for the best and brightest IT pro in the bitcoin community to be the lead developer in a venture backed bitcoin startup company. The ideal candidate would have at least several years of web application development experience, having built applications from the ground up. A solid understanding of oop and software architecture is a must. Experience in a start-up environment is a plus, or just being super hard working, self-motivated, and creative.
> Compensation can be in the form of equity or a salary, or somewhere in-between.
> If interested, please send your answers to the following questions to rossulbricht at gmail dot com
>
> 1) What are your qualifications for this position?
> 2) What interests you about bitcoin?
>
> From there, we can talk about things like compensation and references and I can answer your questions as well. Thanks in advance to any interested parties. If anyone knows another good place to recruit, I am all ears" (Altoid, 2011).

Once SA Alfred secured evidence of the link between the rossulbricht@gmail.com email, the Altoid screen handle, and posts surrounding Silk Road and its .onion address, he secured a warrant to gain access to the Gmail account. Within the email account's records, there were a number of missives revealing Ross Ulbricht as the real identity of Altoid (Mullin, 2015). Once identified and later linked to a host of criminal activities, Ulbritch was subsequently charged with being the founder and main administrator of Silk Road and was ultimately convicted and sentenced to 40 years in prison.

The investigatory examples above leveraged the details associated with the informational accumulation stage of the cryptomarket crime script to de-anonymize market participants.

Step 2: Account Formation

Account Formation: Detailed Script Steps

Once sufficient information has been obtained by a prospective user, a motivated offender can then employ the Tor browser to reach the login screen of a chosen Darknet cryptomarket. At this point, potential buyers and vendors undertake similar steps until the end of this stage of the script, at which point vendors need to take additional steps to establish an "online presence", much as a seller on Etsy or eBay might have to do. Movement through the first three steps of this stage of the script can be somewhat non-linear, with individuals creating cryptocurrency wallets, for example, before setting up a market account.

An intuitive flow, however, is to begin with the Darknet market account creation step. This process usually involves the selection of a screenname and the completion of a CAPTCHA, meant to dissuade web scraping and attacks by bots. Both vendors and buyers also need to set up a cryptocurrency wallet. Bitcoin is the coin of choice on most cryptomarkets, although other currencies such as Monero have gradually gained in popularity over time (ElBahrawy et al., 2020). Setting up a crypto wallet of choice is fairly simple. Generally speaking, cryptocurrencies can be stored in one of three types of wallets: a hosted wallet, a non-custodial wallet, or a hardware wallet (Coinbase, 2020). Hosted wallets, which give more control over a person's cryptocurrency to a third party, are simpler to use, but least desirable from an operational security perspective. Most cryptomarket users likely use either non-custodial or hardware-based wallets, funded with transfers of funds from other locations. While Bitcoin is often talked about as an anonymous payment method, it is better categorized as pseudo-anonymous since all transactions by a wallet address are (unless they are further obfuscated by a tumbler/mixing service) recorded in the blockchain. The blockchain, in turn, is visible to all, meaning that a record of all bitcoin transactions (including wallet addresses and amount transferred) is visible and analyzable to anyone who downloads the blockchain. Since many cryptocurrency exchanges are subject to anti-money laundering rules and KYC (know your customer) legislation, sufficient analysis of the blockchain can sometimes lead back to real-world identities.

As a part of the account creation stage, vendors and buyers could also set up a PGP key to ensure secure, encrypted communication when using a cryptomarket. PGP encryption involves the use of both a public (known to everyone) and private (unknown to the public) key. Individuals sending messages encrypted with PGP would use an intended recipient's known public key to encrypt a message and the recipient would then use their private key to decrypt the message. PGP is highly effective, easy to employ, and has stood the test of time, making it a common security step employed by cryptomarket participants. It is not, however, strictly necessary, as messages can be sent between buyers and sellers via markets (at times with built in PGP) or via other peer-to-peer channels, such as the messaging applications Telegram or Signal, or private email services such as Proton Mail (Childs et al., 2020; Moyle et al., 2019).

Having established market, bitcoin and potentially PGP accounts, vendor and buyer scripts diverge somewhat, as shown in Figure 4. Buyers can move on at this stage to the market use stage of the cryptomarket script. Vendors, however, need to post product listings, complete with descriptions and uploaded photos, if they are to successfully compete in the cryptomarket ecosystem. More generally, vendors need to carefully develop and manage their online identity. This identity cultivation process is not dissimilar to the activity of sellers on Clear Web sites such as Etsy or eBay. Indeed, features of a vendor's account help determine 1) the prices they can charge (Hardy & Norgaard, 2016), 2) the degree of cooperation and trust that emerges between buyers and sellers (Norbutas et al., 2020; Przepiorka et al., 2017), and 3) the clustering of many customers onto few vendors that is a common pattern of e-commerce on Darknet cryptomarkets (Christin, 2013; Soska & Christin, 2015). Once a vendor has taken the additional steps of curating their profile and product pages, they are then ready to move into the market use stage of the script.

Account Formation: Known Law Enforcement Interventions

The account formation stage of the script also presents a number of unique points of intervention for law enforcement. While the steps taken by prospective users at this stage will be masked by the Tor browser (which is needed if one is to reach a cryptomarket), market account creation, the funding of bitcoin wallets, transactions between cryptocurrency wallets, or even the curation of online vendor identities can leave traces that can be collected, cross-referenced, and potentially used to identify market participants.

One of the best examples of law enforcement activity targeting this stage of the script for investigative purposes occurred during Operation Bayonet/GraveSac in 2018. This operation was a joint undertaking by the Darknet Opioid Taskforce (J-Code) in the FBI and the Netherlands National High Tech Crime Unit (NHTCU).

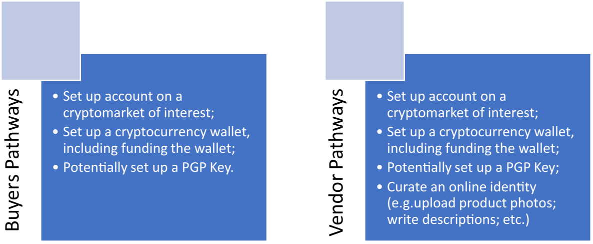

Buyers Pathways
• Set up account on a cryptomarket of interest;
• Set up a cryptocurrency wallet, including funding the wallet;
• Potentially set up a PGP Key.
Vendor Pathways
• Set up account on a cryptomarket of interest;
• Set up a cryptocurrency wallet, including funding the wallet;
• Potentially set up a PGP Key;
• Curate an online identity (e.g.upload product photos; write descriptions; etc.)

Fig. 4 Stage 2: Account Formation

These agencies targeted two of the largest Darknet sites in operation at the time: AlphaBay and Hansa.

The joint operation began as two separate initiatives. The Dutch police had been investigating the Hansa market since 2016, when it became apparent that the main administrators were in Europe. Mirroring FBI tactics used in the closure of the Darknet child abuse site Playpen in 2015 (Chertoff & Jardine, 2021), the NHTCU decided that they would attempt to seize direct control of the Hansa cryptomarket so that they might run the site as administrators (Greenberg, 2018). As Gert Ras, the head of the NHTCU put it, "We came up with this plan to take over. […] We had to get rid of the real administrators to become the administrators ourselves (Greenberg, 2018)." During the course of the NHTCU's investigations, it also became apparent that the FBI had located the primary server of the site AlphaBay, run by a Canadian named Alexandre Cazès, who was then living in Thailand.

The identification of server locations and the identities of the actors behind the two largest cryptomarkets in use at the time created an opportunity for law enforcement. Since approximately 66.1% (+/- 16.1%) of cryptomarket participants tend to migrate from a closed market to the next largest available marketplace (ElBahrawy et al., 2020), the prospect of being able to coordinate the disruption of the two biggest players gave rise to a lot of possibilities. As NHTCU Director Ras put it, "Not only would we get this effect of undermining the trust in dark markets [by controlling Hansa], we'd also get this influx of people" from AlphaBay when it went offline (Greenberg, 2018).

The NHTCU investigation into Hansa leveraged information from the account creation stage of the cryptomarket crime script in two primary ways. First, in order to seize control of the Hansa cryptomarket, the Dutch police needed to locate the server upon which the site was hosted. Since Tor obfuscates these details by design, server location is often not readily apparent to law enforcement unless there is a configuration error (e.g. potentially Silk Road 1) or some other way to track down the physical location of the server. In this case, having previously zeroed in on a couple of individuals as the likely Hansa administrators, Dutch investigators eventually located a bitcoin wallet address left in an old IRC protocol chat between the two suspects. By analyzing the blockchain, law enforcement was then able to link this address to a payment provider, which the Dutch police approached with a warrant for additional information. The payment service provider pointed to a Lithuanian webhosting company as the ultimate recipient of the bitcoin transaction. By next approaching the Lithuanian company, the NHTCU was able to locate the physical site of the server hosting Hansa and assume administrative control of the site.

Once the Dutch police had full control of Hansa, they were then able to re-write the code of the site in such a way as to capture information about vendors and buyers as revealed during the account formation stage of the cryptomarket script. First, by tweaking the site's code, they were able to store user passwords as plaintext in place of encrypted hashes. Second, by reconfiguring the site, they were also able to compromise its communication functions. The site had provided a function where vendors and buyers could communicate via PGP encrypted messaging. The NHTCU reconfigured the system to save a version of the message before it was encrypted using the recipient's public key. These messages often included home addresses and delivery instructions. Finally, the original Hansa site had been set up to strip metadata information from uploaded product photographs. The NHTCU re-wrote this function to record the metadata information instead, allowing the Dutch police to pinpoint the precise geographical location where drug product photos were taken (Greenberg, 2018).

Without any other intervention, the site reconfiguration steps would have allowed the Dutch police to collect a lot of useful investigatory information about users as they created accounts and curated online product descriptions. But, with the FBI closing in on Alexandre Cazès and AlphaBay, they were also able to take clear advantage of the displacement of users from one site to another. Cazès was taken into custody in Thailand on July 5th, 2017. He later committed suicide while in Thai custody. AlphaBay went offline the same day. True to form, users from the world's largest cryptomarket flooded to Hansa, with the number of new users spiking from around 1,000 to over 6,000 in the days following the closure. Due to the various site reconfigurations, the Dutch police were able to record details of these new users in great detail as they created their accounts.

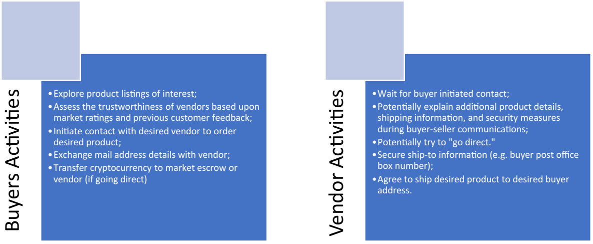
As a result of the joint operation, law enforcement was reportedly able to get information on some 420,000 users, including at least 10,000 home addresses, seize 1,200 bitcoin from Hansa's market escrow, and make a number of arrests in Europe and elsewhere (Greenberg, 2018). The joint operation also led users who migrationed from Hansa to Dream to undertake more extensive security steps, including a greater use of PGP communication keys and the abandonment of previous vendor identities (van Wegberg & Verburgh, 2018).

In sum, law enforcement has demonstrably and effectively leveraged aspects of the cryptomarket Account Creation stage of the cryptomarket script to police drug crimes in this setting.

Step 3: Market Use

Market Use: Detailed Script Steps

The market use stage of the cryptomarket crime script involves all the steps needed to leverage a Darknet market to engage in a drug exchange. As shown in



Buyers Activities

- Explore product listings of interest;
- Assess the trustworthiness of vendors based upon market ratings and previous customer feedback;
- Initiate contact with desired vendor to order desired product;
- Exchange mail address details with vendor;
- Transfer cryptocurrency to market escrow or vendor (if going direct)

Vendor Activities

- Wait for buyer initiated contact;
- Potentially explain additional product details, shipping information, and security measures during buyer-seller communications;
- Potentially try to "go direct."
- Secure ship-to information (e.g. buyer post office box number);
- Agree to ship desired product to desired buyer address.

Fig. 6 Stage 3: Market Use

Figure 6, the detailed scripts for buyers and vendors diverge in the market use phase, even as they interact with one another.

Buyers begin the process of market use by using built-in market search functions to look for a desired product. Such activity could include, for example, searches for drugs using various formal and street permutations of a drug name (e.g., heroin, dope, skag, China white, etc.). Searches can be further refined to include ship-from/ship-to details, in order to ensure that the selected vendor would be willing to send the product to the buyer's location.

Next, a buyer would assess the overall trustworthiness of products and vendors based upon market-hosted trust signals. These signals include items such as 5-star rating systems, a transparent number of previous customers, and previous customer feedback. Some markets employ more sophisticated measures including "trustworthiness" scores that aggregate available statistics into a single metric. Users can also search comment forms to get a sense of whether a vendor is trustworthy or a product is as advertised. Once a buyer has found a desired product and selected a potential vendor from which to buy their desired good, they would then initiate contact with the vendor, likely through market-based messaging functions.

At this stage, the vendor, who has likely been sourcing supply, completing other sales, and engaging in profile curation activities while awaiting contact from a buyer, would begin their steps of the market use stage of the cryptomarket crime script. Depending upon the nature of the initial contact, a vendor might need to provide additional information to the buyer, including but not limited to further detail on 1) the product, 2) packaging and shipping methods, and 3) the wider security measures used by the vendor. Such conversations are presumably especially likely if the product might ship across international boundaries, where law enforcement scrutiny tends to be higher (Décary-Hétu et al., 2016).

During this communication phase, a vendor can also attempt to convince the buyer to "go direct," which essentially implies that the buyer and seller would move their communications away from the cryptomarket toward secure peer-to-peer messaging applications (e.g. Telegram or Signal) and would exchange funds directly. While direct exchanges raise a number of buyer anxieties about potential exposure to law enforcement via undercover operations and the quality of substances secured through such direct channels, decentralization of this sort is an increasingly common feature of the process of online drug exchange, particularly as law enforcement has increased their presence on the Darknet (Childs et al., 2020; Moyle et al., 2019; Shortis et al., 2020).

In the next step of the market use stage of the cryptomarket script, the buyer would supply a mailing address to the vendor. At this point, the vendor would agree to ship the desired product to the supplied address and provide any special receipt details, such as additional security suggestions at time of pick up. Assuming the vendor agrees to ship to the supplied address, the buyer would also transfer the funds for the purchase from their cryptowallet to either the market escrow or, if the buyer and seller decide to go direct, the vendor's wallet. These last steps complete the third stage of the cryptomarket script, moving both buyer and seller into the final stage of the script.

Market Use: Known Law Enforcement Interventions

Interventions involving this stage of the script can take two forms: 1) investigatory and 2) deterrent. Investigatory operations targeting this stage of the script leverage the anonymity of Tor and the inevitable sociality of cryptomarket exchanges (Barratt et al., 2016b; Jardine, 2015; Maddox et al., 2016). To complete the market use stage of the script effectively, putative buyers and sellers need to interact with one another under a cloak of anonymity, up to and including exchanging some amount of sensitive personal details (e.g. addresses) and potentially going direct (which might involve sharing phone numbers).

These social interactions under the cloak of anonymity open up a space for potential exploitation by undercover law enforcement agents (Jardine, 2015; Martin, 2014a). Law enforcement can readily pose as any of the three primary agents in the cryptomarket ecosystem: admins, buyers, or vendors. Law enforcement has, as in the case of Silk Road 1.0, for example, infiltrated the group of individuals administering the site in order to secure details on site operation and to learn the identities of the other admins (Bilton, 2017; Ormsby, 2014). More recently, US law enforcement undertook an extensive year-long investigation targeting Darknet vendors which culminated in 2018. In this case, an agent of the Department of Homeland Security's Investigations division posed as a money launderer, offering to exchange "U.S. currency for virtual currency" (United States. Department of Justice, 2018). This operation led to the prosecution of some 35 US-based Darknet vendors, the confiscation of drugs and additional contraband, and the seizure of over $23.6 million USD in ill-gotten cryptocurrency (United States. Department of Justice, 2018).

More to the deterrent side of things, law enforcement has also employed information from the market use stage of the script to engage in what are known as "knock and talk" operations (Bradley, 2019; Bradley & Stringhini, 2019). In these operations, law enforcement leverages details gleaned from previous investigations to approach individuals who used a cryptomarket in the past to engage in a drug exchange. These individuals are then notified that they have been observed engaging in these sorts of activities. The goal of knock and talk operations is to deter the future use of Darknet cryptomarkets by showcasing the intelligence-gathering power of law enforcement. Operations Decrypt in the United States and Mirum in Europe, for example, leveraged data gleaned from the Hansa takedown to approach suspects and issue stern warnings. As the DEA European Regional Director, Kevin Scully, put it in an official press release for the 2018 Operation in the US: "These law enforcement actions should serve notice that no drug criminal is safe or anonymous on the dark web" (United States. Drug Enforcement Agency, 2018).

Another very well-documented example of a knock and talk exercise is Operation Hyperion (Bradley, 2019; Bradley & Stringhini, 2019). This knock and talk operation took place in the Fall of 2018. Like other operations of this sort, the goal was to approach those suspected of engaging in drug exchange on Darknet markets in order to dissuade future use. As is not uncommon in this space, the operation generated chatter on Reddit. Within two threads in particular, /r/darknetmarkets and /r/dnmuk, some 184 posts and over 1,000 comments about Operation Hyperion emerged in the week after the announcement of the Operation by law enforcement. The content of these posts and comments tended to cluster around five primary areas, as presented by Bradley and Stringhini and summarized in Table 1 (Bradley & Stringhini, 2019).

User speculation about how law enforcement conducted the Operation is revealing, as all of the predominant theories point to law enforcement exploitation of some sort of data generated during the Market Exchange stage of the cryptomarket script. These data, the theories go, were collected after the fact by law enforcement, either by commandeering the servers for the site in question or by analyzing the Bitcoin blockchain. This example, like those of Operations Decrypt, Mirum, and Hyperion, highlights the way in which the Market Exchange stage of the cryptomarket script can be leveraged for the purpose of interventions aimed at deterring future use of these markets. Much of the data leveraged in knock and talk operations of this sort could also be used to direct police surveillance efforts, as was done during Operation DisrupTor in 2020 (see below (Barrett, 2020; United States. Federal Bureau of Investigation, 2020)).

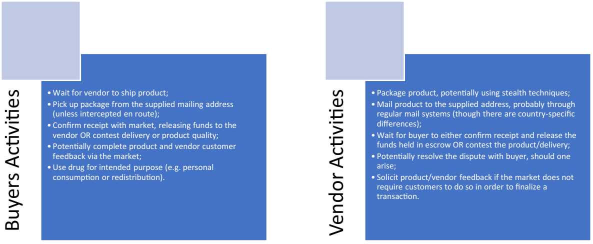
Step 4: Delivery/Receipt

Delivery/Receipt: Detailed Script Steps

The final stage of the cryptomarket crime script largely moves off the networks of Tor and into the physical world. Figure 7 details the discrete steps taken during

Table 1 Reddit Chatter Following a High Profile Knock and Talk Operation

Thematic Point	Findings
Personal Descriptions	Only a small number of posters indicated they were approached by law enforcement, most saying so only after the announcement of the Operation. Some might not realize they were being contacted as a part of a coordinated effort, suggestive of the idea that the operation's scope and impact might be limited.
How it was Done	Many speculated that law enforcement was leveraging details from market exchange conducted on either Silk Road 1.0 or Silk Road 2.0. Both markets were captured by law enforcement, who, it was assumed, might be leveraging details (e.g. addresses, names, etc.) to contact those involved. Other speculated that the weak point was the bitcoin blockchain ledger and that law enforcement was retroactively observing market transactions via this mechanism.
Consequences	Many posters linked the operation to Canadian seizures of product, but these concerns quickly subsided. Few thought those approached in the Operation were in any serious legal jeopardy.
Advice	Most advice seemed to be either jokes or suggestion for calm. Some suggested various obfuscation steps of various levels of veracity, such as destroying computer hardware or moving to another address or country.
Opinions on the Operation	Views on the Operation tended to be split. Some thought that the operations into the Darknet were inevitable and that Operation Hyperion was maybe better than most. Many others felt the Operation was illegitimate. A few posters and comments felt it was effective.



- Wait for vendor to ship product;
- Pick up package from the supplied mailing address (unless intercepted en route);
- Confirm receipt with market, releasing funds to the vendor OR contest delivery or product quality;
- Potentially complete product and vendor customer feedback via the market;
- Use drug for intended purpose (e.g. personal consumption or redistribution).

- Package product, potentially using stealth techniques;
- Mail product to the supplied address, probably through regular mail systems (though there are country-specific differences);
- Wait for buyer to either confirm receipt and release the funds held in escrow OR contest the product/delivery;
- Potentially resolve the dispute with buyer, should one arise;
- Solicit product/vendor feedback if the market does not require customers to do so in order to finalize a transaction.

Fig. 7 Stage 4: Delivery/Receipt

this stage by buyers and sellers. After a transaction has been initiated during the Market Use phase of the script, buyers usually move into an initially passive position while they await the delivery of their desired product.

Vendors (or vendor conglomerates), for their part, start this stage of the script by packaging the ordered product for delivery. Vendors who aim to maintain or build their reputations as well as minimize potential interception of the product in transit will likely package the drugs using a variety of stealth shipping techniques (Aldridge & Askew, 2017; Rhumorbarbe et al., 2016). While law enforcement manuals on drug interdiction are widely shared on Darknet forums (Martin, 2014a), online discussion of the specifics of vendor stealth practices tends to be discouraged by forum participants out of fear that law enforcement is watching (Smith & Frank, 2020). Nevertheless, several stealth techniques, as detailed in

Table 2 Known Stealth Shipping Techniques for Darknet Drug Market Exchange

Stealth Shipping Type	Description
Moisture barrier bags (MBB)	Airtight packing to avoid having the smell of drugs leak out of a package.
Alcohol/bleach dripping	A technique used to mask the odor of a package and obliterate DNA.
Heat sealed bags	Plastic packaging melted together to produce an airtight seal.
Printed labels	Use of printed labels to mask handwriting and reduce delivery errors due to illegible print.
Drug size, shape, and texture obfuscation	Masking the feel, shape or texture of drugs through alternative packaging. For example, shipping pills of MDMA in a DVD case or hollowed-out book.
Drop shipping	Use of third parties in the buyer's country of origin who can be tasked with shipping the product so as to avoid crossing international boundaries with greater scrutiny. Drop shipping can also be used to avoid having the drug originate in countries deemed high risk, such as the Netherlands, USA or Canada.
Real destination/recipient addressing	Vendors often suggest buyers provide their real name and address so as to not arouse suspicion of local mail carriers. This advice is asymmetrical, as vendors are unlikely to supply a valid return address information.

Table 2, are widely used. Common to the various methods is the idea of obfuscation, of either smell, size, shape, texture, or point of origin.

Once the ordered product has been packaged, a vendor would then mail the product to the address supplied by the buyer. Drop shipping obfuscation techniques would imply that a vendor uses a third party to physically ship the package, changing the locus of this step. If drop shipping is not used, then a vendor (or a local agent) would deposit the package in the mail themselves. Despite its ties to government, vendors typically prefer to use official mail systems for delivery, in place of private services such as UPS or FedEx. State-based mail systems have several desirable features from a vendor's perspective, including volume, greater restrictions on search and seizure, and potential anonymity of drop off. (In Finland, vendors and buyers on Darknet drug markets such as *Sipulikanava* often forgo the mail altogether and instead use direct person-to-person meet ups, changing this aspect of the script (Demant et al., 2019). Such behaviors seem to be rare in most other countries and might result from a combination of Finnish social forces and population distribution).

When preparing to complete the mail drop-off step, vendors are able to leverage robust online discussion to glean best practices that help manage risk, reduce the probability of getting caught, and potentially minimize the severity of any charges (Aldridge & Askew, 2017). One poster on a Silk Road 1.0 forum, for example, advised: "Rotate your mailbox drops randomly in case LE [law enforcement] are watching particular boxes. If LE makes an order it can be traced to a box. All they have to do is find TOR users in the vicinity, so avoid using mailboxes near you" (Cited in Aldridge & Askew, 2017, p. 105). Another admonished: "Well done. You've now been filmed on CCTV mailing packages with illegal content. NEVER go into a post office or hand to a postal employee." Yet another post simply noted: "ship the usual (anonymous!) way using a mailbox" (Cited in Aldridge & Askew, 2017, p. 105).

Once mailed, the package would work its way through the postal system transit route. Law enforcement might intercept the package at this stage *en route*. While many packages containing illicit substances are intercepted daily, it is not uncommon for many more to make it past various screening points, even at international entry points. During the initial investigation into Silk Road, for example, the DHS officers involved ordered an assortment of drugs for delivery through the Chicago O'Hare processing facility. The goal was to discern the fraction of packages ordered from Silk Road that were interdicted by customs. The results of the experiment were grim. Of the 18 orders placed, one package was lost in transit and 16 failed to be intercepted, meaning only a single package was effectively stopped at customs at a major point of mail entry (Bilton, 2017, p. 88)

Assuming the package is not intercepted by law enforcement, a buyer would then be able to pick up the package from the supplied postal address. Similar to online discussions detailing best practices for vendors at the timing of shipping, many forums on Clear Web sites such as Reddit and Darknet equivalents such as Dread detail prudent steps for buyers at time of pickup. One Reddit post, for example, suggests that buyers should act casual: "Don't be waiting by your mailbox everyday go and get the mail later on. Don't do anything suspicious that'll make your mail deliverer raise a red flag. All it takes is for them to report to their supervisor that a specific address has been receiving many packages from strange places" (Cited in Smith & Frank, 2020, p. 4699).

If the package is picked up by the buyer with no further issue and the buyer and seller have not agreed to "finalize early", then the buyer can then either confirm receipt and finalize the transaction or contest the delivery. Contesting the delivery will lead to a potential arbitration process by the marketplace. Finalizing the safe arrival of the product will cue the market escrow to release the buyer's cryptocurrency to the vendor. Some cryptomarkets, such as Silk Road, required customer feedback of the product and vendor in order to finalize the sale. Other markets, such as AlphaBay, make this step optional. Regardless of its obligatory nature, customers often do rate transactions and provide comments on completed exchanges. Vendors can also follow up with buyers and solicit feedback in an effort to curate their online identity. The vendor's steps of the script end at this point. The buyer, having received the illicit substance and finalized the transaction, can then use the product for its intended purpose, which could range from personal use to social supply and local redistribution (Aldridge & Décary-Hétu, 2016; Aldridge et al., 2018; Demant et al., 2018).

Thus ends one cycle of the Darknet cryptomarket crime script.

Delivery/Receipt: Known Law Enforcement Interventions

Offline interception is one obvious way to stifle the use of Darknet markets to procure and distribute illicit substances. Law enforcement can also use the physical world portion of the cryptomarket crime script to target vendors and buyers directly. Operation DisrupTor in 2020 is a good example of a joint law enforcement operation that leveraged the vulnerabilities of the Delivery/Receipt stage of the cryptomarket script to arrest some 179 individuals in seven countries (United States. Department of Justice, 2020). The initial leads into the location, screennames, and shipping patterns of vendors started with the closure of Wall Street Market during Operation SaboTor the year prior in 2019, where the backend server was seized for examination by law enforcement (Barrett, 2020). From there, discrete investigations into individual vendor networks began across the US.

Both sellers and buyers remain vulnerable during the final offline stage of the cryptomarket script. In discussion of Operation DisrupTor, FBI Special Agent Christopher Siliciano, for example, noted that even while the online portions of the cryptomarket script provide some protections, sellers remain vulnerable during the Delivery/Receipt stage of the process: "Sellers still have to turn their money into cash, they still have to pick up the drugs, they still have to transport the drugs. Not all of that happens on the internet" (FBI, 2020). Buyers, too, face offline challenges. Special Agent Christopher Hick noted the challenges for buyers: "Even if you're getting stuff shipped to a post office box under a fake name, you have to open that mailbox. You have to touch that package" (United States. Federal Bureau of Investigation, 2020). Law enforcement can monitor postal addresses gleaned from various methods and set up sting operations to capitalize upon the final stage of the Darknet market crime script.

Conclusions

While technological innovation in drug exchange continues apace (Childs et al., 2020; Moyle et al., 2019), Darknet cryptomarkets are now a permanent feature of local, regional, and global drug supply (Winstock et al., 2019). Law enforcement has undertaken a number of market closures over time, but the ecosystem as a whole has proven to be very resistant to these actions (Décary-Hétu & Giommoni, 2017; Duxbury & Haynie, 2018; ElBahrawy et al., 2020; Van Buskirk et al., 2017).

In line with other works employing cybercrime scripts to analyze various forms of criminal activity (Chiu et al., 2011; Cornish, 1994; Dehghanniri & Borrion, 2021; Hutchings & Holt, 2014), this article provides a wider view of law enforcement interventions by introducing a novel crime script for Darknet drug markets. New buyer and seller activities using Darknet markets invariably move through four stages: 1) informational accumulation; 2) account formation; 3) market use; and 4) Delivery/Receipt. In detailing the stages of the novel cryptomarket crime script, the article also documents numerous examples of known law enforcement interventions targeting each discrete stage in the process of online drug exchange via Darknet marketplaces. These examples show that Darknet market closure is only one tool in the proverbial toolkit and that law enforcement has learned to intervene effectively at each stage of the script in ways that can introduce additional friction into the process of online, anonymous drug sale and procurement.

References

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.

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

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

Altoid. (2011). *IT pro needed for venture backed bitcoin startup*. https://bitcointalk.org/index.php?topic=47811.msg568744#msg568744

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society, 20*(4), 497–512.

Barabási, A.-L. (2014). *Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life*. Basic Books.

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, 109*(5), 774–783. https://doi.org/10.1111/add.12470

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016a). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, *35*(Supplement C), 24–31. https://doi.org/10.1016/j.drugpo.2016.04.019

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016b). 'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road.

International Journal of Drug Policy, *35*(Supplement C), 50–57. https://doi.org/10.1016/j.drugpo.2016.04.006

Barrett, B. (2020). 179 Arrested in Massive Global Dark Web Takedown. *Wired*. https://www.wired.com/story/operation-disruptor-179-arrested-global-dark-web-takedown/

Bilton, N. (2017). *American kingpin: The epic hunt for the criminal mastermind behind the Silk Road*. Penguin.

Bradley, C. (2019). *On the Resilience of the Dark Net Market Ecosystem to Law Enforcement Intervention* UCL (University College London)].

Bradley, C., & Stringhini, G. (2019). A Qualitative Evaluation of Two Different Law Enforcement Approaches on Dark Net Markets. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),

Chen, A. (2011). The Underground Website Where You Can Buy Any Drug Imaginable. *Gawker*. https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160

Chertoff, M., & Jardine, E. (2021). *Policing the Dark Web: The Legal Challenges in the 2015 Playpen Case*. CIGI Papers, no. 259 - November 2021.

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/10.1177/0022042619897425

Chiu, Y.-N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology, 51*(2), 355–374.

Christin, N. (2013). *Traveling the silk road: a measurement analysis of a large anonymous online marketplace* Proceedings of the 22nd international conference on World Wide Web, Rio de Janeiro, Brazil.

Coinbase. (2020). *How to set up a crypto wallet*. https://www.coinbase.com/learn/tips-and-tutorials/how-to-set-up-a-crypto-wallet

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention.

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime, 2*(2), 122–141.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous [journal article]. *Crime, Law and Social Change, 67*(1), 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*(Supplement C), 69-76. https://doi.org/10.1016/j.drugpo.2016.06.003

Dehghanniri, H., & Borrion, H. (2021). Crime scripting: A systematic review. *European Journal of Criminology, 18*(4), 504–525. https://doi.org/10.1177/1477370819850943

Demant, J., Bakken, S. A., Oksanen, A., & Gunnlaugsson, H. (2019). Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review, 38*(4), 377–385.

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going Local on a Global Platform:A Critical Analysis of the Transformative Potential of Cryptomarkets for Organized Illicit Drug Crime. *International Criminal Justice Review, 28*(3), 255–274. https://doi.org/10.1177/1057567718769719

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

Dolliver, D. S., Ericson, S. P., & Love, K. L. (2018). A Geographic Analysis of Drug Trafficking Patterns on the TOR Network. *Geographical Review, 108*(1), 45–68. https://doi.org/10.1111/gere.12241

Duxbury, S. W., & Haynie, D. L. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks, 52*, 238–250. https://doi.org/10.1016/j.socnet.2017.09.002

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific Reports, 10*(1), 18827. https://doi.org/10.1038/s41598-020-74416-y

Gehl, R. W. (2018). *Weaving the dark web: legitimacy on Freenet, Tor, and I2P*. MIT Press.

Greenberg, A. (2015). Feds Demand Reddit Identify Users of a Dark-Web Drug Forum. *Wired*. https://www.wired.com/2015/03/dhs-reddit-dark-web-drug-forum/

Greenberg, A. (2018). Operation Bayonet: Inside the Sting That Hijacked an Entire Darknet Drug Market. *Wired*. https://www.wired.com/story/hansa-dutch-police-sting-operation/

Hardy, R. A., & Norgaard, J. R. (2016). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics, 12*(3), 515–539. https://doi.org/10.1017/S1744137415000454

Horton-Eddison, M., & Di Cristofaro, M. (2017). Hard interventions and innovation in crypto-drug markets: The escrow example. *Policy Brief, 11*.

Hout, M. C. V., & Bingham, T. (2013a). 'Silk Road', the virtual drug marketplace: A single case study of user experiences. *International Journal of Drug Policy, 24*(5), 385–391. https://doi.org/10.1016/j.drugpo.2013.01.005

Hout, M. C. V., & Bingham, T. (2013b). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*(6), 524–529. https://doi.org/10.1016/j.drugpo.2013.08.011

Hutchings, A., & Holt, T. J. (2014). A Crime Script Analysis of the Online Stolen Data Market. *The British Journal of Criminology, 55*(3), 596–614. https://doi.org/10.1093/bjc/azu106

Jardine, E. (2015). The Dark Web Dilemma: Tor, Anonymity and Online Policing. *Global Commission on Internet Governance Paper Series*(21), 1-24. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711

Jardine, E. (2017). 'Something is rotten in the state of Denmark:' Why the Internet's advertising business model is broken [Facebook; Twitter; advertising business model; big data; platform economics]. *First Monday, 22*(7). https://doi.org/10.5210/fm.v22i7.7087

Jardine, E. (2019a). Online content moderation and the Dark Web: Policy responses to radicalizing hate speech and malicious content on the Darknet [Darknet; Darknet; Radicalization; Content Moderation]. *2019*, *24*(12). https://doi.org/10.5210/fm.v24i12.10266

Jardine, E. (2019b). The trouble with (supply-side) counts: the potential and limitations of counting sites, vendors or products as a metric for threat trends on the Dark Web. *Intelligence and National Security, 34*(1), 95–111. https://doi.org/10.1080/02684527.2018.1528752

Jardine, E., & Lindner, A. M. (2020). The Dark Web and cannabis use in the United States: Evidence from a big data research design. *International Journal of Drug Policy, 76*, 102627. https://doi.org/10.1016/j.drugpo.2019.102627

Jardine, E., Lindner, A. M., & Owenson, G. (2020). The potential harms of the Tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences, 117*(50), 31716–31721. https://doi.org/10.1073/pnas.2011893117

Kowalski, M., Hooker, C., & Barratt, M. J. (2019). Should we smoke it for you as well? An ethnographic analysis of a drug cryptomarket environment. *International Journal of Drug Policy, 73*, 245–254. https://doi.org/10.1016/j.drugpo.2019.03.011

Lecher, C. (2019). Feds take down dark web index and news site Deep Dot Web. *The Verge*. https://www.theverge.com/2019/5/7/18535731/fbi-dark-web-deep-dot-web-takedown-notice-arrests

Lorenzo-Dus, N., & Di Cristofaro, M. (2018). 'I know this whole market is based on the trust you put in me and I don't take that lightly': Trust, community and discourse in crypto-drug markets. *Discourse & Communication, 12*(6), 608–626. https://doi.org/10.1177/1750481318771429

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

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

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

Matthews, B., Collier, B., McVie, S., & Dibben, C. (2020). Understanding the geography of cryptomarkets using administrative data on postal drug deliveries in Scotland.

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). #Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy, 63*, 101–110. https://doi.org/10.1016/j.drugpo.2018.08.005

Mullin, J. (2015). The incredibly simple story of how the gov't Googled Ross Ulbricht. *Ars Technica*. https://arstechnica.com/tech-policy/2015/01/the-incredibly-simple-story-of-how-the-govt-googled-ross-ulbricht/

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

Norbutas, L., Ruiter, S., & Corten, R. (2020). Believe it when you see it: Dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs. *Social Networks, 63*, 150–161. https://doi.org/10.1016/j.socnet.2020.07.003

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

Ormsby, E. (2014). *Silk Road*. Macmillan Publishers Aus.

Owen, G., & Savage, N. (2015). The Tor Dark Net. *Global Commission on Internet Governance Paper Series*(20), 1-20. https://www.cigionline.org/sites/default/files/no20_0.pdf

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

Perdue, R. T., Hawdon, J., & Thames, K. M. (2018). Can Big Data Predict the Rise of Novel Drug Abuse? *Journal of Drug Issues, 48*(4), 508–518. https://doi.org/10.1177/0022042618772294

Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs. *European Sociological Review, 33*(6), 752–764. https://doi.org/10.1093/esr/jcx072

Reuter, P. (1986). *Disorganized crime: the economics of the visible hand*. The MIT Press.

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

Shortis, P., Aldridge, J., & Monica, J. (2020). Drug cryptomarket futures: structure, function and evolution in response to law enforcement actions. In *Research Handbook on International Drug Policy*. Edward Elgar Publishing.

Smith, R., & Frank, R. (2020). Dishing the Deets: How dark-web users teach each other about international drug shipments. Proceedings of the 53rd Hawaii International Conference on System Sciences,

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. 24th USENIX Security Symposium Washington, D.C.

United States. Department of Justice (2018). *First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More Than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million* https://www.justice.gov/opa/pr/first-nationwide-undercover-operation-targeting-darknet-vendors-results-arrests-more-35

United States. Department of Justice (2020). *International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Worldwide and the Seizure of Weapons, Drugs and over $6.5 Million* https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170

United States. Department of Justice. (2021). *DeepDotWeb Administrator Pleads Guilty to Money Laundering Conspiracy* https://www.justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy

United States. Drug Enforcement Agency (2018). *DEA, Dutch Law Enforcement Continue Attack On Dark Web Drug Sales* https://www.dea.gov/press-releases/2018/02/15/dea-dutch-law-enforcement-continue-attack-dark-web-drug-sales

United States. Federal Bureau of Investigation. (2020). Operation DisrupTor. https://www.fbi.gov/news/stories/operation-disruptor-jcode-shuts-down-darknet-drug-vendor-092220

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., & Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence, 173*, 159–162. https://doi.org/10.1016/j.drugalcdep.2017.01.004

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*(Supplement C), 16-23. https://doi.org/10.1016/j.drugpo.2016.07.004

Van Buskirk, J., Roxburgh, A., Bruno, R., & Burns, L. (2013). *Drugs and the Internet*. https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/DrugsTheInternet_Newsletter%20FINAL%20with%20ISSN.pdf

Van Buskirk, J., Roxburgh, A., Bruno, R., & Burns, L. (2014). *Drugs and the Internet*. https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/Drugs&TheInternet_Issue2.pdf

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. https://doi.org/10.1016/j.drugpo.2013.10.009

Van Wegberg, R., & Verburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. Proceedings of the Evolution of the Darknet Workshop,

Winstock, A.MJ, B, Maier, L., Aldridge, A., Zhuparris, A., Davies, E., Hughes, C., Johnson, M., Kowalski, M., & Ferris, J. (2019). *Global Drug Survey (GDS) 2019 Key Findings Report*. https://www.globaldrugsurvey.com/gds-2019/

York, N. N. (2011). Schumer Pushes to Shut Down Online Drug Marketplace. *NBC 4 New York*. https://www.nbcnewyork.com/news/local/schumer-calls-on-feds-to-shut-down-online-drug-marketplace/1920235/

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Eric Jardine is an assistant professor at Virginia Tech and a Senior Fellow at CIGI.