International Journal of Drug Policy 63 (2019) 113–121

Contents lists available at ScienceDirect

International Journal of Drug Policy

journal homepage: www.elsevier.com/locate/drugpo

Crime displacement in digital drug markets

Isak Ladegaard

Boston College, USA Isak Ladegaard, Department of Sociology, 410c McGuinn Hall, Boston College, 140 Commonwealth Avenue, Chestnut Hill, MA 02467-3807, USA

ARTICLE INFO

Keywords:
Crime displacement
Cybercrime
Crime control
Crime prevention
Hot spot policing
Cryptomarkets
Information and communication technology

ABSTRACT

Background Crackdowns on urban sites with concentrated criminal activity are sometimes followed by geographical relocation of crime. Is this also the case in cyberspace, where illegal websites and online networks can be wiped clean, but also quickly rebuilt and replaced on new servers and URLs?

Methods I address this question in three steps. First, I measure MDMA trade in a large digital market for drugs, before and after the arrest of a leading MDMA seller in the same market. Second, I count the number of available digital drug markets and vendor shops in the period February 2014–June 2018, to see if websites closed by police were replaced by new ones. Third, I track the digital movement and trading activities of individual drug sellers, before and after law enforcement shut down two large markets.

Results After police arrested a leading MDMA seller, other MDMA sellers filled most – but not all – of the gap. A major law enforcement crackdown reduced the number of available markets, but new ones were created, and market counts eventually surpassed the previous peak. When law enforcement shut down two big markets, many of the sellers relocated to other e-commerce sites and continued high-earning operations there.

Conclusion Arrests and market closures redirect digital drug trade to other sellers and markets. Hot spot policing in cyberspace might produce temporary results, but is arguably ineffective in the long run, as actors use information and communication technology's unique capacities to reorganize.

Introduction

When law enforcement cracks down on areas with clustered criminal activity, so-called 'hot spots', will crime simply go around the corner? Scholars suggest that geographically focused policing reduces crime in targeted areas, and that crime control benefits can diffuse into nearby surroundings, but at times, lawbreakers do shift to other areas (Braga, Papachristos, & Hureau, 2014; Eck, 1993; Guerette & Bowers, 2009; Hesseling, 1994; Telep, Weisburd, Gill, Vitter, & Teichman, 2014; Weisburd et al., 2006). Little is known of the post-intervention dynamics in non-urban domains (Johnson, Guerette, & Bowers, 2014), including cyberspace (for a notable exception, see Décary-Hétu & Giommoni, 2017). This lacuna warrants attention because crime's organizational logic might differ when activities are computer-mediated rather than bound by geography, due to the particular spatial-temporal characteristics of online interaction (Yar, 2005).

Silk Road (SR1) was among the first websites that brought digital reputation systems to trade of banned goods and services (Barratt, 2012; Christin, 2013; Martin, 2014; Hardy & Norgaard, 2016; Barratt & Aldridge, 2016). Scholars see SR1 as the first 'cryptomarket', a class of e-commerce websites that use sophisticated anonymization technology such as The Onion Router (Tor) to protect its customers and sellers (Barratt, 2012; Martin, 2014). As long as participants use the tools correctly it is difficult for law enforcement to connect illicit online activities to real-world identities (Van Hout & Bingham, 2013). Even the National Security Agency has failed to identify specific Tor users on demand (NSA, in The Guardian, 2013). Although law enforcement agencies shut down SR1 and its 'successor', Silk Road 2 (SR2), and have arrested numerous market users, available court documents and criminal complaints suggest that law enforcement's advances were based on traditional policework and there is to my knowledge no evidence that the encryption and anonymization technology at the core of all cryptomarkets has been cracked (Christin, 2014). Law enforcement have circumvented encrypted communication (Apuzzo, 2016) and bypassed Tor by exploiting vulnerabilities in misconfigured software (U.S. v. Ulbricht, 2014), but cryptomarket actors are astute consumers of security-related news and often discuss their practices, as when they review evidence put forth in court (Ladegaard, 2018a) and propose ideas for averting law enforcement raids (Ladegaard, 2017). At large, cryptomarket users are technologically competent, well informed, and feel able to assess the risks they face (Aldridge & Askew, 2017).

I study the digital movement of people and capital in cryptomarkets, following law enforcement interventions. I first measure the revenue of MDMA sellers in the cryptomarket Agora, before and after one of

E-mail address: isak.ladegaard@bc.edu.

https://doi.org/10.1016/j.drugpo.2018.09.013
Received 28 December 2017; Accepted 23 September 2018
0955-3959/

Agora's leading MDMA sellers was arrested. Next, I examine the number of available cryptomarkets and vendor shops (i.e. smaller cryptomarkets for individual sellers) after law enforcement brought down several such markets (Europol, 2014; FBI, 2014). Lastly, I trace capital flows and vendor relocation after the FBI shut down Silk Road (SR1), the first cryptomarket, in October 2013 (U.S. v. Ulbricht, 2015), and after a multinational law enforcement operation shut down its 'replacement,' Silk Road 2 (SR2), in November 2014.

Routine activities and crime displacement

Hot spot policing will sometimes be followed by increased incidents of crime in other areas (e.g. Cerezo, 2013; Braga et al., 2014; Constantinou, 2015), but diffusion of benefits also occur, and in the targeted areas, crime is often effectively reduced (Bowers, Johnson, Guerette, Summers, & Poynton, 2011; Braga et al., 2014; Eck, 1993; Guerette & Bowers, 2009; Johnson et al., 2014; Ratcliffe, 2005). The theoretical rationale as to why displacement may or may not happen draws on the routine activities perspective, which hypothesizes that 'criminal acts require the convergence in space and time of likely offenders, suitable targets and the absence of capable guardians' (Cohen & Felson, 1979: 588). These three central concepts maintain currency in crime research (Bennett, 1991; Sherman, Gartin, & Buerger, 1989), e.g. when scholars argue that repeat victimization is 'rational' to the offender, because detection and sanctioning were successfully evaded the first time (Farrell, Phillips, & Pease, 1995; Johnson et al., 2007; Bernasco, 2008). Instead of explaining criminal motivations, then, the routine activities perspective focuses on how lawbreaking involves practical challenges that can be tweaked. If the perceptive risks, rewards, and mere possibilities of lawbreaking are manipulated, then so is the individual would-be criminal's decision making, and in aggregate, the frequency of criminal activities (Clarke & Cornish, 1985; Clarke, 1983).

People remember routinely visited places and the paths between them (Brantingham & Brantingham, 1993, 1995). This cognitive mapping generates opportunities for lawbreaking because people have a keen awareness of what can be done in that particular environment. If people who want to purchase drugs find that their usual source has been arrested, crime might be reduced as they might decide to not buy anything at all, e.g. because doing so would require a long detour, or because they don't trust unknown sellers (Eck, 1993). However, arrests might also create opportunities for other would-be criminals (Barr & Pease, 1990). The buyer might ask peers (Coomber & Turnbull, 2007), or find sellers by searching for drug codes (e.g. '420' for cannabis) on publicly available websites such as Craigslist (Tofighi et al., 2016). The emergence of cryptomarkets has arguably made it even easier to locate new sources, as a large number of sellers are concentrated in a few e-commerce markets.

In the cryptomarket economy, buyers and sellers ('likely offenders') can review information about avenues they might relocate to ('suitable targets'). Their decisions are arguably better informed than in some cases of geographical relocation, which might require people to approach unknown buyers and sellers in unfamiliar city areas. For example, some sellers offer free drug samples to promote their services and products to new potential customers (Ladegaard, 2018b), and the e-commerce interface enable sellers to detail their rules of exchange (Bakken, Moeller, & Sandberg, 2017). However, cryptomarket trade is complex, and even experienced, well-informed users have to place their faith in expert systems, that is, systems that they are unlikely to fully understand (Giddens, 1996), such as Tor, encryption technology, and the back-end design of cryptomarkets. Informed cryptomarket actors know that law enforcement is actively trying to circumvent the technological barriers they depend on, and that police monitor their public discussions of collective problems (Ladegaard, 2017), activism (Maddox, Barratt, Allen, & Lenton, 2016; Munksgaard & Demant, 2016; Sotirakopoulos, 2017), and safety issues (Aldridge & Askew, 2017). In the words of an SR1 user: 'Do not let your guard down. Trust no one' (Aldridge & Askew, 2017, p.106). Actors are thus not operating in the absence of capable guardians, but rather in the presence of incapable guardians. Practically, it would be easy for motivated actors to shift their buying to other vendors, and to register at new cryptomarkets. In part due to information and communication technology's capacity to facilitate mass communication, but also because cryptomarkets and individual vendor pages are similarly structured. Considering both the challenges and capacities of digital drug trade, I expect to find some measure of crime displacement after law enforcement interventions in the cryptomarket economy.

Table 2
Change in weekly revenue for vendors who were active at least four weeks before and after the arrest of HollandOnline (excluding Christmas).

Vendor	Before	After	%
Vendor 1	12,036.46	15,172.32	+26.05
HollandOnline	11,786.72	0	−100
Vendor 2	4,939.38	2,679.64	−45.75
Vendor 3	4,192.36	933.07	−77.74
Vendor 4	2,137.43	8,932.30	+317.9
Vendor 5	1,900.6	2,316.89	+21.9
Vendor 6	1,860.41	1,468.56	−21.06
Vendor 7	1,599.77	2,227.72	+39.25
Vendor 8	1,582.96	1,530.83	−3.29
Vendor 9	891.22	127.25	−85.72
Vendor 10	431.77	990.73	+129.46
Vendor 11	412.07	302.67	−26.55
Vendor 12	367.14	304.5	−17.06
Vendor 13	316.98	1,967.7	+520.77
Vendor 14	208.82	243.15	+16.44
Vendor 15	197.35	195.85	−0.76
Vendor 16	61.47	438.28	+613
Vendor 17	44.93	296.88	+560.79
Vendor 18	30.03	66.85	122.63
Sum:	44,997.85	40,195.17	−10.67%
Sum, excl. HollandOnline:	33,211.13	40,195.17	+21.03%

Table 1
The combined revenue in Agora for Netherlands-based vendors of MDMA decreased significantly after the arrest of the top vendor, HollandOnline. Revenue increased for the same period in the European MDMA market and in the 'control group', that is, trade of other drugs in all regions.

	Netherlands MDMA (log)		Europe MDMA		All countries Non-MDMA	
ARIMA model	(0,0,0)(2,0,0)[7][a]		(1,0,0)(2,0,0)[7][a]		(1,0,0)(2,0,0)[7][a]	
Parameter	Estimate	SE	Estimate	SE	Estimate	SE
AfterArrest	−0.02	0.1	842.00	4170	10060.64	30198.89
Xmas	−0.62	0.13	−11136.72	5220.15	−38554.21	27493.35
MarketDownTime	−0.33	0.23	−15582.95	5897.22	−133363.98	19306.12
AR1	–	–	0.35	0.08	0.62	0.07
SAR1	0.16	0.08	0.25	0.08	0.38	0.08
SAR2	0.22	0.08	0.13	0.09	0.20	0.09
Box–Ljung (lag 14):	$X^2 = 11.53$	P = 0.64	12.57	0.56	8.6	0.86

[a] With non-zero mean, ARIMA: Autoregressive integrated moving average, Box-Ljung: Box-Ljung Q-test for residual autocorrelation.

Methods

I collected daily data from three cryptomarkets: SR2, Evolution, and Agora. The data were downloaded on a daily basis, from the original sources, in the period October 2014 – September 2015. The first two markets were terminated during the data collection period, while Agora lasted throughout. To establish whether SR1 vendors were actively trading in SR2, I also draw on archived data on SR1 vendors that I downloaded from a forum associated with SR2 in late 2013. I also collected archived data from the website DeepDotWeb, which manages a frequently updated list of available cryptomarkets and vendor shops.

Vendor revenue

A key measure of displacement in this study is the ability of individual vendors to generate income after law enforcement operations. To calculate vendor revenue, I collected original data from SR2, Evolution, and Agora with data mining programs written in Python. I downloaded all HTML files from the markets that contained feedback from customers. Because customers in these cryptomarkets were required to leave feedback for each purchase, I used the feedbacks as proxies for transactions, as others have done before me (e.g. Christin, 2013; Aldridge & Décary-Hétu, 2014). I extracted all data I wanted to analyze from the downloaded files (e.g. feedback from customers, vendor location, price per item). I subsequently matched historic Bitcoin–U.S. dollar exchange rates with the timestamps in the downloaded files, and calculated the median price for each item, for further analyses. Median was used instead of mean because vendors sometimes raised the price of sold out items to astronomical levels. I read through all items with a median price above $1000 and compared those that seemed spuriously high with prices per-gram in the literature (e.g. Collins, 2014), and removed if necessary. In some cases, I used the lowest price for the item instead of median price. I eliminated duplicates in the dataset based on item title, vendor name, item category, and feedback date. I gave all vendors mentioned in the study additional pseudonyms, except HollandOnline, whose activities have been detailed by Dutch police.

To examine how people and capital move between markets I compiled lists of vendors from various cryptomarkets, removed whitespace, made all letters lowercase, and examined overlapping vendor names. I then calculated the Jaro–Winkler distance between the more similar vendor names (where 1.0 is identical), and manually included or excluded those with a score larger than 0.9. In uncertain cases I looked up vendor identities using a vendor database available in Grams, a now defunct search engine for cryptomarkets (Soska & Christin, 2015). It is possible that some users pretended to be well-known vendors by operating under similar usernames, but this is unlikely as cryptomarket usernames are policed and attempts to mislead customers sanctioned.

Auto-regressive integrated moving average (ARIMA)

To examine crime displacement following the arrest of HollandOnline, a major MDMA vendor who operated in the Agora marketplace, I generated ARIMA models to measure trade revenue before and after the arrest. ARIMA models forecast time-series data as a linear combination of errors and past values. ARIMA models have been used to measure policy impacts on substance abuse (Kelly Garrett, 2006; Cunningham & Liu, 2003; Koski, Sirén, Vuori, & Poikolainen, 2007; Cunningham, Liu, & Muramoto, 2008), efforts to reduce crime (Chamlin, 1988), and crime trends (Tennenbaum & Fink, 1994). The method is considered quite powerful for assessing interventions (Cook, Campbell, & Day, 1979). I selected the model with minimal AICc values with auto.arima (Hyndman & Athanasopoulos, 2014; Hyndman & Khandakar, 2008), and examined the models for residual autocorrelation, using a Ljung-Box test.

I adjusted trade data for seasonality. Market trade was substantially reduced on Sundays – possibly because cryptomarket customers are likely to place their orders earlier in the week, in order to receive the products in time of the weekend. Analyses of sewages in 19 European cities have similarly suggested that illicit drug use spikes on Fridays and Saturdays (and early Sunday morning) (Thomas et al., 2012). To control for reduced trade due to technical problems, which are common in cryptomarkets (Soska & Christin, 2014) and indeed was a problem in Agora, I used data from DNStats.net, which tested the downtime status of the Agora market website 288 times a day, throughout my data collection period.

As one my goals was to measure how MDMA trade in the Netherlands was affected by the arrest of a major MDMA vendor in the same region, I created dummy variables for the periods before ('0') and after ('1') the arrest, and estimated whether trade continued as it had in the weeks before the event, or if the event was followed by a significant decrease or increase in trade. To create a visually intuitive measure how the arrest affected trade I compared forecasted post-interveual observations (McDowall, 1980; Dugan, 2010). For this analysis, the location of vendors were determined by the 'shipping from' section of their market profiles.

Market availability

Did law enforcement operations that shut down SR2 and several other markets permanently reduce the tally of available markets and vendor shops? To answer this question I collected data from the website DeepDotWeb, which has for several years managed a list of available cryptomarkets and vendor webshops. All archived versions of the site's list for the period February 2014 – June 2018 were downloaded from archive.org. This resulted in 57 unique lists, which had been revised a total of 702 times in the examined 53-month period. I extracted data from the lists, removed closed markets, deleted duplicates, and counted the number of available vendor shops and cryptomarkets for each list. To plot the number of available markets and shops over time, I used each list's timestamp (e.g. 'Last update: 5.8.18').

Findings

Crime displacement after the arrest of HollandOnline

The Netherlands-based vendor HollandOnline operated out of numerous cryptomarkets, including SR1, SR2, and Agora. In Agora, HollandOnline was among the top vendors for MDMA, with a weekly revenue of $11,800 from his MDMA sales. In the Netherlands he was only rivaled by one other MDMA vendor, who had a weekly revenue of $11,900; the rest of the pack were far behind. The 55-year-old man behind the HollandOnline moniker was arrested on December 16, 2014 (Openbaar Ministerie, 2015). Dutch police did not reveal the arrest of HollandOnline until March 2015, several months after the event, which means that customers could not know for sure why he disappeared from the market, and therefore, post-intervention change in trade cannot be directly attributed to criminal deterrence.

Dutch MDMA trade decreased after local police arrested HollandOnline (Fig. 1). That is, the combined revenue for all Dutch MDMA vendors declined, relative to the forecasted values, which trend in the data. Moreover, MDMA trade decreased in all of Europe, possibly in part due to the incapacitation of HollandOnline, who was among the continent's top ten MDMA sellers and listed on his profile that he shipped to 'EU'. However, the decreases in MDMA revenue in the Netherlands and Europe might also be due to the Christmas season that followed HollandOnline's arrest on December 16. To explore if trade that would be unaffected by the arrest decreased in the same period, I created a third subset of Agora trade, this one made up of trade in the entire Agora market for all countries and all drug categories except

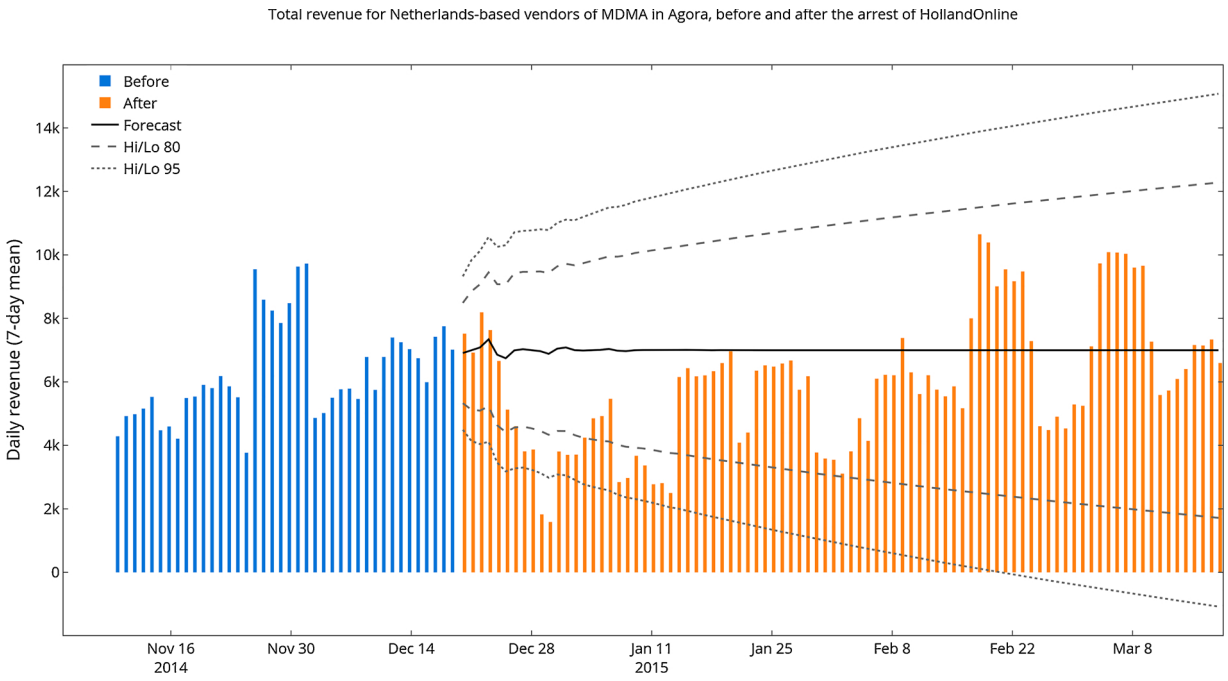


Fig. 1. Combined revenue from MDMA sales, for Netherlands-based vendors in Agora, before and after the arrest of HollandOnline.

MDMA. I found that trade decreased following the intervention in this population as well, which suggests that the Christmas season had an independent effect on Agora trade at large. At the very least, the data suggest that some other external factor reduced trade in the two-week period after the arrest, as there is no reason to expect that the overall trend in the market would be affected by the arrest. Sale of cannabis in Australia, for example, would presumably be unaffected by the absence of HollandOnline.

After the Christmas period, trade in the pseudo-control population increased significantly, relative to the forecast. European MDMA trade also increased. In the Dutch MDMA market, however, post-Christmas trade remained below the forecast. The combined revenue of all Netherlands-based MDMA vendors in the period December 20, 2014 to March 18, 2014 remained lower than the forecasted trade, after controlling for the Christmas period, seasonality, trend, and market instability (Table 1, Fig. 2).

When I examined Netherlands-based MDMA vendors who were active in the market at least four weeks before and after HollandOnline's arrest, excluding the Christmas period, I found that revenue decreased for nine vendors (incl. HollandOnline), and increased for ten. Overall trade in the Dutch MDMA market for these vendors decreased by nearly 11%, but the revenue for established vendors increased by as much as 21% (Table 2). HollandOnline's main competitor in terms of revenue, for example, increased weekly earnings in the four-week period after the arrest and Christmas by 26%, from $12,000 to about $15,200. Fig. 3, which includes data on all Netherlands-based MDMA vendors regardless of how many weeks they were active, show that trade after the arrest increased for some, and decreased for others. In sum, these findings suggest that the law enforcement operation that sought to reduce illegal trade by incapacitating HollandOnline was moderately successful, as overall trade was reduced, but at least some of HollandOnline's business was taken up by other Dutch MDMA vendors, and established MDMA vendors in particular. It is impossible to say if the observed changes in revenue were directly caused by the arrest, as a vendor's business might be affected by unknown external factors, but the evidence suggests that HollandOnline's absence created opportunities for other Dutch MDMA vendors.

Market availability after Operation Onymous (and operation bayonet)

On November 6, 2014, law enforcement in the United States and 16 European countries initiated 'Operation Onymous'. A central target was the SR2 marketplace, but several other cryptomarkets were also closed (Europol, 2014; FBI, 2014). The head of Europol's European Cybercrime Centre said the operation demonstrated that global law enforcement agencies 'are able to efficiently remove vital criminal infrastructures that are supporting serious organized crime'. A top FBI official added that they 'disrupt[ed] several websites dedicated to the buying and selling of illegal drugs and other unlawful goods [and will] continue to aggressively investigate, disrupt, and dismantle illicit networks' (Europol, 2014). U.S. Assistant Attorney General Leslie R. Caldwell said 'the global law enforcement community has innovated and collaborated to disrupt these dark market websites, no matter how sophisticated or far-flung they have become' (USAO, 2014).

The number of available cryptomarkets plummeted after Operation Onymous, from 19 to 12 (Fig. 4). It took a little more than six months for the number of available cryptomarkets to return to the same level as before Operation Onymous (19 markets in late October 2014; 22 markets in mid-May 2015). A new peak (25) was reached in March 2016, nearly one and a half years later. The number of individual vendor shops, which unlike most cryptomarkets are operated by vendors, was reduced from 5 to 3 following Operation Onymous.

I observed a similar reduction in the number of available cryptomarkets and vendor shops after Operation Bayonet in July 2017, in which American and Dutch law enforcement took down two large cryptomarkets, AlphaBay and Hansa. A comprehensive examination of the consequences of this particular intervention is beyond the scope of this study, but I note that the number of available cryptomarkets was reduced from 26 to 17, while the number of individual vendor shops was reduced from 20 to 16 (Fig. 4). In mid-June the following year, nearly 11 months later, the tally was the same for cryptomarkets, and down to 10 for vendor shops. That is, the number of markets and shops was still down about 50% compared to pre-Bayonet peaks of 30 and 24 markets and shops. If the numbers will climb to new highs 1–2 years after the crackdowns, as they did following Operation Onymous, remains to be seen.

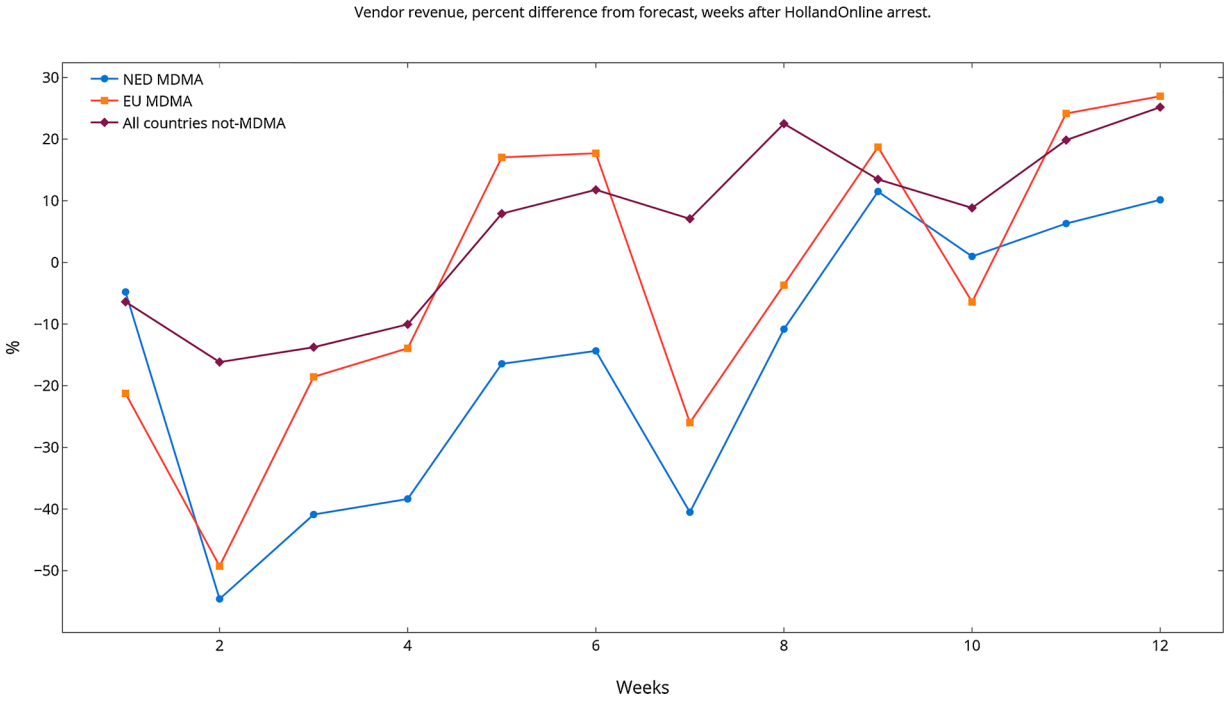


Fig. 2. Vendor revenue, percent deviation from forecasts, weeks after the arrest of HollandOnline. The pattern of MDMA trade in Europe and the Netherlands moves in tandem for most of the 12-week period after the arrest of HollandOnline, but Dutch vendor revenue is substantially more reduced, relative to their respective forecasts.

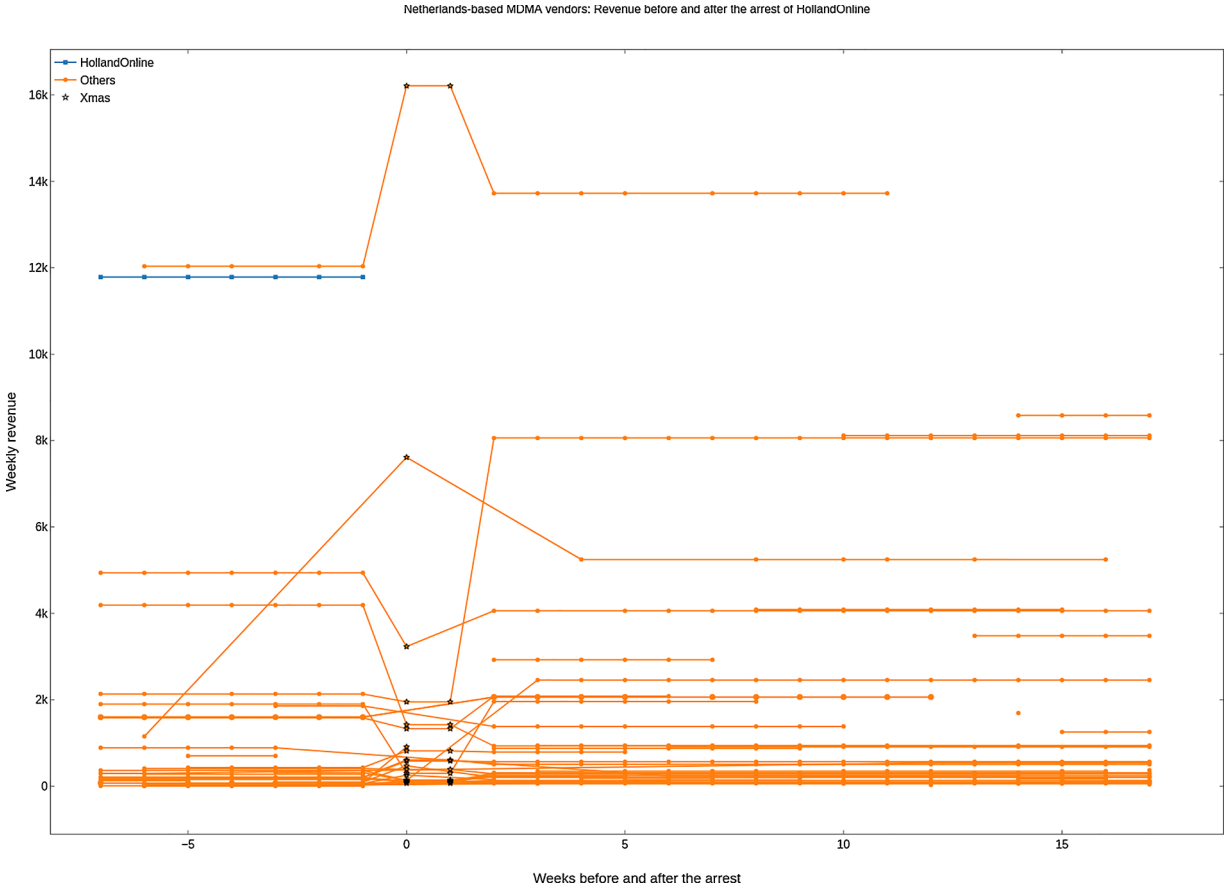


Fig. 3. Individual revenue for MDMA vendors based in the Netherlands, in Agora, seven weeks before the “intervention”, two weeks covering Christmas holidays, and the following seventeen weeks. To reduce noise in the illustration, weekly means for the three periods were used.

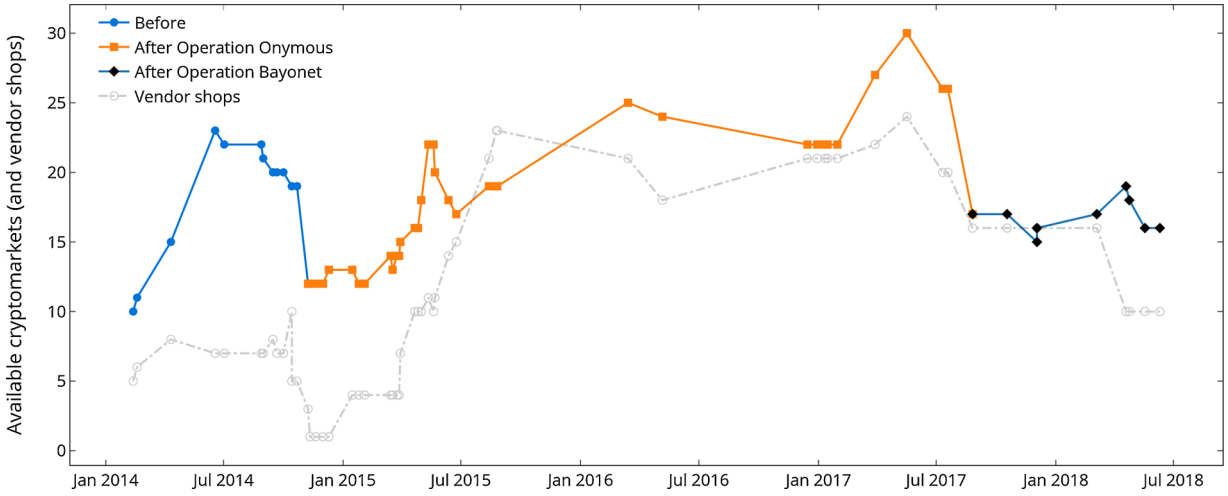


Fig. 4. Number of available cryptomarkets and vendor shops before and after two law enforcement operations.

Counts of available markets and shops say nothing about the economic activities within the sites, but they suggest that vendors and customers had multiple options, even after successful law enforcement interventions. The mean number of available cryptomarkets for the period February 2014-June 2018 was 18.14, which is a dramatic increase from the first months following the launch of SR1, when there was only one alternative market (Black Market Reloaded). Individual vendor shops have also multiplied since they first started to emerge in early 2014. The mean number of available vendor shops for the same period was 11.21. The absence of a clear upward or downward trend in the years since could suggest that the decentralization of the cryptomarket economy has plateaued.

Trade after the SR1 crackdown

The FBI shut down SR1 in October 2013. SR2, which opened the following month, became nearly as successful as its predecessor. In the period 19 October–6 November 2014, right up to the day SR2 was shut down, 573 vendors received a total of 28,600 feedbacks. Inferred from the feedbacks and the price of the items, the total revenue for all categories of trade in SR2 during these 19 days was $3.99 million. Excluding the last day of this period, which was cut in half due to the law enforcement operation that shut down the market, the mean per-day revenue for the period was $215,000, or $6.56 million per month. This figure exceeds the monthly revenue of SR1 in 2012, which was estimated to be $1.22 million (Christin, 2013), but not quite that of 2013, which was estimated to be $7.48 million (Aldridge & Décary-Hétu, 2014).

My data on SR2 vendors who were active in October and November 2014 goes all the way back to the market's first operational month in 2013. I find that eight of the top ten vendors in SR2 as of Oct/Nov 2014, had been in the market for more than 300 days, and the other two were not far behind, at 287 and 296 days. The pattern continues down the rank: a total of 307 SR2 vendors were active in the market for at least six months. That hundreds of vendor accounts were created in SR2 less than half a year after the FBI shut down SR1 suggests that there was at least some movement between the markets. And indeed, at least 84 former SR1 vendors had active, income-generating vendor accounts on SR2 nearly a full year after the FBI shut down the market, about 15% of all SR2 vendors at that time (Fig. 5). Their total combined revenue for the period November 28, 2013 – November 5, 2014 was $6.14 million. These findings confirms what Soska and Christin (2015) suggested, that vendors relocate after crackdowns, with individual-level data. My estimates of vendor relocation are highly conservative for at least two reasons. Firstly, established vendors might have elected to start over with new usernames after law enforcement seized SR1's servers. Secondly, many vendors might have been active for a period and then closed their businesses prior to my data collection, e.g. by choice or force, or they might have removed some product listings (and all feedback tied to those listings), e.g. because they stopped selling them.

Trade after the SR2 crackdown

Law enforcement shut down SR2 in November 2014, one year after it opened, and 13 months after the FBI shut down SR1. The largest alternative markets were Evolution and Agora (Van Buskirk, Roxburgh, Naicker, & Burns, 2015; Décary-Hétu, Paquet-Clouston, & Aldridge, 2016). I found that of the 672 vendors who were active in SR2 in October and/or November 2014, 298 continued to do business in Evolution, and 357 in Agora (Figs. 6 and 7). SR2 vendors in Evolution, for the period November 4, 2014 – March 17, 2015, earned $11.99 million, or $2.73 million per month. SR2 vendors in Agora, for the period November 4, 2014 – August 26, 2015, earned $27.88 million, or $2.9 million per month. In both markets, most of the revenue of SR2 vendors came from selling drugs (> 95%). Specifically, the lion's share of revenue for SR2 vendors in Agora and Evolution, respectively, came from selling MDMA (32% and 34%), stimulants (22% and 23%), cannabis (19% and 17%), psychedelics (9% and 7%), prescription drugs (8% and 7%), and opioids (3% and 5%). I found in sum compelling evidence of crime displacement following the law enforcement take-down of SR2. Hundreds of SR2 vendors continued to sell drugs in at least two other markets, earning millions of dollars.

Discussion

Law enforcement has arrested at least one hundred individual cryptomarket vendors since 2013 (Branwen, 2015). The arrest of HollandOnline, one of Netherland's largest MDMA vendors, reduced Agora trade of MDMA in the same region, relative to forecasted levels. This finding holds firm when compared to change in revenue for European MDMA vendors and non-MDMA trade in all countries, where trade *increased*. However, data on individual vendor revenue suggests that at least some of HollandOnline's business was replaced by other vendors, in line with the routine activities theory, which posits that crime will relocate if there are adequate opportunities to do so, and if risk is deemed sufficiently low.

Police have also shut down numerous cryptomarkets, presumably to reduce the number of options for potential buyers and sellers. I found that Operation Onymous successfully reduced the number of available cryptomarkets, in line with law enforcement reports. However,

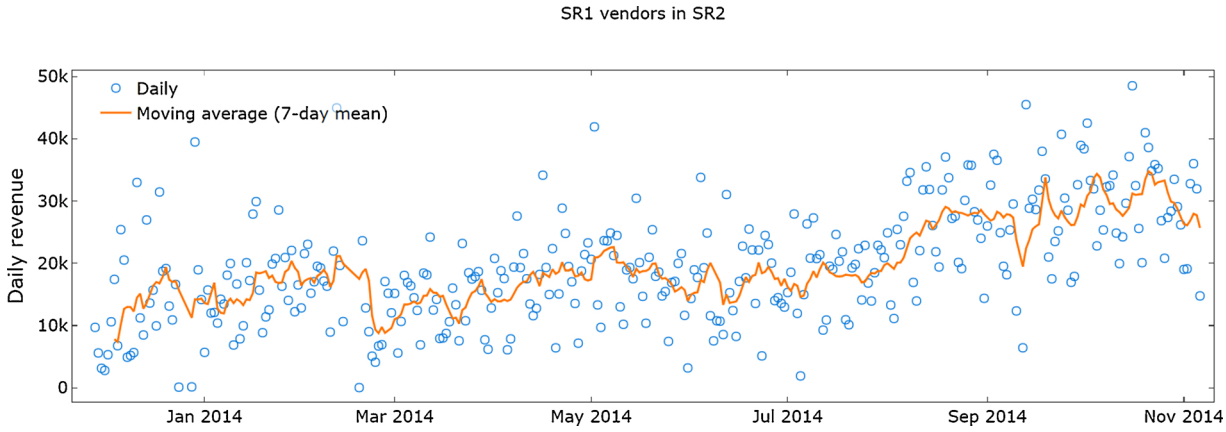
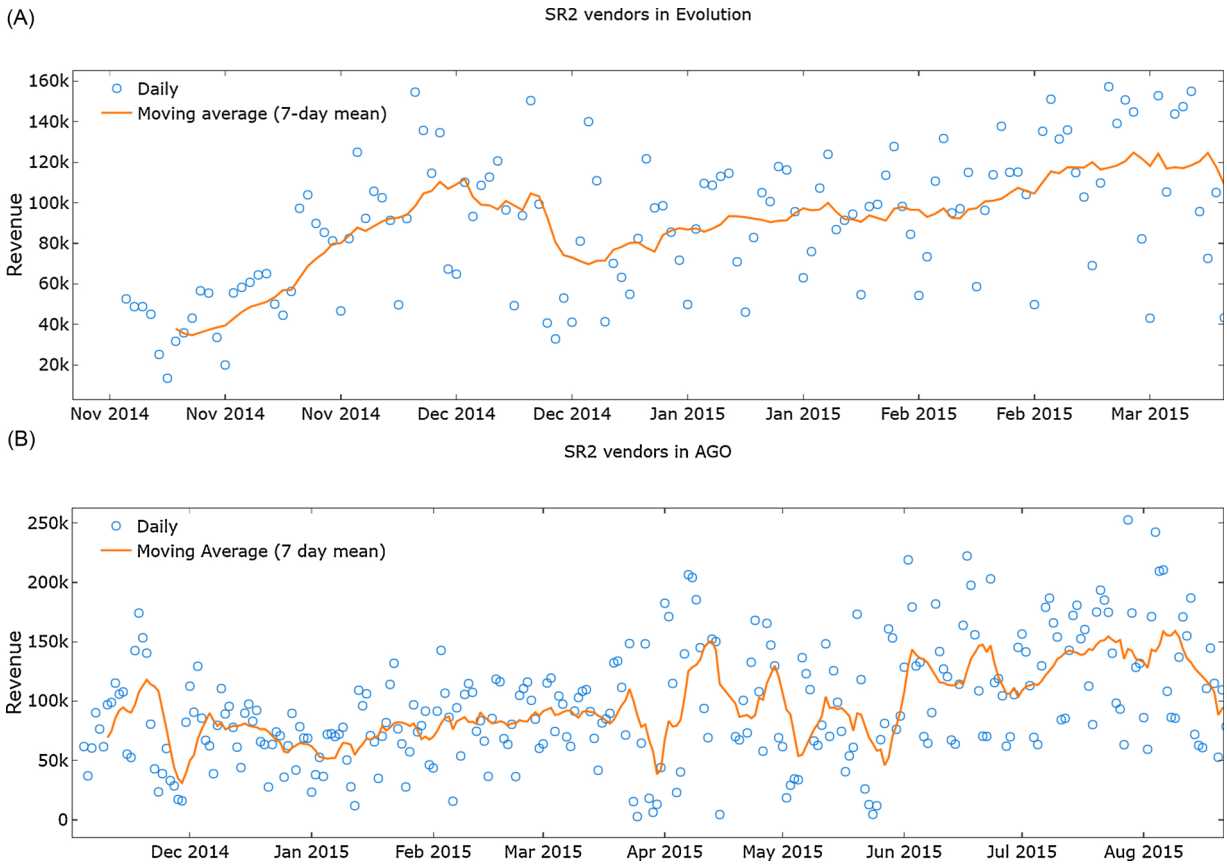


Fig. 5. Several SR1 vendors were active in SR2 for most of 2014. Note that vendors who deleted their accounts before the data collection in October and November 2014 are excluded from this chart. Despite this issue of missing data, it can be said that the mean revenue for all SR1 vendors in aggregate was at least $18,300 per day.

Europol's assertion that the operation closed 'upwards of 50 markets' seems exaggerated (Weiser & Carvajal, 2014). By my estimates, the number of available cryptomarkets was reduced from 19 to 12. (Vendor shops dropped from 5 to 3.) Moreover, the tally of available markets recovered to an above-mean level after about six months. These findings add to the discrepancies between figures reported by law enforcement and cryptomarket research. Following the crackdown on SR1, the FBI claimed that the market had facilitated trade worth more than $1.2 billion (Federal Bureau of Investigation, 2013), a figure which was highly inflated due to incorrect exchange rate calculations (Christin, 2014). Considering previous research on SR1 trade (Christin, 2013; Aldridge & Décary-Hétu, 2016), the real figure of the market's total revenue since its conception in 2011 is probably closer to $100 million, or about 8% percent of what was claimed by law enforcement. After the take-down of SR2, the FBI claimed that the market generated sales of 'at least approximately $8 million per month' (FBI, 2014). My own estimates suggest that the market's monthly revenue was $6.56 million.

Data on continuing trade after market closures suggests that vendors relocate to other markets (Décary-Hétu & Giommoni, 2017; Soska & Christin, 2015). However, I have found elsewhere that media attention – which typically surges after a market has been shut down – is also a



Figs. 6 and 7. Silk Road 2 vendors continued to trade for many months in at least two other markets in the cryptofield. The mean revenue for all SR2 vendors in Evolution (top), in aggregate, was $89,500 per day. In Agora (bottom), the daily mean was $95,000.

driver of market trade, presumably because new buyers and sellers are introduced to digital drug markets (Ladegaard 2018). To establish if vendors who are active pre-crackdown are responsible for post-crackdown trade, or if they are largely replaced by newcomers, it was therefore necessary to examine individual-level data. Décary-Hétu and Giommoni (2017) did this when they estimated that 8% of the vendors in seized markets registered in new markets, 12 weeks after Operation Onymous, but the present study is to my knowledge the first to quantify the scale of post-crackdown trade by relocated vendors, on an individual level, and in terms of revenue.

I found that at least 84 SR1 vendors had active vendor accounts on SR2 nearly a full year after SR1 was shut down, and of the 672 vendors who were active in SR2 in Oct/Nov 2014, 298 continued to do business in Evolution, and 357 in Agora. These findings contrast with Décary-Hétu and Giommoni (2017), who argued that 'the vast majority' of vendors on several cryptomarkets that were shut down by law enforcement 'did not displace to Agora and Evolution' (p. 69). The discrepancy between our findings might be due to the examined markets: Décary-Hétu and Giommoni (2017) collected data from Agora and Evolution, but also included Andromedia, Bluesky, Cloud-Nine, and Hydra. They covered in other words a larger share of the cryptomarket economy than I did. Another possible explanation is that Décary-Hétu and Giommoni (2017) relied upon secondary data, which collection had been 'irregular at best' (p. 62), but also covered a period that included several months before and after Operation Onymous. I collected my data directly from the markets on a daily basis over ten months, but most of that period was after Operation Onymous. However, our broad findings – which draw on different data sources and units of analyses – are in concert: law enforcement interventions in the cryptomarket economy might produce short-term results, but are largely ineffective in the long-term.

Concluding thoughts

Evidence of crime displacement suggest that cryptomarket trade is highly resilient to conventional crime control efforts. Cryptomarket actors embrace information and communication technology's capacity for group organization and communication, and have generated an enormous amount of data. They write product reviews (Hardy & Norgaard, 2016), discuss market practices (Ladegaard, 2018b; Martin, 2014), and partake in activism (Ladegaard, 2017; Maddox et al., 2016; Munksgaard & Demant, 2016; Sotirakopoulos, 2017). These data are a highly valuable resource for cryptomarket users, but also for law enforcement. The unique data-generating characteristic of cryptomarket trade may speed up innovation on both sides (Aldridge & Askew, 2017), as contesting efforts to protect and break organized anonymity (Bancroft & Scott Reid, 2017) continue in what surveillance researcher Marx (2003) calls an endless game of cat-and-mouse, between the watchers and the watched.

Law enforcement agencies that aim to reduce digital drug trade might have to amend their strategies. In early 2017, cryptomarket traffic was substantially reduced by continuous distributed denial of service (DDoS) attacks, which in simple terms overload websites and render them inaccessible. It is possible – but by no means certain – that the DDoS attacks were a carpet-bombing effort to reduce cryptomarket activity. If it was, it should be noted that the efficacy of DDoS attacks will most likely be temporary; DDoS-protection services continue to improve, as such attacks have become a common cyber security challenge for all kinds of websites. Even more recently, an innovative law enforcement approach to cryptomarket trade has been to exploit crime displacement. In June 2017, the Dutch National Police took control over the cryptomarket Hansa, and kept it online for nearly a month. When American law enforcement seized another major cryptomarket, Alphabay, many buyers and sellers relocated, and the Dutch police harvested intelligence on the 'refugees' who failed to properly encrypt their communications (Greenberg, 2018).

Shortly after taking control of the Hansa market, the Dutch police banned trade of the extremely potent chemical drug fentanyl. Other drugs were not banned because 'they would have taken place anyway … on a different market' (Greenberg, 2018). The fentanyl ban was a notable moment in cryptomarket policing, because it recognized that some forms of cryptomarket trade do more harm than others, and as such warrant different attention. The idea of banning particular products goes back to the first cryptomarket, SR1, which prohibited child pornography, weapons, and stolen bank card data (Zetter, 2013). The market Pandora similarly banned products and services that can 'harm people' (Martin, 2014), and the Hansa/police ban on fentanyl was preceded by a similar policy in the market Darknet Heroes League, which was announced in 2016: 'due to recent deaths and the threat to customers' well-being … we will no longer allow the sale of fentanyl and its related analogues on our market'. While cryptomarket users discuss security issues (Aldridge & Askew, 2017; Ladegaard, 2018a), they also debate harm reduction (Van Hout & Bingham, 2014; Buxton and Bingham 2015) and morality (Maddox et al., 2016; Martin, 2014), and policing efforts might be more successful in the long run if they recognize the multifaceted characteristics of their targets. Buxton and Bingham (2015) suggest that cryptomarket users might reject markets that sell particularly harmful products, e.g. weapons, but evidence suggests that they will not, if there are few reliable options. The market Evolution, which many SR2 vendors relocated to, sold a wide range of harmful products, including firearms, stolen credit card data, and, like most markets, fentanyl. However, while cryptomarket actors are arguably most concerned about security and reliability, Buxton and Bingham (2015) are right to stress that actors also make normative judgements that a more nuanced law enforcement strategy would recognize. Law enforcement could state that while all forms of banned trade are inevitable policing targets, markets that facilitate trade of the most dangerous substances and services will be prioritized. When cryptomarket actors relocate their activities, as evidence suggests they will, they might opt for markets that shun fentanyl and other dangerous products and services, due to both security and moral concerns. This in turn may shift the flow of people and capital away from markets that facilitate the most destructive trade, and ultimately reduce harm.

Funding

This work was supported by the National Science Foundation [#1702919].

References

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. *The International Journal on Drug Policy*.
Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *The International Journal on Drug Policy, 41*, 101–109.
Apuzzo, M. (2016). *F.B.I. Used Hacking Software Decade Before IPhone Fight.* The New York Times. The New York Times 13 Apr. 2016. Web. 20 Jul.
Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: The case of cryptomarket users. *Information, Communication & Society, 20*(4), 497–512.
Bakken, S. A., Moeller, K., & Sandberg, S. (2017). Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminologyt* 1477370817749177.
Barr, R., & Pease, K. (1990). Crime placement, displacement, and deflection. *Crime and Justice,* 277–318.
Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction, 107*(3) 683-683.
Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets*(* but were afraid to ask). *The International Journal on Drug Policy, 35*, 1–6.
Bennett, R. R. (1991). Routine activities: A cross-national assessment of a criminological perspective. *Social Forces, 70*(1), 147–163.
Bernasco, W. (2008). Them again? Same-offender involvement in repeat and near repeat burglaries. *European Journal of Criminology, 5*(4), 411–431.
Bowers, K. J., Johnson, S. D., Guerette, R. T., Summers, L., & Poynton, S. (2011). Spatial displacement and diffusion of benefits among geographically focused policing initiatives: A meta-analytical review. *Journal of Experimental Criminology, 7*(4),

347–374.
Braga, A. A., Papachristos, A. V., & Hureau, D. M. (2014). The effects of hot spots policing on crime: An updated systematic review and meta-analysis. *Justice Quarterly, 31*(4), 633–663.
Brantingham, P. L., & Brantingham, P. J. (1993). Nodes, paths and edges: Considerations on the complexity of crime and the physical environment. *Journal of Environmental Psychology, 13*(1), 3–28.
Brantingham, P., & Brantingham, P. (1995). Criminality of place. *European Journal on Criminal Policy and Research, 3*(3), 5–26.
Branwen, G. (2015). *'Tor DNM-related arrests.' N.p.* Web. 04 May 2017.
Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy Brief, 7*.
Cerezo, A. (2013). CCTV and crime displacement: A quasi-experimental evaluation. *European Journal of Criminology, 10*(2), 222–236.
Chamlin, M. B. (1988). Crime and arrests: An autoregressive integrated moving average (ARIMA) approach. *Journal of Quantitative Criminology, 4*(3), 247–258.
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,* 213–224.
Christin, N. (2014). Commentary on Barratt et al. (2014): Steps towards characterizing online anonymous drug marketplace customers. *Addiction, 109*(5), 784–785.
Constantinou, A. (2015). Is crime displacement inevitable? Lessons from the enforcement of laws against prostitution-related human trafficking in Cyprus. *European Journal of Criminology* 1477370815617190.
Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review,* 588–608.
Cook, T. D., Campbell, D. T., & Day, A. (1979). *Quasi-experimentation: Design & analysis issues for field settings, Vol. 351*. Boston: Houghton Mifflin.
Collins, J. (2014). *Ending the drug wars: Report of the LSE expert group on the economics of drug policy*.
Coomber, R., & Turnbull, P. (2007). Arenas of drug transactions: adolescent cannabis transactions in England—social supply. *Journal of Drug Issues, 37*(4), 845–865.
Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice,* 147–185.
Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and Justice,* 225–256.
Cunningham, J. K., & Liu, L. M. (2003). Impacts of federal ephedrine and pseudoephedrine regulations on methamphetamine-related hospital admissions. *Addiction, 98*(9), 1229–1237.
Cunningham, J. K., Liu, L. M., & Muramoto, M. (2008). Methamphetamine suppression and route of administration: Precursor regulation impacts on snorting, smoking, swallowing and injecting. *Addiction, 103*(7), 1174–1186.
Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going International? Risk Taking by Cryptomarket Drug Vendors. *The International Journal on Drug Policy*.
Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law, and Social Change, 67*(1), 55–75.
Dugan, L. (2010). *Estimating effects over time for single and multiple units. Handbook of quantitative criminology*741–763.
Eck, J. E. (1993). *The threat of crime displacement. Criminal justice abstracts, Vol. 25*, 527–546 No. 3.
Europol (2014). *Global ACTION Against DARK markets on TOR NETWORK.* Web. 17 Feb. 2016.
FBI (2014). *'Dozens of online 'Dark markets' seized pursuant to forfeiture complaint filed in manhattan federal court in conjunction with the arrest of the operator of silk road 2.0.* FBI FBI, 07 Nov, Web. 05 May 2017.
Federal Bureau of Investigation (2013). *Criminal complaint: Ross William Ulbricht a/k/a dread pirate roberts, DPR, Silk Road.* Available at: https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf (accessed 13 March 2014); archived at http://www.webcitation.org/6LWf6foGa.
Farrell, G., Phillips, C., & Pease, K. (1995). Like taking candy: why does repeat victimization occur? *The British Journal of Criminology,* 384–399.
Giddens, A. (1996). *The consequences of modernity.* Polity Press.
Greenberg, A. (2018). *Operation Bayonet: Inside the Sting that Hijacked and Entire Dark Web Drug Market.* Wired.
Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention evaluations. *Criminology, 47*(4), 1331–1368.
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*(03), 515–539.
Hesseling, R. (1994). Displacement: A review of the empirical literature. *Crime Prevention Studies, 3*(1), 97–230.
Hyndman, R. J., & Athanasopoulos, G. (2014). Forecasting: Principles and practice. *OTexts.*.
Hyndman, R. J., & Khandakar, Y. (2008). Automatic time series forecasting : the forecast package for R. *Journal of Statistical Software, 26*(3), 1–22.
Johnson, S. D., Bernasco, W., Bowers, K. J., Elffers, H., Ratcliffe, J., Rengert, G., et al. (2007). Space–Time patterns of risk: A cross national assessment of residential burglary victimization. *Journal of Quantitative Criminology, 23*(3), 201–219.
Johnson, S. D., Guerette, R. T., & Bowers, K. (2014). Crime displacement: What we know, what we don't know, and what it means for crime reduction. *Journal of Experimental Criminology, 10*(4), 549–571.
Kelly Garrett, R. (2006). Protest in an information society: A review of literature on social movements and new ICTs. *Information, Communication and Society, 9*(02), 202–224.
Koski, A., Sirén, R., Vuori, E., & Poikolainen, K. (2007). Alcohol tax cuts and increase in alcohol-positive sudden deaths—A time-series intervention analysis. *Addiction, 102*(3), 362–368.
Ladegaard, I. (2017). "I pray that we will find a way to carry on this dream": How a law enforcement crackdown united an online community. *Critical Sociology* 0896920517735670.
Ladegaard, I. (2018a). We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *The British Journal of Criminology, 58*(2), 414–433.
Ladegaard, I. (2018b). 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.
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 and Society, 19*(1), 111–126.
Martin, J. (2014). *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs.* Springer.
Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.
McDowall, D. (1980). *Interrupted time series analysis.* .
Munksgaard, R., & Demant, J. (2016). Mixing politics and crime–The prevalence and decline of political discourse on the cryptomarket. *The International Journal on Drug Policy, 35*, 77–83.
Openbaar Ministerie (2015). *Aanhoudingen voor grootschalige drugshandel op ondergrondse marktplaatsen* Web. Mar. 2016.
Ratcliffe, J. H. (2005). Detecting spatial movement of intra-region crime patterns over time. *Journal of Quantitative Criminology, 21*(1), 103–123.
Sherman, L. W., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology, 27*(1), 27–56.
Soska, K., & Christin, N. (2015). *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. USENIX Security Symposium*33–48.
Sotirakopoulos, N. (2017). Cryptomarkets as a libertarian counter-conduct of resistance. *European Journal of Social Theory* 1368431017718534.
Telep, C. W., Weisburd, D., Gill, C. E., Vitter, Z., & Teichman, D. (2014). Displacement of crime and diffusion of crime control benefits in large-scale geographic areas: A systematic review. *Journal of Experimental Criminology, 10*(4), 515–548.
Tennenbaum, A. N., & Fink, E. L. (1994). Temporal regularities in homicide: Cycles, seasons, and autoregression. *Journal of Quantitative Criminology, 10*(4), 317–342.
The Guardian (2013). *'Tor stinks' presentation.* Web. 18 Oct. 2013.
Thomas, K. V., Bijlsma, L., Castiglioni, S., Covaci, A., Emke, E., Grabic, R., et al. (2012). Comparing illicit drug use in 19 european cities through sewage analysis. *The Science of the Total Environment, 432*, 432–439.
United States of America v. Ross William Ulbricht, Defendant. Case 1:14-cv-08812-UA Document 3. Southern District of New York. 2015. Print.
United States of America v. Ross William Ulbricht, Defendant. Southern District of New York. 2015. S1 14 Cr. 68 (KBF). Document 57. Print. 2014.
USAO (2014). *U.S. attorney's office.' U.S. attorney's office.' U.S. Department of justice. Southern district of new york.* 7 Nov., Web. 03 May 2017.
Van Buskirk, J., Roxburgh, A., Naicker, S., & Burns, L. (2015). A response to Dolliver's' Evaluating drug trafficking on the Tor network'. *The International Journal on Drug Policy, 26*(11), 1126–1127.
Van Hout, M. C., & Bingham, T. (2013). Surfing the Silk Road': A study of users' experiences. *The International Journal on Drug Policy, 24*(6), 524–529.
Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *The International Journal on Drug Policy, 25*(2), 183–189.
Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology, 44*(3), 549–592.
Weiser, B., & Carvajal, D. (2014). *'International raids target sites selling contraband on the 'Dark web'.* The New York Times N.p., 7 Nov, Web. 22 Feb. 2016.
Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.
Zetter, K. (2013). Feds Arrest Alleged' Dread Pirate Roberts,' the brain behind the silk road drug site. *Wired, Conde Nast, 2*(October)www.wired.com/2013/10/silk-road-raided/.