CSLF Articles   Center for State and Local Finance

1-5-2022

The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces

Marie Ouellet
Georgia State University, mouellet@gsu.edu

David Maimon
Georgia State University, dmaimon@gsu.edu

C. Jordan Howell
University of Texas at El Paso, cjhowell@utep.edu

Yubao Wu
Georgia State University, ywu28@gsu.edu

Recommended Citation

The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces

Marie Ouellet[1]
Assistant Professor
Department of Criminal Justice & Criminology
Georgia State University
55 Park Place NE
Atlanta, GA 30303

David Maimon
Associate Professor
Department of Criminal Justice & Criminology
Department of Computer Science
Georgia State University
55 Park Place NE
Atlanta, GA 30303

C. Jordan Howell
Assistant Professor
University of Texas at El Paso
Department of Criminal Justice
2300 Randolph
El Paso, TX 79968

Yubao Wu
Assistant Professor
Department of Computer Science
Georgia State University
1 Park Place
Atlanta, GA 30303

[1] Corresponding author: mouellet@gsu.edu, +01-404-413-1023

The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces

Abstract: In the face of market uncertainty, illicit actors on the darkweb mitigate risk by displacing their operations across digital marketplaces. In this study, we reconstruct market networks created by vendor displacement to examine how digital marketplaces are connected on the darkweb and identify the properties that drive vendor flows before and after a law enforcement disruption. Findings show that vendors' movement across digital marketplaces creates a highly connected ecosystem; nearly all markets are directly or indirectly connected. These network characteristics remain stable following a law enforcement operation; prior vendor flows predict vendor movement before and after the interdiction. The findings inform work on collective patterns in offender decision-making and extend discussions of displacement into digital spaces.

INTRODUCTION

The emergence of digital marketplaces for the sale of illicit goods has transformed the illicit economy. Digital marketplaces provide centralized platforms for sellers to advertise their products, connect with buyers, and expand their clientele. These marketplaces enable new and exclusively virtual transactions and complement illicit exchanges that occur offline (Leukfeldt, Kleemans and Stol 2017).

Digital marketplaces are not a new phenomenon, yet evidence shows that only recently have vendors begun to displace their operations across multiple marketplaces at higher rates (Ladegaard 2020). The movement of vendors across digital marketplaces suggests they have become increasingly interdependent; that is, what happens on one marketplace affects the marketplaces around it. Law enforcement interventions, including the seizure of a marketplace, impact surrounding markets, displacing vendors to other platforms. The flow of 'market refugees' from seized to neighboring markets has been identified as one of the focal mechanisms through which the online economy has remained resilient to interventions (Ladegaard 2020). Vendors can maintain their online identities and reconnect with existing and new clients on similarly situated digital platforms.

Crime displacement is central to criminological scholarship. Where offenders resume their illicit activities following an intervention sheds insight into the emergence of hot spots and the ability to deter crime (Braga et al. 2019). Yet, we know little about what motivates offenders' decisions to move their illicit activities to a new location - physical or otherwise. Digital marketplaces offer a unique opportunity to extend discussions of crime displacement to online environments. Vendors, their products, and transactions often leave a record, providing mass digital traces across illicit marketplaces and large populations of vendors as they unfold. Digital records from online marketplaces offer a unique opportunity to investigate crime displacement, allowing us to pinpoint where crime moves to and the pathways it takes

to get there. This extends current discussions of displacement and offender decision-making to include *where* offenders move to (also see Hatten and Piza 2021).

The current study adopts a network approach to better understand how digital marketplaces are connected through vendor displacement and assess vendors' decisions to move between markets. Specifically, we ask two interrelated questions: 1) how are digital marketplaces on the darkweb connected through vendor flows, and 2) does the overarching structure of the network help explain vendor flows before and after a law enforcement intervention? To answer these questions, we reconstruct vendor flows across digital marketplaces on the darkweb and examine the connectivity of these marketplaces before and after a major interdiction. We then use exponential random graph models to identify the correlates of vendor flows and assess whether the drivers of vendor movement are disrupted following a law enforcement intervention. Together, the study aims to inform broader processes about crime displacement as it extends to digital spaces.

We begin with a review of digital marketplaces on the darkweb with a focus on their maturation from more centralized to decentralized illicit economies. We then connect this work with research on the impact of interdictions on darknet markets, theoretically grounding our discussion in rational choice and social learning theories. We then detail a mass longitudinal data collection effort to track vendor flows across multiple large-scale marketplaces and the social network methods used to examine the connectivity of this darknet ecosystem. After looking at the aggregate patterns driving vendor flows, we assess the impact of a law enforcement seizure on vendor movement. We conclude by discussing the implications of the findings for advancing criminological theory on crime displacement and offender decision-making.

CRIME DISPLACEMENT IN DIGITAL SPACES

Digital marketplaces on the darkweb

In 2011, Silk Road became one of the first large-scale marketplaces to sell illicit goods on the darkweb. Adopting a similar infrastructure to legal e-commerce sites, such as Amazon and eBay, it set the stage for the trade of illicit goods, facilitating more than $300k in transactions daily (Barratt 2012; Soska and Christin 2015). At its launch, Silk Road was one of a handful of marketplaces providing an online platform for illicit e-commerce; however, its success was accompanied by the emergence of competitors and its downfall even more so. In the months following the marketplace's seizure, several other marketplaces emerged to fill its void (Soska and Christin 2013), a pattern that has since continued (Van Buskirk et al. 2017).

Although digital marketplaces on the darknet are highly volatile, rarely surviving more than a year (Branwen 2019), the larger darknet economy is resilient to external shocks. Much of the scholarship on the impact of law enforcement disruptions have found the stock of illicit transactions, the volume of vendors, and the number of markets recovers relatively quickly after marketplace seizures. For instance, Décary-Hétu and Giommoni (2017) observed that a large-scale seizure led to initial sharp drops in the number of transactions and new vendors registering on e-commerce sites; however, were restored to similar levels within a few months of the intervention (also see Van Buskirk et al. 2017). Likewise, Ladegaard (2019) found that while a law enforcement crackdown led to a significant reduction in the number of available markets, the stock of markets returned to the same level six months following the operation and increased a year and a half later.

Indeed, rather than cripple the darknet economy, recent studies suggest that shocks to digital marketplaces have increased their interdependency. Markets have become increasingly interdependent because vendors are more likely to cross-list their products across multiple marketplaces. One Europol official, commenting on this phenomenon, observed that "[vendors] don't just operate on one market, they cover the full spectrum of the dark web" (Barrett 2020). Consistent with this observation, scholars have documented large numbers of

vendors selling their products across multiple marketplaces (Décary-Hétu and Giommoni 2017; Ladegaard 2019; 2020; Norbutas, Ruiter and Corten 2020).

In one of the most persuasive accounts of the impact of law enforcement interventions on vendor displacement, Ladegaard (2020) documented the widespread adoption of authentication systems across digital marketplaces after a major disruption. Authentication systems allowed marketplaces to validate vendors' online identities, increasing the ease of moving between markets and bringing their online reputations with them. Analyzing vendor migration across three markets, Ladegaard (2020) found that many newly registered vendors had migrated from recently seized digital marketplaces. In effect, the intervention triggered marketplaces' adoption of authentication systems, increasing the ability of illicit actors to navigate between what were once independent marketplaces. In addition, the intervention also led to an uptick in the number of available directories or 'information hubs' that provide lists of active markets, further increasing the resources from which vendors could draw on to make informed decisions on where to set up shop. These adaptations enabled illicit marketplaces to resemble legal ones more closely. Online identities could be verified, and users could consult directories with up-to-date listings of active markets.[1]

Crime displacement, rational choice, and offender networks

Crime displacement, which includes where individuals resume their activities after an intervention, is of central theoretical importance to scholarship on crime and criminal justice. Prior research shows that crime reduction efforts often lead to displacement (Gabor 1981;

---

[1] It is important to note that the increase in ease with which vendors can move between digital platforms has resulted in two distinct but related phenomenon: 1) vendors' cross-use of platforms (instances where vendors advertise their products across multiple marketplaces), and 2) vendors' migration across platforms (instances where vendors move their product listings from an old marketplace to a new marketplace). While vendors' cross-use of platforms and migration represent distinct phenomena, they overlap considerably. Indeed, the volatility of darknet marketplaces has led to increases in vendors operating out of multiple marketplaces and 'refugees' who move to new markets once one has shut down. Both phenomena represent movement patterns, where an offender may move to additional sites to mitigate risk and expand their operations, and both phenomena increase the connectivity and dependency between marketplaces. In the remainder of this article, we use the term vendor movement and flow to capture instances where vendors expand their operations or relocate to new markets.

Repetto 1976), with spatial relocation the most common response (Rossmo and Summers 2021). Where offenders move to is theoretically informed by rational choice theory and to a certain extent, social learning theory.

Rational choice theory views offenders as decision-makers who engage in a cost-benefit analysis of the anticipated risks and rewards of engaging in a criminal act, including the decision of where to offend (Becker 1968; Clarke and Felson 1993). In applying rational choice theory to the study of illicit markets, Reuter and Kleiman (1986) highlight the salient role of perceived rewards and costs associated with illicit market activity, including earnings, incapacitation, and loss of product. Indeed, this same economic calculus has been found to underlie the decision making of actors on digital platforms, including the decision to transition to online markets from offline markets, where profits are viewed as higher and risks as lower (Décary-Hétu and Giommoni 2017; Martin et al. 2020).

More recently, scholars have emphasized that offender decision-making does not occur in a vacuum but is informed by the behaviours and actions of others. In criminology, past work has found that peers shape the anticipated risks associated with engaging in crime (McGloin and Thomas, 2016; Pogarksy, Piquero and Paternoster 2004; Stafford and Warr 1993), perceived benefits (Warr 2002) as well as the skills and opportunities to commit crimes (Morselli et al. 2006; Weerman 2003). The role of peers in shaping offender decisions is a core tenet of social learning theory, which emphasizes that individuals model the behaviours of those around them. Indeed, social learning theory highlights peers as a key reference group from which individuals observe and learn criminal and delinquent behaviours (Akers 2011; Bandura 1978). Consistent with social learning theories, network frameworks offer an important tool to understand the role of peers on behaviours, with its starting point the premise that individuals' actions and beliefs depend on the actions of others in their networks (Wasserman and Faust 1994).

In illicit online markets the role of offenders' networks is clear. Online communities provide individuals with access to a pool of peers who inform individuals' risk of engaging in illicit activity (Aldridge and Askew 2017; Holt, Blevins and Kuhns 2008). Indeed, past work has provided anecdotal evidence that vendor decisions to move to new marketplaces are made collectively (Ladegaard 2020). Moeller et al. (2017) succinctly summarized this phenomenon with a quote from a darknet news forum, "If Silk Road is down, everyone moves to Agora, if Agora is down everyone moves to Evo … and so on […] the DNM's user base is VERY herd like" (p. 1434). Together, these works suggest that offenders weigh the costs and benefits of illicit activity *and* rely on their peer networks for informing their decision calculus, including where to sell their illicit products.

Although prior work suggests offenders' draw from their peers to select illicit marketplaces, there is a notable gap in empirical work investigating precisely how peers shape vendor flows across markets. This work suggests that peers serve as important behavioural models, providing sources of information to evaluate a market's benefits and costs. Instances where vendors see many of their peers on a marketplace can increase the anticipated benefits (e.g., seeing that other vendors have selected the platform as a valuable place to conduct their business) and reduce perceived costs (e.g., signaling trust in the site as not a scam and providing a public display that they have not been arrested) (Ladegaard 2020, p. 13). Alternatively, where individuals see few of their peers on the market may increase a site's perceived risk and dependability. For instance, marketplaces with few of their peers may cue a site that has been planted by agents looking to observe vendor behaviours or indicating there are few buyers on these sites.

In sum, drawing from past theoretical work that contends peers serve as important behavioural models from which to observe and learn offending behaviours, and more recent work that finds illicit market participants draw from their peers to assess the costs and benefits

of illicit activities, we expect vendors' peers to play an important role in shaping online behaviours. Specifically, we expect vendors to move to marketplaces where their peers have moved to in the past, leading to the following hypothesis:

Hypothesis 1: Vendor flows are more likely to occur between marketplaces where vendors' peers have moved to in the past.

Further, drawing on past research that emphasizes disruptions increase vendor movement across marketplaces, we expect this relationship to strengthen following a law enforcement intervention. Indeed, we would expect the anticipated costs of participating in illicit activity to be heightened with increased attention from law enforcement. In these contexts, vendors may be more risk-averse and more likely to rely on their peer network to identify trusted sites, following those vendors who were not detected in the past shutdown. Indeed, prior work has shown that reputation and trust take on a higher market value after a disruption (Duxbury and Haynie 2020). This line of work led to the following hypothesis:

Hypothesis 2: A law enforcement disruption will strengthen the relationship between current vendor flows and where vendors peers' have moved to in the past.

AN EXAMININATION OF VENDOR FLOWS BETWEEN DIGITAL MARKETPLACES

The current study empirically tests these hypotheses by reconstructing vendor flows across digital marketplaces before and after a major law enforcement interdiction. Prior research on crime displacement has primarily focused on whether interventions reduce crime or relocate it to other areas (Hatten and Piza 2021). Here, we examine a large sample of offenders and explore the properties that lead them to move to specific online spaces. In doing so, we seek to move the scholarship on crime displacement forward, substantively and methodologically, by looking at how vendor movement connects digital marketplaces and assessing how the structure of market networks shapes collective patterns in offender decision-making.

Theoretically, our study draws from rational choice and social learning theories to better understand offender decision-making and crime displacement in online spaces. While early scholars emphasized the necessity to study where (and when) crime occurs (Felson 2006), a lack of detailed data precluded these efforts. The digital landscape offers a new source of data to investigate offenders' choice structures and provide insight into the basic determinants of offender displacement patterns. In the current study, we explicitly test whether vendors' decisions on where to sell their products is modeled off the behaviour of their peers. Our results shed light on the processes through which vendors move to different illicit marketplaces, with a focus on the economic and social forces that structure these decisions.

Methodologically, a network approach allows us to explore questions central to scholarship on crime displacement. The questions being raised on online platforms are not new. Crime displacement has been studied for decades, with much of this literature focusing on the impact of crime reduction efforts on the movement of crime to new areas (Braga et al. 2019; Weisburd et al. 2006), and more recent applications on where offenders move to (Hatten and Piza 2021). Specifically, we conceive of marketplaces as a network in which individual e-commerce sites are nodes, and the movement of sellers between sites are edges. We then use exponential random graph models to examine the drivers of vendor movement before and after a law enforcement seizure of one of the largest markets. In doing so, we show how a network approach provides a unique lens through which to explore the etiology of crime displacement.

DIGITAL TRACE DATA ON THE DARKWEB

The data for this paper comes from English-language marketplaces that sell stolen data products hosted on the darkweb. Stolen data products are defined here as fraudulent documents (e.g., drivers' licenses, passports), financial items (e.g., bank accounts, credit cards), counterfeit currencies, services to steal data (e.g., account crackers, injectors), and tutorials or guides related to any of the preceding categories. Because some markets do not classify product

listings or misclassify listings, we used a set of keywords to extract the relevant listings for the analysis (see Appendix I for a full list of keywords). The data only includes marketplaces with more than one vendor and more than 100 stolen data listings.

Marketplaces meeting these criteria were identified by consulting marketplace directories, websites that list active markets on the darkweb and the onion.links to access them. These websites provide a valuable resource for vendors and buyers to identify up-to-date information on markets, including their links, as markets may switch their onion.link in efforts to elude law enforcement or other hostile actors. In addition, marketplaces were located by consulting popular forums on the darkweb for discussions of new markets. Digital records from each marketplace were then compiled into a structured database using web-scraping and parsing tools that extracted all publicly available product listings, and vendor profiles pertaining to stolen data items (Wu et al. 2019). Our final sample comprises 17 markets, 979 unique vendor aliases, and 221,094 product listings over an approximately 12-week period from November 15, 2020, to February 9, 2021.

Methodological barriers largely explain why prior research on the networks of digital markets is limited. To assess vendor flows requires capturing vendor activity across a large sample of digital marketplaces, demanding data across multiple platforms, each with thousands of data points with different infrastructure that can change over time. Because few comprehensive longitudinal datasets across multiple markets exist, these analyses have yet to be carried out. However, collecting data from multiple markets creates empirical obstacles, and the limits to our approach should be noted.

First, marketplaces on the darkweb are notoriously unstable. Markets often go down for maintenance and are not accessible for extended periods. Because of this, we knowingly omit some listings if the market went down during the scraping period. Our data collection approach partially overcomes this limitation, as we scraped the markets weekly and then aggregated this

data over 4-weeks, providing more comprehensive data points. However, we may be missing listings that went up and then were taken down within shorter time intervals. Relatedly, we also faced issues with our own scrapers with the seized market, DarkMarket, not fully scraped in the three weeks prior to it being shut down.

One other limitation that could potentially impact our analysis should be noted. Our data only contains information on vendors' online aliases. It is feasible that vendors use different aliases across marketplaces or that aliases are 'mimicked' by others in efforts to scam buyers, and there is some evidence of this effect (Martin et al. 2020; van Wegberg and Verburgh 2018). However, recent work suggests that the adoption of vendor verification processes by website administrators has limited this possibility (Ladegaard 2020; Norbutas et al. 2020), and others have shown that vendor aliases serve as a valid proxy for identifying vendors' unique identities (Broséus et al. 2016; van Wegberg and Verburgh 2018). Indeed, vendors' aliases provide 'brand recognition', and are directly tied to their online reputations, one of the main ways customers select sellers (Duxbury and Haynie 2018). Although not perfect, in the absence of more reliable approaches we follow past work (Décary-Hétu and Giommoni 2017; Ladegaard 2018; 2019) and treat each vendor alias as unique. In doing so, we are conservative in our approach, requiring exact matches of vendor aliases to be classified as the same vendor.

To help interpret our quantitative findings, we also reached out to vendors to conduct interviews on the factors that structured their decisions to set up storefronts on digital marketplaces. We recruited vendors who made at least one sale on a darknet market in the month preceding the recruitment message. In total, 865 unique vendors fitting these criteria were identified. Due to market volatility, our research team was only able to contact 360 vendors across 12 markets. Specifically, 360 vendors were contacted between 4/14/2021 and 5/1/2021 and asked to participate in an asynchronous interview on an encrypted platform of

their choice. Follow-up messages were sent two weeks after the first participation request. From the 360 vendors contacted, twelve replied. Of those twelve, one completed the full interview, and one completed a partial interview. Content from these interviews is incorporated to provide insight into the decision-making processes underpinning vendor movement; however, we emphasize our limited sample, which we return to in the limitations.

ANALYTIC APPROACH

Our analysis focuses on the social networks created by vendor flows in which the nodes represent markets, and the ties represent the stock of vendors who move between any set of markets. Conceptualizing and measuring vendor flows as market-level social networks allows us to assess the structural features of the network and permit the analyses of the mechanisms driving the structure of the observed market network. We measure the market networks in the one-month period before and after the seizure of one of the largest marketplaces on the darkweb - DarkMarket. We begin by describing the structural characteristics of the market networks, including stability in these structures over time. This includes properties of the network graph such as its overall clustering (density), local clustering (clustering coefficient), and the extent to which vendor movement is centralized around a few key markets (degree centralization). We then use exponential random graph models (ERGMs) to examine the local processes that shape global patterns in the structure of vendor flows, and whether these processes change before and after the market seizure.

Seizure of DarkMarket

The seizure of the DarkMarket on January 11, 2021, by Europol authorities closely resembles a long line of enforcement interventions aimed at curbing illicit activity on the darkweb. At the time of its operation, DarkMarket was identified as one of the largest marketplaces for illicit goods on the darkweb (Europol 2021). Overnight, the site was taken down, with law enforcement seizing the servers that hosted the website and arresting the alleged operator of

the market. Its takedown provides a unique opportunity to test how an intervention impacts vendor flows across markets and is consistent with other studies that have tested the impact of law enforcement interventions on digital marketplaces (Décary-Hétu and Giommoni 2017; Ladegaard 2019; van Buskirk et al. 2017).

Dependent variable: Vendor flows between digital marketplaces

The dependent variable measures the intensity of vendor flows between any two sets of digital marketplaces involved in the sale of stolen data. The networks are two-mode network affiliation data that records all markets a vendor advertised stolen data products (vendor-by-market) and the dates they were recorded as listing these products. The affiliation networks are then converted into networks of co-affiliation by creating a new matrix that records the number of vendors who moved between any pair of markets. The resulting data is a one-mode network (market-by-market) with the same market listed in the rows and columns of the matrix. The value of each cell in the market matrix indicates the number of vendors who passed from the sender market (rows) to the receiver market (columns), allowing us to identify the stock of vendors who listed stolen data products in one market (Market A), and then began listing stolen data products on another (Market B). As such, markets are connected if 1) a vendor expanded the number of marketplaces they are on (listed products on Market A at time t and then listed products on Market B at time $t + 1$), or 2) a vendor left a marketplace and joined a new one (discontinued listing products on Market A at time t and then began listing products on Market B at time $t + 1$). Thus, ties between markets are directed and valued, indicating the direction of the vendor flow and the intensity of the flow, with more vendors moving between any two sets of markets having higher values. We measure our dependent variable at two time points, one month before the seizure of DarkMarket (pre-seizure network) and one month after the seizure of DarkMarket (post-seizure network).

To control for the fact that certain markets may have greater opportunity for higher out-flows based on the total vendor population on that market, we measure vendor out-flows as the number of vendors who move from the market as the proportion of all vendors on the market at time t. After calculating the ratio of market out-flow to the market vendor population across all pairs of markets, we use quartiles to determine thresholds between markets that send few vendors and those that send many vendors. The quartiles classify the edges into categories based on the intensity of vendor flows, with lower values indicating a lower proportion of out-flow and higher values indicating a higher proportion of out-flow. This approach was adopted from analyses of human migration networks to control for countries of different sizes (Vogtle and Windzio 2016).

Exponential Random Graph Models (ERGMs)

While the network statistics allow us to describe patterns in vendor flows, the use of ERGMs allows us to test 1) the mechanisms that drive the formation of the market networks and 2) the impact of a law enforcement interdiction on disrupting the structure of vendor flows between markets. ERGMs model the likelihood of tie formation within the observed network as a function of both actor attributes and characteristics of the network itself. ERGMs are uniquely suited to answer our research question, as they provide a means to overcome the problem of endogeneity that is inherent to network data and thus violates assumptions of traditional regression techniques (Robin, Lewis and Wang 2012). ERGMs resolve the problem of non-independence by explicitly modeling how one network tie influences the likelihood of other network ties (Lusher, Koskinen and Robins 2013). Further, ERGMs allow us to explicitly test peer effects by including network features as covariates in the model. This is key to the current study, which aims to directly test whether patterns in vendor displacement are influenced by the behaviours of other vendors.

The longitudinal nature of the data provides two analytical approaches for modeling change in the market networks: 1) a temporal ERGM (TERGM) with binary network data, or 2) two separate ERGMs (pre- and post- seizure) with valued network data and a lagged dyadic covariate for prior network structure. The first option, TERGMs extend standard ERGMs by modeling the extent to which the edges (and non-edges) are stable across observations. However, current applications of TERGM are restricted to binary data, and thus would potentially treat markets with high and low volumes of vendor out-flows as equivalent, conflating very different marketplace profiles. In contrast, the second option, valued ERGMs, extends standard ERGMs by also modeling whether a covariate increases or decreases the value of an edge between network actors (Krivitsky 2012). As such, valued ERGMs allow us to assess not only which markets experience vendor flows but also the intensity of these flows, allowing us to measure the stock of vendor movement across markets.

Valued ERGMs require specifying a reference distribution to model how edge values are distributed among network actors. Here, we use a Poisson-reference distribution to model the overall network (Krivitsky 2012). We estimate the likelihood and intensity of ties forming between markets using two classes of predictors: nodal covariates and structural covariates. Nodal covariates test whether actor attributes impact their probability of receiving or forming a tie and the intensity of that tie. Nodal covariates are dyad independent as the likelihood any pair of nodes will have a network tie depends on their attributes but is not conditional on other network ties. Structural covariates test whether properties of the network itself impact the probability any pair of nodes will have a network tie and the intensity of that tie. Structural covariates are dyad dependent, with the probability of a tie being modeled as conditional on other network ties. Together, these covariates offer different insights into the local processes that dictate collective patterns in vendor flows.

Nodal covariates

Number of vendors is a measure of the number of unique vendor aliases on the marketplace at time *t*. This measure serves as a proxy of market supply and is theoretically informed by rational choice perspectives, which contend that economic calculations, including supply and demand, drive illicit activity on and offline (Aldridge and Décary-Hétu 2016; Décary-Hétu and Giommoni 2017; Demant, Munksgaaard and Houbourg 2016; Reuter and Kleiman 1986). We would expect greater supply (i.e., more vendors) to reduce the likelihood vendors would join an already competitive market. However, we also recognize that the number of vendors may also impact vendors' risk assessment for joining the market, independent of financial considerations. Indeed, past work has shown the presence of others impacts the decision to engage in illicit activity, increasing an individual's perceived anonymity and decreasing the anticipated sanctions with engaging in the activity (McGloin and Thomas 2016). Thus, is it also possible to conceive that markets with more vendors will attract additional vendors to the market.

Price change is a measure of the extent to which listing prices change on the marketplace at time *t*. We measure the average price change of a product listing by taking the same listing and comparing its price at weekly intervals. We measure this across all listings and then take the average over the four-week period, providing the average price change across product listings on the market. This measure serves as a proxy of a marketplace's demand, an approach consistent with other studies (Décary-Hétu and Giommoni 2017). Similar to our measure of market supply, we draw from the rational choice perspective that shows vendors are motivated by financial incentives (Martin et al. 2020; Reuter and Kleiman 1986). We thus expect vendors to be more attracted to marketplaces with increases in demand (price increases) and less attracted to marketplaces with drops in demand (price decreases).

In addition, directed networks offer the opportunity to investigate how market covariates impact the probability of sending ties or receiving ties. Thus, for both nodal

covariates described - *number of vendors* and *price change* - we examine the impact of the nodal attribute on out-degree (the likelihood a market will send high out-flows of vendors to other markets), and in-degree (the likelihood a market will receive high in-flows of vendors from other markets) , allowing us to disentangle vendor decisions to leave old markets, from vendor decisions to join new ones.

Network covariates

Density is modeled using the *sum* parameter, which indicates the expected value of a tie between any pair of markets based on the value of all observed network ties (Handcock et al. 2021). The sum term is analogous to an intercept in standard regression techniques, reflecting the baseline edge value across network actors.

Reciprocity is modeled using the *mutual* term, which estimates the likelihood a tie between any pair of network nodes will be reciprocated (Handcock et al. 2021). That is, the extent to which vendors from Market A move to Market B also influences whether vendors from Market B move to Market A. Reciprocity is a well-established network process that can impact network structure, serving as an important control for estimating structural processes.

Transitivity is measured using the *transitiveweights* term, which examines whether a tie value in the network could be explained by triad closure. Transitivity occurs in networks when ties between two sets of actors increase the likelihood of a tie between a third actor. In our case, transitivity allows us to test whether vendor flows are likely to move between markets that have a tie in common, and thus whether clustering dictates how vendors' move between markets. Prior research on criminal networks has observed that illicit networks are more likely to adopt decentralized and secure structures following a law enforcement intervention (Morselli, Giguère and Petit, 2007; Ouellet et al. 2017). However, recent work on digital marketplaces has suggested that vendors are more likely to displace their operations following a market seizure, which would suggest that they become more connected and less secure. A negative

effect for this term this would support the former hypothesis (more secure structures), while a positive effect would support the latter hypothesis (more efficient structures) with greater clustering in network ties.

Prior network structure is our main covariate and is modeled using a dyadic covariate term, which entails the adjacency matrix of vendor flows in the preceding four-week period, i.e., a lagged dependent variable. The dyadic covariate term allows us to test the hypothesis that vendor flows are more likely to occur between markets in which they have occurred in the past and whether a law enforcement operation strengthens or interrupts this peer effect. A positive and statistically significant effect would suggest that vendor flows are structured by where their peers moved in the fast. Should this effect become stronger in the post-seizure network, this would suggest vendors increase their reliance on their peers to decide where to sell their illicit products.

RESULTS

We present our results in two stages. The first stage describes the structural features of the digital marketplaces before and after a law enforcement seizure. This stage aims to determine the extent to which vendor flows connect the various marketplaces and the features of these networks. The second stage explains the generative processes that led to the observed networks, presenting the results from the ERGMs. This stage aims to identify the basic explanatory variables associated with vendor displacement across markets and whether this changes following a disruption. Across both sections, we supplement quantitative findings with accounts from our interviews with vendors.

How vendor flows connect digital marketplaces

Figure 1 depicts the marketplace networks before and after a law enforcement seizure. Each node in the network represents a market involved in the sale of stolen data on the darknet. The size of the node indicates the extent to which vendors moved to that market: larger nodes signal

markets that received vendor flows from a greater number of markets. The edges show the intensity of the vendor flows between markets, with thicker edges representing a higher stock of vendors moving between these markets and arrows indicating the direction of the flows.

Figure 1 highlights two key features of the network. First, digital marketplaces on the darkweb are highly connected. The flow of vendors across digital marketplaces creates a network that links almost all markets into a single component. Nearly all marketplaces are directly or indirectly connected to one another through vendor flows. Second, this connectivity persists before and after a major law enforcement intervention. Together, this figure provides a first look at the structure of vendor flows across digital marketplaces, showing the connected nature of the darknet ecosystem.

Table 1 presents the descriptive statistics for the market networks, providing a more detailed understanding of how vendor flows are distributed across the network. The pre-seizure market network consists of 17 markets and 95 ties connecting them. A network density of .349 before the seizure of DarkMarket indicates that 35 percent of all possible ties between network actors are observed in the market. The clustering coefficient looks at the local connectivity of the market network, the extent to which ties are clustered around actors. A clustering coefficient of .676 suggests that there is a relatively high degree of clustering within markets. Degree centralization indicates whether network ties are concentrated around a few central actors, with higher values indicating higher concentrations (Freeman 1979). In-degree centralization captures the extent to which a few markets receive the majority of ties. In contrast, out-degree centralization captures the extent to which a few markets send the majority of ties. Prior to the seizure, markets that received vendors tended to be more centralized with an in-degree centralization of .401. In contrast, markets that sent vendors tended to be slightly more distributed across marketplaces, with an out-degree centralization of .276.

Vendor flows pre-law enforcement seizure
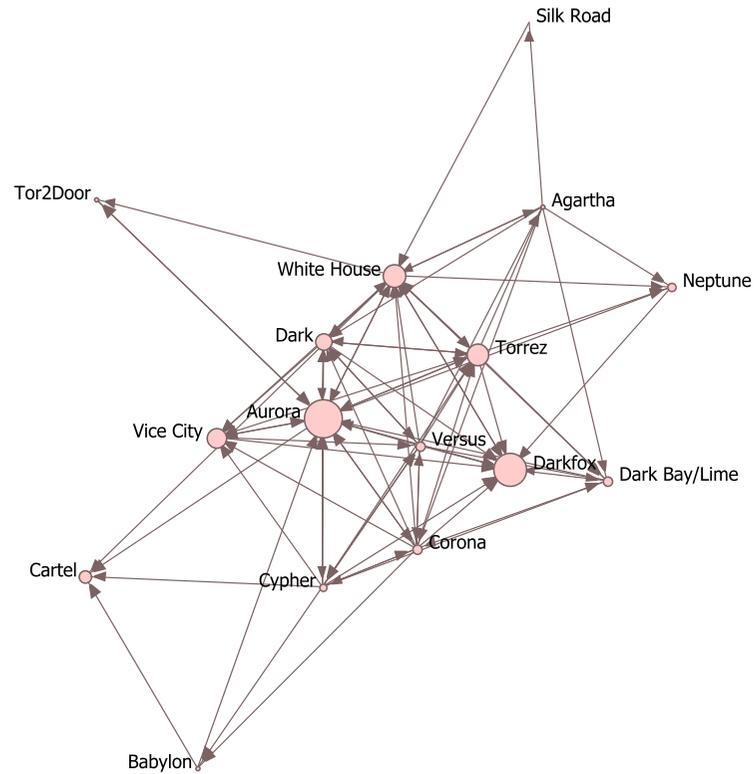
**Vendor flows post-law enforcement seizure**
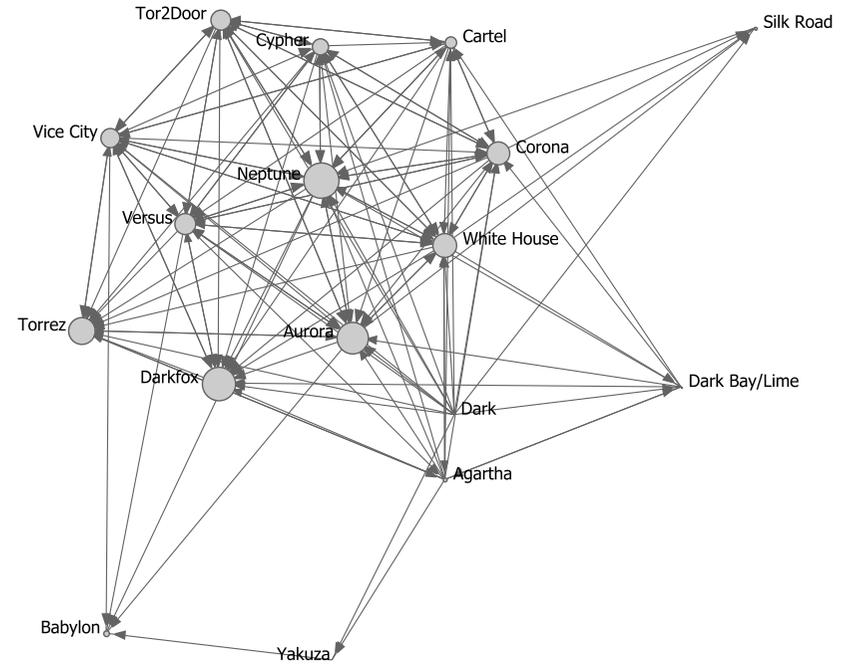
Figure 1. Vendor flows between digital marketplaces on the darknet

Notes: Node size indicates a market's in-degree. Edge width captures the intensity of vendor flows, with thicker edges indicating a higher volume of vendors flowing between any pair of markets and arrows the direction of the flow. One isolate in the pre-seizure network, Yakuza Market, is not shown.

Table 1. The network structure of vendor flows between digital marketplaces on the darkweb

Measure	Pre-seizure network	Post-seizure network
Size	17	17
Edges	95	122
Density	.349	.449
Clustering coefficient	.676	.838
In-degree centralization	.401	.301
Out-degree centralization	.276	.364

Consistent with the pre-seizure network, the post-seizure network consists of 17 markets, but they are better connected with a higher number of ties between them, 122 edges as compared to 95 edges before the seizure. Although DarkMarket was seized, we include it in the post-seizure network to observe the out-flow of vendors to other markets. The post-seizure market network becomes more connected, with the density increasing to .449 and the clustering coefficient to .838, as compared to the pre-seizure network. This suggests that vendor flows became more dispersed, with vendors connecting more of the markets, a finding consistent with prior work that suggests vendor flows increased following an intervention (Ladegaard 2020). While out-degree centralization increases slightly across the pre- and post-seizure period, in-degree centralization drops slightly in the post-seizure period. This suggests markets sending vendors become slightly more concentrated around a few markets, consistent with the takedown of DarkMarket and large outflows from this market. In addition, vendor in-flows become slightly less centralized; the network figure confirms this, highlighting a larger core group of markets that received greater vendor in-flows after the law enforcement seizure.

The tendency for vendors to move across multiple platforms can be seen in one vendor's account of how they choose which marketplaces to sell their products: "I initially got grandfathered into one of the top markets places also known as white house market, thats where all the real players are. From white house i was able to get vendor bond waived on almost every other market place". Another vendor emphasized that having multiple storefronts minimized any concerns about a market going down: "i have plenty of backup storefronts already active

21

and my customers will know how to find me not super difficult." This finding confirms what has been found by others, setting up shop across multiple marketplaces is facilitated by marketplace administrators (waiving vendor fees for established vendors), and is a strategy for vendors' coping with the volatility of markets. In the next section, we explore the processes that lead vendors to select specific marketplaces.

The correlates of vendor flows between digital markets on the darkweb

Table 2 introduces the results for the Poisson ERGMs, which model the intensity of vendor flows between any pair of markets. We estimate two models: the predictors of vendor flows pre-seizure (left) and vendor flows post-seizure (right). For both sets of models, we include the same set of nodal and structural covariates. For the pre- and post-seizure networks, the prior network structure term entails the lagged adjacency matrix of vendor flows in the prior four-week period. In the post-seizure network, this term entails the adjacency matrix of the pre-seizure network. In the pre-seizure network, this term entails the adjacency matrix of the market network 4-weeks prior to the pre-seizure network.

Table 2. Poisson exponential random graph models predicting vendor flows between digital marketplaces

	Pre-seizure network Model 1	Post-seizure network Model 2
Sum	-.233 (.220)	-.824*** (.232)
Market variables		
N vendors – receiving market	-.001 (.001)	$.003^{\dagger}$ (.001)
N vendors – sending market	-.003* (.001)	.004* (.001)
Price change – receiving market	-.009 (.024)	-.040** (.013)
Price change – sending market	-.114** (.039)	-.034*** (.009)
Network variables		
Reciprocity	-.582* (.240)	-.918*** (.189)
Transitivity	.290 (.189)	.854*** (.220)
Prior network structure	.670*** (.139)	.340*** (.123)
AIC	-32.16	-62.36
BIC	-3.31	-33.51

*** $p < .001$, ** $p < .01$, * $p < .05$, $^{\dagger} p < .10$

Table 2 shows that vendor flows prior to the seizure of DarkMarket were guided by the number of vendors and prices. The negative and significant effect for the *number of vendors –*

sending market indicates that markets with more vendors were less likely to experience out-flows of vendors to other marketplaces. The finding that vendors are less likely to move away from markets with a high number of vendors aligns with past work, which observes individuals' perceptions of risks decreases when more peers are present (McGloin and Thomas 2016). The negative and significant effect for *price change – sending market* indicates that markets that had a drop in listing prices were more likely to experience out-flows of vendors to other markets. The finding that markets with a drop in demand are consistent with core tenets of rational choice and the well-established finding that offender decision-making is structured by financial motives (Martin et al. 2020; Reuter and Kleiman 1986). Together, these results show that marketplace factors shaped vendor decisions to displace their operations but not where they chose to move to.

In terms of the network variables, the *reciprocity* term had a negative and significant effect, showing that out-flows of vendors to other markets tended not to be reciprocated from the receiving market. However, the *transivity* term had null effects on vendor flows, showing no clustering within the pre-seizure network. In support of our main hypothesis, the network lag term - *prior network structure* - had a positive and significant effect, indicating that the movement of vendors between markets was guided by the collective patterns of where individuals had moved in the past.

The model of vendor flows after the seizure of DarkMarket, suggests a change in vendor preferences for selecting marketplaces. Specifically, we observe positive and significant effects for both the *number of vendors – receiving market* and the *number of vendors – sending market,* showing that marketplaces with a higher number of vendors were more likely to experience out-flows and in-flows of vendors. Thus, after a major marketplace was seized, vendors responded by moving to markets where there were more vendors; however, they also left markets that had higher numbers of vendors. The former result is consistent with theoretical

expectations that vendors would move to sites where there were more vendors, potentially signally greater anonymity, where they were less likely to be singled out and hidden within a larger group. However, the finding that vendors left markets with a higher number of vendors contrasts with what we found in the pre-seizure market, potentially suggesting that the disruption may have made vendors more risk-averse to remain on the same market, and more inclined to expand their operations.

Price changes remained a significant factor for shaping vendor out-flows and helped explain vendor in-flows in the post-seizure models. After the seizure of DarkMarket, there was a negative and significant effect for both *price change – receiving market* and *price change – sending market*, indicating vendors were more likely to move to and from markets that had drops in prices. Although counterintuitive at first, this finding may also be partially explained by the tendency for vendors to look for their own deals, which they can then resell. For instance, one vendor explained, "If I see something that's a good deal i will buy it just for the sole intention to resell but always bulk listings obviously, that's how you make money." From this perspective, vendors may be attracted to marketplaces from which they can also source their products more efficiently.

Consistent with the pre-seizure model, the *reciprocity* term is negative and significant, indicating that vendor flows were not reciprocated across marketplaces after the intervention. In contrast to the pre-seizure model, the *transitivity* term is positive and significant, indicating that after the seizure there was clustering of vendor flows between markets, with vendors more likely to move to markets that had a shared market in common. This result is consistent with our descriptive findings that showed the network became more clustered following the law enforcement seizure. Lastly, consistent with the pre-seizure network, the *prior network structure* term remains positive and significant. This provides support for our first hypothesis that vendors were more likely to move to markets that their peers had moved to in the past.

However, we do not find evidence for our second hypothesis, which expected this relationship to become stronger in the post-seizure network. Rather, we find that vendor flows stayed relatively stable before and after the intervention.

DISCUSSION

In the current study, we find that digital marketplaces on the darkweb are highly connected through vendors who span multiple platforms. Further, we observe that vendors do not randomly select into markets, and these micro-preferences produce aggregate level patterns that generate the ecosystem's structure. Below we detail the main findings of our study and discuss how they build on prior theoretical and empirical work on offender networks and displacement.

The current study extends investigations of crime displacement and offender-decision making to show that where offenders decide to commit their crimes is shaped by their peers. Vendors were more likely to select into marketplaces where their peers had moved to in the past, and this finding stayed consistent before and after a law enforcement disruption. This result is consistent with larger propositions from social learning theory emphasizes the role of peers in offender decision making (Akers 2011). Although our data do not allow us to uncover the mechanisms that underlie peer effects, prior research offers some clues. Peers shape the perceptions of costs and benefits of deviance, including perceived sanction risk (McGloin and Thomas 2016; Pogarsky et al. 2004; Stafford and Warr; 1993) and the anticipated rewards (Warr 2002). In digital marketplaces, vendors observing their peers move to another market may provide cues that the market is trustworthy. Indeed, scholars have long emphasized that a dominant driver of illicit market activity is trust, with buyers more likely to purchase products from trustworthy vendors, more so than the cost of the products being purchased (Duxbury and Haynie 2018, also see Diekmann et al. 2014), and reputation takes on a higher market value after a disruption (Duxbury and Haynie 2020). Our results suggest that just as buyers pick up

cues on trustworthy sellers from other buyers' experiences, vendors also rely on their networks to assess which markets are trustworthy on which to sell their wares. In essence, seeing their peers move to a new marketplace serves as an endorsement of the platform.

In addition, our study's findings showed that marketplace networks became more connected after a law enforcement intervention, a result that runs counter to the well documented finding that illicit networks tend to adopt more secure and decentralized structures in the face of risk and uncertainty (Morselli et al. 2007; Ouellet et al. 2017). The different responses of criminal networks across offline and contexts may be partially explained by the anonymity afforded by the darknet. A key consideration as to whether a network will adopt secure structures hinges on if they have access to trusted participants or depend on more risky affiliates (Morselli et al. 2007). When risk increases, individuals may protect themselves by adopting more secure network positions where they are less dependent (or connected) to these less trusted others. In online markets, an individual's identity remains hidden to the market participants, and thus their networks are less subject to concerns that predominate offline criminal activity. In these anonymous contexts, vendors more closely resemble sellers on licit e-commerce sites, relying on online reviews and ratings to establish the quality of their products. When markets become more volatile, vendors can mitigate risks by already having established a storefront on another platform where their vendors can easily find them. Indeed, one of our vendor interviews emphasized that setting up multiple storefronts provide 'backups', allowing them to mitigate the loss from market closures.

Lastly, we observe that economic calculus drives offenders' decisions on where to sell their products online. Specifically, we found that vendors were more likely to move to and from marketplaces that recently experienced drops in demand. The finding that vendors move *from* marketplaces that experienced drops in demand is consistent with a rational choice perspective that identifies financial factors as weighing heavily in offender decision-making,

with the aim of maximizing profits (Reuter and Kleiman 1986). However, the finding that vendors move *to* marketplaces that also experience drops in demand runs counter to this logic. While counterintuitive at first, this may indicate that vendors who were experiencing a decrease in demand decided to expand their research to other markets, in line with prior research which has found vendors on multiple markets are more likely to reap higher profits (Ladegaard 2020; Norbutas et al. 2020), and vendor interviews expressing how lower prices allow vendors to capitalize by reselling these products on their own terms. Vendors may absorb these costs in the short-term, establishing themselves on the platform on the belief that demand will resume later, a proposition consistent with past work (Décary-Hétu and Giommoni 2016).

Limitations

Our study relies on vendors involved in the sale of stolen data products on digital marketplaces on the darkweb. Stolen data items are the second largest category of illicit products on darkweb marketplaces (after drugs); however, they only represent a subset of all illicit online listings (Hutchings and Holt 2014). While we can capture a high number of markets, we do not have data on all vendors active on these markets, or all markets active on the darkweb and clearnet. Limiting our analysis to the subset of products on the darkweb provides the necessary infrastructure to compare multiple vendors using the same variables; however, this could potentially obscure some patterns that may be observed in these other settings, and thus findings apply primarily to this context.

Further, our analysis only focuses on the impact of a single shock to digital marketplaces on the darkweb - the seizure of DarkMarket on January 11, 2021. However, this only captures one of many law enforcement interventions on the darknet. Earlier interventions, including the shutdown of Empire market in August of 2020, may still be creating waves on the darknet where markets and vendors are recovering from these earlier shocks. Relatedly, while darknet marketplaces provide troves of data on illicit transactions, they miss data on

some of the core covariates of criminality, including offender backgrounds, such as sex, and age, which may impact decisions to offend, and where they decide to commit their offences.

Lastly, we emphasize that our interviews rely on a small sample. Our low response rate may be a function of our sampling frame, recruitment strategy, or a combination of both. Vendors who sell stolen data products on the darknet may perceive the risks associated with being interviewed as outweighing the rewards. Thus, it is our belief the response rate could be improved by increasing the rewards (incentivizing participants) or decreasing the perceived risks (establishing trust and credibility) of participation. In addition, we also take note of the small samples of recent research adopting similar approaches, including the largest sample of qualitative interviews being 13 vendors selling drugs on these platforms (Martin et al. 2020). Strategies, such as developing rapport in online spaces, including partnering with established websites, may partially explain the discrepancies, and we encourage further work in this area.

CONCLUSION

Our study advances a network framework to understand digital marketplaces as an ecosystem. Drawing from data across multiple marketplaces, we showed illicit marketplaces are highly connected through vendors who move between different platforms, and that these networks became more connected after a disruption. Investigating the local mechanisms that drove the structure of the observed market network, we observed that economic considerations including fluctuations in market demand structured vendor flows between markets. We also found that vendor flows were more likely to occur between marketplaces where their peers had moved to in the past, providing an endorsement of the platform. Together, our study demonstrates the importance of bringing together economic and social forces, including peers' behaviours, for explanations of crime displacement and offender-decision making.

REFERENCES

Akers, R. (2011), *Social Learning and Social Structure: A General Theory Of Crime And Deviance,* Transaction Publishers.

Aldridge, J., and 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.

Aldridge, J., and Décary-Hétu, D. (2016), 'Hidden Wholesale: The Drug Diffusing Capacity of Online Drug Cryptomarkets', *International Journal of Drug Policy,* 35:7-15.

Barratt, M. J. (2012), 'Silk Road: Ebay for Drugs', *Addiction* 107/3:683--683.

Barrett, B. (2020), '179 Arrested in Massive Global Darkweb Takedown', *Wired*. Retrieved June 13, 2021 (https://www.wired.com/story/operation-disruptor-179-arrested-global-dark-web-takedown/).

Becker, G. S. (1967), 'Crime and Punishment: An Economic Approach', *Journal of Political Economy,* 76:169-217.

Braga, A. A., Turchan, B. S., Papachristos, A. V., and Hureau, D. M. (2019), 'Hot Spots Policing and Crime Reduction: An Update of an Ongoing Systematic Review and Meta-Analysis', *Journal of Experimental Criminology,* 15/3:289–311.

Branwen, G. (2019), 'Darknet Market Mortality Risks', *Gwern.Net*. Retrieved June 13, 2021 (https://www.gwern.net/DNM-survival).

Clarke, R. V. G., and Felson, M. (1993), *Routine Activity and Rational Choice*. Transaction Publishers.

Décary-Hétu, D., and 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.

Demant, J., Munksgaard, R., and Houborg, E. (2018), 'Personal Use, Social Supply or Redistribution? Cryptomarket Demand on Silk Road 2 and Agora', *Trends in Organized Crime,* 21/1:42–61.

Duxbury, S. W., and Haynie, D. L. (2018a), 'Building Them up, Breaking Them down: Topology, Vendor Selection Patterns, and a Digital Drug Market's Robustness to Disruption', *Social Networks,* 52:238–250.

Duxbury, S. W., and Haynie, D. L. (2018b), 'The Network Structure of Opioid Distribution on a Darknet Cryptomarket', *Journal of Quantitative Criminology,* 34/4:921–941.

Duxbury, S. W., and Haynie, D. L. (2020), 'The Responsiveness of Criminal Networks to Intentional Attacks: Disrupting Darknet Drug Trade', *PLOS ONE.* 15/9:e0238019.

Europol. (2021), 'DarkMarket: World's Largest Illegal Darkweb Marketplace Taken Down.', *Europol*. Retrieved June 16, 2021 (https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down).

Felson, M. (2006). *Crime and Nature*. SAGE Publications.

Freeman, L. C. (1978), 'Centrality in Social Networks: Conceptual Clarification', *Social Networks,* 1:215–239.

Gabor, T. (1981), 'The Crime Displacement Hypothesis: An Empirical Examination', *Crime & Delinquency,* 27/3:390–404.

Gibbs, J. P. (1975), *Crime, Punishment, and Deterrence,* New York, NY: Elsevier.

Handcock, M., Hunter, D., Butts. C., Goodreau. S., Krivitsky. P., and Morris, M. (2021), *ergm: Fit, Simulate and Diagnose Exponential-Family Models for Networks*. The Statnet Project (https://statnet.org). R package version 4.0.1, https://CRAN.R-project.org/package=ergm.

Hatten, D., Piza, E. L. (2021), 'When Crime Moves Where Does It Go? Analyzing the Spatial Correlates of Robbery Incidents Displaced by a Place-Based Policing Intervention.' *Journal of Research in Crime and Delinquency*, Online First.

Holt, T. J., Blevins, K. R., and Kuhns, J. B. (2008), 'Examining the Displacement Practices of Johns with On-Line Data', *Journal of Criminal Justice.* 36/6:522–28.

Howell, C. J., and Burruss, G. W. (2020), 'Datasets for Analysis of Cybercrime', in T.Holt and A. Bossler, eds., *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Palgrave Macmillan, Cham.

Hutchings, A., and Holt, T. J.. (2015), 'A Crime Script Analysis of the Online Stolen Data Market', *British Journal of Criminology,* 55/3:596–614.

Krivitsky, P. N. (2012), 'Exponential-Family Random Graph Models for Valued Networks', *Electronic Journal of Statistics,* 6:1100–1128.

Ladegaard, I. (2018), '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,* 58/2:414–33.

Ladegaard, I. (2019), 'Crime Displacement in Digital Drug Markets', *International Journal of Drug Policy*, 63:113–21.

Ladegaard, I. (2020, 'Open Secrecy: How Police Crackdowns and Creative Problem-Solving brought Illegal Markets out of the Shadows', *Social Forces,* 99:532-559.

Leukfeldt, R. E., Kleemans, E. R., and Stol, W. P. (2017), 'Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks.', *British Journal of Criminology,* 57/3:704–22.

Lusher, D., Koskinen, J., and Robins, G. (2013), *Exponential Random Graph Models for Social Networks: Theory, Methods, and Applications*, Cambridge University Press.

Martin, J., Munksgaard, R., Coomber, R., Demant, J., and Barratt, M. J. (2020), 'Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards', *British Journal of Criminology*, 60/3:559–78.

Mcgloin, J. M, and Thomas, K. J. (2016), 'Incentives for Collective Deviance: Group Size and Changes in Perceived Risk, Cost, and Reward', *Criminology,* 54/3:459–86.

Moeller, K., Munksgaard, R., and Demant, J. (2017), 'Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs', *American Behavioral Scientist*, 61/11:1427–50.

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., and Aldridge, J. (2017), 'Conflict Management in Illicit Drug Cryptomarkets', *International Criminal Justice Review,* 27/4:237–54.

Morselli, C., Giguere, C, and Petit, K. (2007), 'The Efficiency/Security Trade-off in Criminal Networks', *Social Networks,* 29/1:143-153.

Morselli, C., Tremblay, P., and McCarthy, B. (2006), 'Mentors and Criminal Achievement', *Criminology,* 44/1:17–43.

Norbutas, L., Ruiter, S., and Corten, R. (2020), 'Believe It When You See It: Dyadic Embeddedness and Reputation Effects on Trust in Cryptomarkets for Illegal Drugs', *Social Networks,* 63:150–61.

Ouellet, M., Bouchard, M., & Hart, M. (2017), 'Criminal Collaboration and Risk: The Drivers of Al Qaeda's Network Structure Before and After 9/11', *Social Networks,* 51:171-177.

Pogarsky, G., Piquero, A. R., and Paternoster, R. (2004), 'Modeling Change in Perceptions about Sanction Threats: The Neglected Linkage in Deterrence Theory', *Journal of Quantitative Criminology,* 20/4:343–69.

Reuter, P., and Kleiman, M. A. R. (1986), 'Risks and Prices: An Economic Analysis of Drug Enforcement', *Crime and Justice,* 7:289–340.

Robins, G., Lewis, J. M., and Wang, P. (2012), 'Statistical Network Analysis for Analyzing Policy Networks', *Policy Studies Journal,* 40/3:375–401.

Rossmo, D. K., and Summers, L. (2021), 'Offender Decision-Making and Displacement', *Justice Quarterly,* 38/3:375–405.

Soska, K., and Christin, N. (2015), 'Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem' Paper presented at USENIX Security 2015. Washington, DC.

Stafford, M. C., and Warr, M. (1993), 'A Reconceptualization of General and Specific Deterrence', *Journal of Research in Crime and Delinquency,* 30/2:123–35.

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S., and Roxburgh, A. (2017), 'The Recovery of Online Drug Markets Following Law Enforcement and Other Disruptions', *Drug and Alcohol Dependence,* 173:159–62.

Vögtle, E. M., and Windzio, M. (2016), 'Networks of International Student Mobility: Enlargement and Consolidation of the European Transnational Education Space?', *Higher Education,* 72/6:723–41.

Weerman, F. M. (2003), 'Co-Offending as Social Exchange', *British Journal of Criminology,* 43/2:398–416.

van Wegberg, R., and Verburgh, T. (2018), 'Lost in the Dream? Measuring the Effects of Operation Bayonet on Vendors Migrating to Dream Market', Paper presented at the Web Science Conference '18 in *Evolution of the Darknet Workshop.*

Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., and Gajewski, F. (2006), 'Does Crime Just Move around the Corner? A Controlled Study of Spatial Displacement and Diffusion of Crime Control Benefits', *Criminology,* 44/3:549–91.

Wu., Y., Zhao, F., Chen, X., Skums, P., Sevigny, E. L., Maimon, D., Ouellet, M., Haavisto Swahn, M., Strasser, S. M., Feizollahi, M. J., Zhang, Y., and Sekhon, G. (2019), 'Python Scrapers for Scraping Cryptomarkets on Tor', Pp. 244–60 in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, *Lecture Notes in Computer Science*, edited by G. Wang, J. Feng, M. Z. A. Bhuiyan, and R. Lu. Cham: Springer International Publishing.

Appendix I. Online Stolen Data Keywords

Category	Keywords
Fraudulent Documents (personal identity)	"birth certificate", "camla", "car title", "citizenship", "college id", "custom ident", "dl template", "dlicense", "dls", "drive license", "driver license", "drivers license", "driver's license", "driving license", "earnings statement", "efset", "electricity bill", "electricity statement", "entry stamp", "fraud id", "gmat", "green card", "holograms id", "id card", "id pack", "id photo", "id scan", "id template", "identity doc", "identity set", "ids", "ids scan", "ielts", "income template", "insurance slip", "license template", "pack of id", "passport", "pay stub", "paystub", "pp template", "proof of employment", "psd template", "registered dl", "registered doc", "registered id", "residence permit", "scan id", "scotiabank", "selfies holding id", "social insurance number", "social security card", "social security number", "ssn", "student id", "tax form", "tax return", "tax statement", "template (psd)", "template psd", "toeic", "toelf", "university id", "utilities statement", "utility bill", "utility statement", "voter id card", "w2 form", "water bill", "water statement"
Financial (bank accounts, dumps, credit cards)	"american express", "amex", "atm blank card", "atm card", "atm cash", "balance", "bank acc", "bank drop", "bank login", "bank of america", "bank statement", "bank transfer", "billing statement","cashapp", "cashing", "cashout", "chase", "cheque", "cibc", "clone card", "credit card", "cvv", "debit card", "desjardin", "dump", "dumpz", "full info", "fullz", "hsbc", "mastercard", "moneygram", "paypal", "prepaid card", "rbc", "routing", "royal bank", "scotia bank", "td", "transfer", "venmo", "western union", "wu transaction", "zelle", "visa"
Counterfeit Currency	("authentic", "cf", "counterf", "fake", "undetect", "quality", "genuine", "light detector test", "pass pen", "pass uv", "passes pen test", "passes uv test") & ("aud", "bank bill", "bank note", "bill", "cad", "cash", "currenc", "dinar", "dirham", "dolas", "dollar", "euro", "frank", "gbp", "krone", "kuwaiti", "money", "note", "pesos", "pound", "rand", "ringgit", "rupee", "sterling", "usd", "yuan")
Malware/Software/Services	"account cracker", "account creator", "address changer", "anonymity tool", "anonymous vpn", "anti browser", "anti detect", "anti logger", "anti public", "anti viral", "anti virus", "bot", "brute", "bypass", "carding", "cpn profile", "crack", "crypt", "database", "ddos", "denial of service", "dox", "drop", "e-mail", "email", "exploit", "hack", "injection", "keylogger", "live track", "malware", "mega pack", "password hacking", "pentesting", "perl attack", "prox", "ransom", "rats", "rdp", "remote administration", "shell", "skim", "socks", "software", "source code", "spam", "spreader", "sql scanner", "tls", "trading bot", "trojan", "virus", "viruses", "vm workstation", "vpn", "vulnerability scanner", "worm",