Drug and Alcohol Dependence 173 (2017) 159–162

Contents lists available at ScienceDirect

Drug and Alcohol Dependence

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

Short communication

The recovery of online drug markets following law enforcement and other disruptions

Joe Van Buskirk[a,*], Raimondo Bruno[b], Timothy Dobbins[a], Courtney Breen[a], Lucinda Burns[a], Sundresan Naicker[a], Amanda Roxburgh[a]

[a] National Drug and Alcohol Research Centre (NDARC), University of New South Wales, Sydney, New South Wales, 2052, Australia
[b] University of Tasmania, School of Medicine, Hobart, Tasmania, 7000, Australia

ARTICLE INFO

Article history:
Received 13 September 2016
Received in revised form
16 December 2016
Accepted 2 January 2017
Available online 20 February 2017

Keywords:
Online drug markets
Cryptomarkets
Darknet
Illicit drug trade
New drug markets
Law enforcement

ABSTRACT

Introduction: Online drug markets operating on the 'darknet' ('cryptomarkets') facilitate the trade of illicit substances at an international level. The present study assessed the longitudinal impact on cryptomarket trading of two major disruptions: a large international law enforcement operation, 'Operation Onymous'; and the closure of the largest cryptomarket, Evolution.
Methods: Almost 1150 weekly snapshots of a total of 39 cryptomarkets were collected between October 2013 and November 2015. Data were collapsed by month and the number of unique vendor aliases operating across markets was assessed using interrupted time series regression.
Results: Following both Operation Onymous and the closure of Evolution, significant drops of 627 ($p = 0.014$) and 910 vendors ($p < 0.001$) were observed, respectively. However, neither disruption significantly affected the rate at which vendor numbers increased overall.
Conclusions: Operation Onymous and the closure of Evolution were associated with considerable, though temporary, reductions in the number of vendors operating across cryptomarkets. Vendor numbers, however, recovered at a constant rate. While these disruptions likely impacted cryptomarket trading at the time, these markets appear resilient to disruption long-term.

1. Introduction

The rise of 'dark net' drug markets, known as cryptomarkets, has led to the development of new methods of distribution of illicit and emerging substances (Schifano et al., 2006; Walsh, 2011; Wax, 2002). Cryptomarkets are accessible only through anonymising servers, with incoming connections stripped of identifiable information (Barratt, 2012). This allows members to sell and source drugs online with greater anonymity, and reduced risk of detection and prosecution (Martin, 2014b). While the technical aspects of cryptomarkets have been discussed in great detail elsewhere (Martin, 2014a), these markets operate in a similar way to other online markets, in which vendors are reliant upon consumer feedback to build and maintain reputation (Cox, 2016). Since cryptomarkets reached public awareness in 2011 (Chen, 2011), they have become well-established sources for purchasing and selling substances at an international level (Martin, 2014a).

1.1. Challenges of cryptomarkets

Cryptomarkets present a formidable challenge to law enforcement agencies tasked with interrupting drug supply networks (Reitano et al., 2015). In addition, cryptomarkets present an opportunity for marketplace moderators to defraud consumers, with little avenue for recourse or recovery of money (Tzanetakis et al., 2016).

1.2. Disruptions to cryptomarket operation

The seizure of the original Silk Road, the first cryptomarket to attract international attention, in October 2013 by the American Federal Bureau of Investigation (FBI), came after many months of intensive surveillance (Soska and Christin, 2015). This represented the first major disruption to cryptomarket operation, and was followed by a proliferation of alternative cryptomarkets including Silk Road 2.0 (Van Buskirk et al., 2014). The second major disruption came in November 2014 in the form of an international law-enforcement collaboration between the FBI, Department of Homeland Security, Europol, and other security agencies, dubbed 'Operation Onymous', and resulted in the seizure of multiple cryp-

* Corresponding author.
E-mail address: j.vanbuskirk@unsw.edu.au (J. Van Buskirk).

http://dx.doi.org/10.1016/j.drugalcdep.2017.01.004
0376-8716/

tomarkets and many arrests worldwide (Barratt and Aldridge, 2016). The third major disruption was the closure of the Evolution marketplace in March 2015. The market closed suddenly, with the moderator/s removing approximately 12 million dollars in customer funds that were stored on the marketplace (Tzanetakis et al., 2016). This type of fraud is known among dark net communities as an 'exit scam' (Tzanetakis et al., 2016). Evolution was the largest marketplace at the time of closure and its closure marked the beginning of a period of instability across cryptomarkets. During this time considerable downtime was observed, in which markets were offline and inaccessible (Van Buskirk et al., 2015).

1.3. Monitoring to date and aims of current paper

Cryptomarket analysis has revealed steady growth in both the number of markets and the numbers of vendors operating on them (Soska and Christin, 2015; Van Buskirk et al., 2015). Existing research (Soska and Christin, 2015) suggests that cryptomarkets recover relatively quickly from disruption. The current work aims to extend these studies by statistically assessing the rate at which vendor numbers recover from disruptions, and the impact disruptions have on this rate.

2. Method

2.1. Data collection

Cryptomarkets were included in the data collection if they had at least 100 current active substance listings, greater than one active seller offering these listings, and were English speaking or offered English translations. Between October 2013 and November 2015, all eligible cryptomarkets were accessed weekly with local copies of every page within the 'drugs' parent category opened manually and saved. This manual data collection allowed for visual verification that all pages were completely loaded and valid, thus bypassing many potential pitfalls of automated collection, leading to incomplete or misleading data (Munksgaard et al., 2016). Multiple attempts were made to access any markets experiencing downtime and, if complete snapshots could not be collected, data from that time point was excluded and treated as missing. Only complete snapshots were included in the analysis.

Listing data were extracted from saved webpages using a Visual Basic for Applications (VBA) macro in Excel 2010 that parsed and collated raw html data into a database detailing date of collection, listing description, vendor name and the name of the cryptomarket from which it was extracted. Listing descriptions were analysed using the vector form 'lookup' function in Excel 2010, based on keyword identification; to verify listings related to a substance; with any non-substance listing excluded. Greater detail of data collection methods is provided elsewhere (Van Buskirk et al., 2016).

Overall, 39 cryptomarkets were monitored for a median of 27 weeks each (range 2–79). Of 1149 possible weekly cryptomarket snapshots, 917 (79.8%) were successfully captured. As unique vendor aliases for each time point were to be summed, the missing 20.2% time point data posed a problem for a reliable estimation of the rate of increase over time. As such, cleaned vendor numbers were summed across markets for each weekly time point, with this number averaged by month, thereby crudely imputing missing values. This resulted in 304 monthly data points across all markets, with only 11 missing data points (3.6%).

2.2. Data analysis

For each listing, a vendor alias is listed. As vendors may operate over multiple marketplaces, as well as within the same market under different aliases, aliases were cleaned to control for duplication. To do this, raw vendor aliases were stripped of any ASCII characters that were not letters or numbers, including spaces. Secondly, common suffixes such as numbers, cryptomarket names, and substance types, were removed and assessed for duplication. Finally, any common word or letter prefixes were removed (such as 'the' or 'the real'), and duplicates were again assessed. Duplicate assessment was conservative, with any duplicates containing common words (e.g., 'drugs' and 'therealdrugs'; or 'weeddealer' and 'dealer') retained as separate vendors.

As a result of this procedure, 23,783 vendor aliases were reduced to 11,335 aliases (a 52.3% reduction). Soska and Christin (2015) were able to reduce 29,258 aliases to 9386 (a 67.9% reduction) using similar methodology in addition to PGP ('pretty good privacy') key verification (unique, public 'keys' employed by users for text encryption) and the vendor search feature of the Grams website (a darknet search engine that may be used to search for products across active cryptomarkets). These latter two methods were unavailable as PGP keys were not collected across the monitoring period, meaning verification could not be performed retrospectively. However, they found that approximately 25% of vendor aliases were actually duplicate vendors operating with different aliases, with this proportion mostly stable after March 2014. As such, the extent to which vendor numbers are inflated due to duplicate vendors appears consistent across time points.

Once cleaning of vendor names was completed, the raw (i.e., uncleaned) number of vendors was compared with cleaned numbers at each time point. This revealed an average of 75.6% raw vendor aliases that were unique at each time point, with a standard deviation of 5.9%, and a roughly normal distribution of percentage values. This would appear to corroborate findings from Soska and Christin (2015) that the proportion of duplicate vendors, and hence the adjustment applied by the cleaning method at each time point, was largely constant over the monitoring period.

Data were placed into three distinct time periods: (1) October 2013 to November 2014, following the seizure of the original Silk Road and leading up to Operation Onymous; (2) December 2014 to March 2015, following Operation Onymous and leading up to the Evolution exit scam; and (3) April 2015 to November 2015, post-Evolution exit scam. The number of unique vendors across markets was then analysed using an interrupted time series regression analysis. The approach described in Wagner et al. (2002) was used, which is based on a standard linear regression model regressing the number of vendors on time. Two variables were added for each disruption, one representing an absolute change in vendor numbers (level change) and one representing a change in slope (trend change). The assumption of independence of the linear regression model was assessed using the Durbin-Watson statistic, and residual plots were examined to assess normality. All statistical analysis was performed using Stata v13.1 (StataCorp., 2013).

3. Results

3.1. Interrupted time series regression

The beginning of both periods saw a significant drop in vendor numbers, with 627 fewer vendors at the beginning of period two and 910 fewer vendors at the beginning of period three. There was no evidence of a change in the rate of increase in vendor numbers between the first and the second and between the second and third periods. The Durbin-Watson d-statistic for auto-correlation for this final model was 1.93, indicating negligible auto-correlation in the model, and the model explained 88.0% of the variability in vendor numbers. Output from the regression is outlined in Table 1, with

Table 1
Output for interrupted time series regression analysis assessing overall vendor numbers.

Variable	Regression Coefficient (95% CI)	Standard Error	*t*	*p*
Baseline trend	120.5 (96.1 to 144.9)	11.68	10.32	<0.001
Level change - Period 2	−626.9 (−1114.0 to −139.9)	233.48	−2.69	0.014
Trend change - Period 2	−78.5 (−244.6 to 87.6)	79.63	−0.99	0.336
Level change - Period 3	−910.0 (−1330.0 to −489.9)	201.37	−4.52	<0.001
Trend change - Period 3	113.7 (−60.1 to 287.5)	83.33	1.36	0.188
Intercept	565.5 (358.1 to 772.9)	99.43	5.69	<0.001

Monitoring began in October 2013 (the closure of the original Silk Road); Period 2 denotes the time between Operation Onymous and the Evolution exit scam (November 2014 to March 2015); Period 3 denotes the time post-Evolution exit scam to the end of the monitoring period (April 2015 to November 2015).

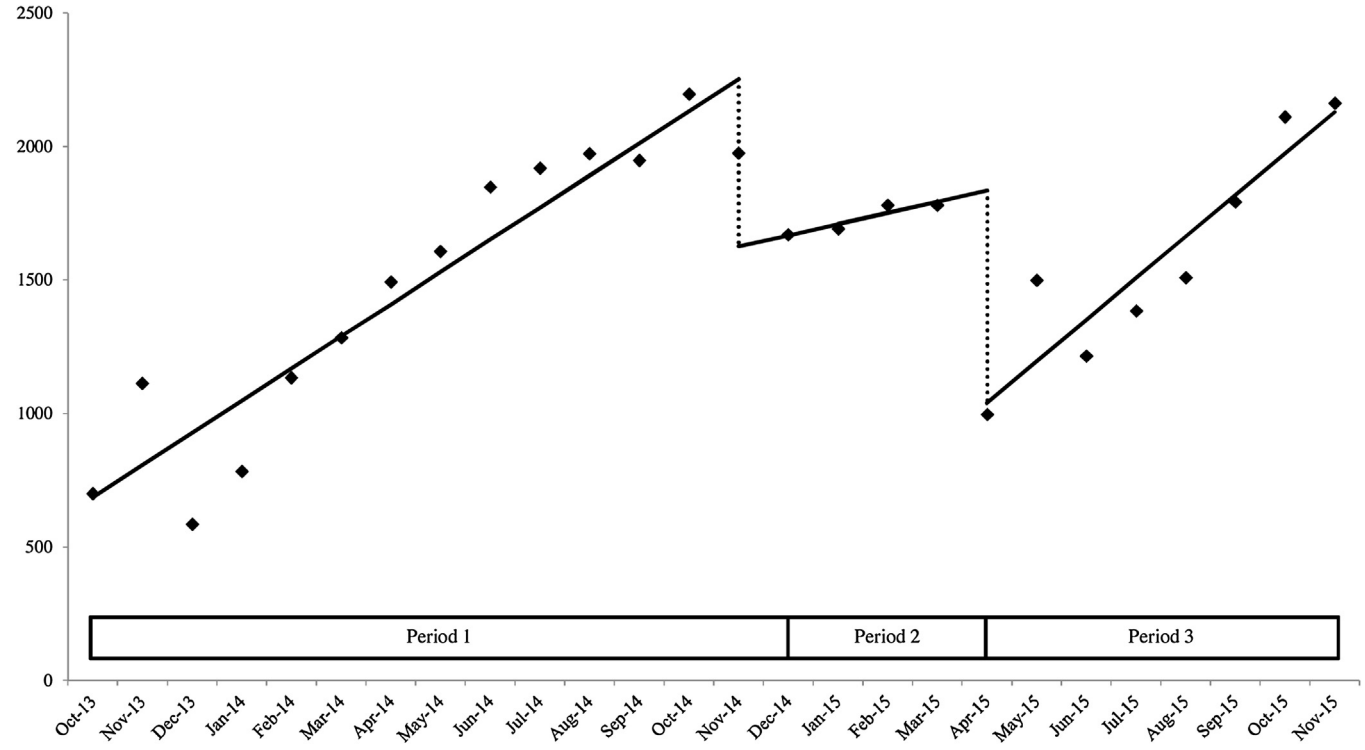

Fig. 1. Average number of unique vendor aliases by month over all monitored cryptomarkets with regression model prediction overlain and time periods marked.
Note: Period 1 denotes the time between the beginning of monitoring in October 2013 (the closure of the original Silk Road) and Operation Onymous; Period 2 denotes the time between Operation Onymous and the Evolution exit scam (November 2014 to March 2015); Period 3 denotes the time post-Evolution exit scam to the end of the monitoring period (April 2015 to November 2015).

predicted values and individual observations outlined graphically in Fig. 1.

3.2. Specificity analysis

A second analysis was conducted on the raw number of vendors operating across monitored cryptomarkets (that is, the number of vendors before cleaning for duplicates). All covariates that reached statistical significance in the first model all reached significance, and the model explained 86.5% of the variability associated with (uncleaned) vendor numbers (results not shown). This further suggests a constant rate of duplicate vendor operation across monitored markets and time points.

4. Discussion

Despite major disruptions such as Operation Onymous and the Evolution exit scam, the rate of increase in vendor numbers operating across cryptomarkets was constant across the monitoring period. That is, disruptions were associated with temporary, significant reductions in overall vendor numbers at the time, with numbers recovering at a consistent rate. However, as of November 2015, the overall number of vendors had not returned to the level seen in November 2014, just prior to Operation Onymous. This would suggest that disruptions may indeed have substantial effects on cryptomarket operation provided they happen in quick succession of one another, reducing the capacity for markets to recover.

Cryptomarkets may thus be affected by disruptions in a similar way to other illegal online services, such as file sharing platforms. That is, disruptions are associated with an overall drop in usage across platforms at the time, before consumers find alternative platforms on which to resume activity (Peukert et al., 2016). While previous research has suggested that disruptions to illegal file sharing platforms may cause consumers to migrate to legal platforms (Danaher et al., 2015), this is largely not an option with cryptomarkets. It is, however, possible that vendors on cryptomarkets may resort to street markets for selling illicit substances following disruptions, and the extent of such migration represents an avenue for future research.

4.1. Limitations

The actual numbers in the analysis likely do not represent the absolute number of unique vendors operating across cryptomar-

kets. The method of duplication assessment applied was superficial, and ignores any duplicate vendors operating with different aliases. While Soska and Christin (2015) have demonstrated that this is common, it also appeared constant over time, and thus estimates in the present study are likely inflated by between 5% and 15% at each time point. In addition, if a vendor were to adopt a similar name of another vendor in the hopes of stealing their business, these two vendors would be counted as duplicates. As such, though coefficients in the regression model may represent an inflated estimate of the rate of increase in vendors from month to month, they indicate that this rate was constant across the monitoring period. Indeed, when uncleaned vendor numbers were analysed in an identical fashion as cleaned vendor numbers, the models were comparable, with identical covariates reaching significance and similar conclusions are supported by both models.

4.2. Conclusion

Over time, consumer awareness of, and interest in, cryptomarkets has increased (Buxton and Bingham, 2015; Winstock, 2015). It is interesting to note that this has not been accompanied by an accelerated increase in vendor numbers operating on these marketplaces. Regardless law enforcement efforts to date do not appear to have affected the overall growth of vendor numbers operating on cryptomarkets, and these markets continue to present new challenges. Future research investigating how vendor and/or marketplace characteristics (e.g., the type of substances for sale, length of time active, and number of listings) may affect the rate at which vendor numbers increase would be useful.

Role of funding source

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Contributors

JVB developed the idea for the manuscript in discussion with AR and CB, collected and cleaned data with assistance from SN, conducted analyses with assistance from TD and drafted the manuscript. RB, LB, CB and AR provided guidance and comments on successive drafts of the manuscript. All authors contributed to, and have approved, the final manuscript.

Conflict of interest

None.

References

Barratt, M.J., Aldridge, J., 2016. Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). Int. J. Drug Policy 35, 1–6, http://dx.doi.org/10.1016/j.drugpo.2016.07.005.

Barratt, M.J., 2012. Silk Road: eBay for drugs. Addiction 107, 683, http://dx.doi.org/10.1111/j.1360-0443.2011.03709.x.

Buxton, J., Bingham, T., 2015. The Rise and Challenge of Dark Net Drug Markets: Policy Brief 7 Policy Brief 7. Global Drug Policy Oberservatory, Swansea,Wales.

Chen, A., 2011. The Underground Website Where You Can Buy Any Drug Imaginable. (Accessed 27 July 2015), from http://www.webcitation.org/6ilcUsljH.

Cox, J., 2016. Reputation is everything: the role of ratings, feedback and reviews in cryptomarkets. In: EMCDDA (Ed.), The Internet And Drug Markets. Publications Office of the European Union, Luxembourg.

Danaher, B., Smith, M.D., Telang, R., 2015. The Effect Of Piracy Website Blocking On Consumer Behavior. (Accessed 29 November 2016), from https://ssrn.com/abstract=2612063.

Martin, J., 2014a. Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs. Palgrave Pivot, New York.

Martin, J., 2014b. Lost on the Silk Road: online drug distribution and the 'cryptomarket'. Criminol. Crim. Just. 14, 351–367, http://dx.doi.org/10.1177/1748895813505234.

Munksgaard, R., Demant, J., Branwen, G., 2016. A replication and methodological critique of the study Evaluating drug trafficking on the Tor Network. Int. J. Drug Policy 35, 92–96, http://dx.doi.org/10.1016/j.drugpo.2016.02.027.

Peukert, C., Aguiar, L., Claussen, J., 2016. Catch me if you can: effectiveness and consequences of online copyright enforcement. In: Paper presented at the Vereins für Socialpolitik 2016: Demographischer Wandel – Session: Empirical Market Studies, Augsburg, Germany.

Reitano, T., Oerting, T., Hunter, M., 2015. Innovations in international cooperation to counter cybercrime: the Joint Cybercrime Action Taskforce (J-CAT). EROC 2, 142–154.

Schifano, F., Deluca, P., Baldacchino, A., Peltoniemi, T., Scherbaum, N., Torrens, M., Farrěf, M., Floresg, I., Rossih, M., Eastwoodi, D., Guionnetj, C., Rawafk, S., Agostia, L., Di Furial, L., Brigadam, R., Majavac, A., Siemannd, H., Leonin, M., Tomasina, A., Rovetton, F., Ghodse, A.H., 2006. Drugs on the web; the Psychonaut 2002 EU project. Prog. Neuropsychopharmacol. Biol. Psychiatry 30, 640–646, http://dx.doi.org/10.1016/j.pnpbp.2005.11.035.

Soska, K., Christin, N., 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In: Paper presented at the 24th USENIX Security Symposium, Washington, D.C.

StataCorp, 2013. Stata Statistical Software: Release 13. StataCorp LP, College Station, TX.

Tzanetakis, M., Kamphausen, G., Werse, B., von Laufenberg, R., 2016. The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. Int. J. Drug Policy 35, 58–68, http://dx.doi.org/10.1016/j.drugpo.2015.12.010.

Van Buskirk, J., Roxburgh, A., Farrell, M., Burns, L., 2014. The closure of the Silk Road: what has this meant for online drug trading? Addiction 109, 517–518, http://dx.doi.org/10.1111/add.12422.

Van Buskirk, J., Roxburgh, A., Bruno, R., Burns, L., 2015. Drugs and the Internet, Vol. 5. National Drug and Alcohol Research Centre, Sydney, Australia (Issue 5).

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. Int. J. Drug Policy 35, 16–23, http://dx.doi.org/10.1016/j.drugpo.2016.07.004.

Wagner, A.K., Soumerai, S.B., Zhang, F., Ross-Degnan, D., 2002. Segmented regression analysis of interrupted time series studies in medication use research. J. Clin. Pharm. Ther. 27, 299–309, http://dx.doi.org/10.1046/j.1365-2710.2002.00430.x.

Walsh, C., 2011. Drugs, the internet and change. J. Psychoactive Drugs 43, 55–63, http://dx.doi.org/10.1080/02791072.2011.566501.

Wax, P.M., 2002. Just a click away: recreational drug web sites on the internet. Pediatrics, 109, http://dx.doi.org/10.1542/peds.109.6.e96.

Winstock, A. R., 2015. The Global Drug Survey 2015 findings. (Accessed 19 October 2015), from http://www.webcitation.org/6jcr1G5hC.