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