Crime, Law and Social Change (2023) 79:263–289
https://doi.org/10.1007/s10611-022-10046-x

Media coverage of darknet market closures: assessing the impact of coverage on US search and Tor use activity

Eric Jardine[1] · Sarah Cruz[2] · Heather Kissel[3]

Accepted: 13 July 2022 / Published online: 27 August 2022

Abstract

Darknet cryptomarkets are a common method of drug procurement and are frequently a focal point for law enforcement intervention as a result. Past works assessing the effectiveness of cryptomarket closures by law enforcement have found a high degree of ecosystem resilience. Previous work, however, has not parsed the potential mediating role that official press statements and media coverage of such events might play on subsequent behavior. Using a new dataset of 27,195 distinct deterrent- or publicity-related sentiment-expressive signals taken from 406 media stories and 47 official press releases between 2013 and 2019, this article traces the potential impact of law enforcement closure of Darknet cryptomarkets on both US Google search activity and US Tor network use. The results generally show: 1) that discussion of certainty and severity of punishment, as deterrent signals, and sensationalism and market resiliency, as publicity signals, are the most forcefully expressed sentiments in the corpus of text; 2) US Google search interest in the Dark Web topic exhibits a fair degree of periodicity that is largely unassociated with the sentiment expressed in media coverage; and 3) US Tor anonymity network usage tends to be somewhat sensitive to how the closure is framed, with drops in Tor client connections in the US following comparatively high deterrence-coverage events and increases in the same following comparatively high publicity closures.

Introduction

Law enforcement takedowns of Darknet drug markets are eye-catching events. When law enforcement shuttered Silk Road in 2013, the first so-called cryptomarket (Martin, 2014), the affair was covered by *Wired* (Zetter, 2013), *USA Today* (Leger, 2013), *Gawker* (Chen, 2013), *The Guardian* (Arthur, 2013), and a host of other major

✉ Eric Jardine
eric.jardine@chainalysis.com

[1] Cybercrimes Research Lead, Chainalysis, New York, USA

[2] Virginia Tech, Blacksburg, VA, USA

[3] Department of Psychological Science, Northern Kentucky University, Highland Heights, KY, USA

media outlets. This coverage included strongly worded quotes from law enforcement. The quoted comments of the Director General of the UK National Crime Agency, Keith Bristow, are indicative: “the hidden internet isn’t hidden and your anonymous activity isn’t anonymous. We know where you are, what you are doing and we will catch you" (Arthur, 2013). Simultaneously, the coverage of the closure of Silk Road also raised public awareness of these markets, illustrated how to use Tor, summarized what sort of things were for sale on the site, and noted the tremendous financial opportunity that exists in the Darknet drug market ecosystem. Indeed, several works have noted the possibility that taking down cryptomarkets might raise awareness of their existence, and could by implication encourage their use (Buxton & Bingham, 2015; Décary-Hétu & Giommoni, 2017; Van Buskirk et al., 2014).

Media coverage of Darknet market takedowns, in other words, often sends both deterrence- and publicity-related signals to the general public. Moreover, the precise balance of media coverage and official statements might condition how narratives about these events are perceived. Strong deterrent sentiment, for example, could inhibit use of Darknet drug markets. Powerful publicity signals that raise awareness of Darknet markets or point to these sites as interesting, lucrative, and sensational settings could have the opposite effect, leading some people to become actively engaged with this sort of content. While the material effects of such engagement would largely depend upon the precise ways in which new users of the Darknet choose to act, strong publicity effects when spread across a large enough population could readily lead to negative outcomes for individuals, communities, and society writ large.

Yet, despite the importance of understanding how media and official statements portray Darknet market closures, several questions about the bifurcated nature this coverage and its potential effects remain unanswered: What is the balance of deterrence- and publicity-related signals within media coverage of Darknet market closures by law enforcement? Are there systematic differences between the official narrative (press releases) and media coverage of the same event in terms of the strength and nature of the signals sent? If so, what are these differences? Has the balance of coverage of these events shifted over time? Lastly, does the balance of coverage matter? Does comparatively high deterrent messaging in the wake of a particular takedown inhibit revealed interest and use of the Dark Web in a way that comparatively high publicity coverage does not?

We answer these questions using newly collected data on all Darknet markets taken offline by law enforcement agencies from 2013 to the end of 2019. The qualitative and quantitative data show that media coverage both reifies and augments with additional context the material present within official press releases. It also appears as though the relationship between Darknet market closures and Google searches is characterized by high degrees of periodicity, while media coverage might be more relevant than press statements when it comes to the after effects of closures on US Tor network use.

In the next section, we briefly summarize the literature on Darknet market takedowns and media presentation that motivated this study. The third section describes the data collection process, the structure of the data, and the analytical procedures. The fourth section presents the results of the analysis, with specific subsections for each descriptive trend under consideration. The fifth section presents a discussion of the implications of the results. The last section concludes.

Previous literature

Darknet markets offer users easy access to drugs, with enhanced anonymity, home delivery, and heightened perceptions of security (Hout & Bingham, 2013a, b; Masson & Bancroft, 2018; Van Hout & Bingham, 2014). As the Darknet market ecosystem has increased in size over time (Christin, 2013; Soska & Christin, 2015), these focal points of drug exchange have become a magnet for law enforcement policing efforts. Silk Road, for example, emerged on the Tor Darknet in February of 2011 and was shuttered roughly two and a half years later in October 2013. During the intervening period, the marketplace grew from a niche e-commerce site for illicit drugs with few vendors and customers into a site processing hundreds of millions of dollars in estimated revenue and inclusive of 8,733 vendors by the time of its shutdown (Kovach, 2013). Yet Silk Road, as big as it eventually became, remains small compared to what some contemporary markets have become. AlphaBay, for example, at the time of its closure in 2017, reportedly had 40,000 active vendors, according to official FBI statements (FBI, 2017), and was likely processing between $600,000 and $800,000 in revenue a day as a conservative estimation, even while it competed with other similarly sized marketplaces such as Hansa (Greenberg, 2017). More recent markets such as Hydra reportedly had millions of user accounts and billions in annual revenue (Glover, 2022).

Though there is some debate about the size and scope of cryptomarkets, this apparent growth in the Darknet market ecosystem has occurred despite persistent efforts by law enforcement to police this ecosystem and shut down these sites (Bradley, 2019; Décary-Hétu & Giommoni, 2017; Duxbury & Haynie, 2018; FBI, 2017; Jardine, 2015; Van Buskirk et al., 2014, 2017). Since the closure of Silk Road, for example, over a dozen additional marketplaces have been seized and shuttered by the FBI, Europol, the Dutch police, and a host of other participating law enforcement agencies. These outright closures occur alongside a number of additional measures targeting specific vendors, customers, and site users, including creative "knock and talk" operations leveraging data collected from previously commandeered servers to approach cryptomarket customers with the aim of dissuading future Darknet market use (Bradley & Stringhini, 2019; Jardine, 2021). Despite these efforts, activity within the Darknet ecosystem (as opposed to what happens on any individual market) has consistently rebounded to pre-takedown levels within a matter of weeks to months (Décary-Hétu & Giommoni, 2017), with somewhat more mixed evidence about the discernable effect on the rate of increase in market vendors (Décary-Hétu & Giommoni, 2017; Van Buskirk et al., 2017). The end result has been an ecosystem of illicit drug-related activities that has grown fairly consistently in size from 2011 to the present day (Christin, 2013; Dolliver, 2015; Martin, 2014; Paquet-Clouston et al., 2018; Soska & Christin, 2015), though most growth in revenue since 2019 has been due to the Russian market Hydra which was closed in April of 2022.

The interrelationship between law enforcement closure of these sites and patterns of recovery and ecosystem growth might be somewhat contingent on how these events are presented to the general public. Two separate effects might be at play: 1) a combined removal and deterrent effect and 2) a publicity effect. Efforts to police Darknet markets plausibly could lead to a reduction in use, as administrators, vendors, and customers are identified and removed from the system. Extending from these outcomes, the closure of these markets could send deterrent signals to the general public, dissuading potentially curious individuals from participating in the Darknet ecosystem. Indeed, during Operation Onymous in 2014, for example, most active vendors from three shutdown markets (CloudNine; Hydra; and Silk Road 2) appear to have been deterred from future vending (at least under the same handle) and did not displace to other markets such as Agora and Evolution (Décary-Hétu & Giommoni, 2017, p. 71).

At the same time, some portion of the demonstrable resilience of the Darknet market ecosystem could be a function of an equifinal sequence of events, running somewhat nonlinearly from law enforcement closure and official press statements, to media coverage and the dissemination of the story on social media sites such as Reddit. In this sense, law enforcement takedowns of Darknet markets might actually contribute to the growth of the Darknet market ecosystem by, in effect, propagating information about how to access the Tor Dark Web, publicizing the financial gains that are to be had within the space, and showcasing the wide range of items for sale or the interesting and sensational content at play. The Darknet ecosystem, then, might be in some measure not just resilient to takedowns, but actually "anti-fragile," in the sense that it might gain from disruption via an information propagation mechanism (Taleb, 2012).

The notion that media coverage and information propagation effects might increase the prevalence of the documented activity is seen in many domains. Media coverage of suicides, for example, can lead to increases in suicides, especially among youth (Gould et al., 2003; Ishii, 1991; Romer et al., 2006; Sinyor et al., 2018). Media depictions of events have also been linked to copy-cat school shootings (Johnston & Joy, 2016; Towers et al., 2015), murders (Cantor et al., 1999), and fluctuations in drug use behavior (Ma et al., 2017; Primack et al., 2009). Indeed, the volume of media coverage surrounding the conviction and sentencing of the Dread Pirate Roberts correlated with an increase in trade on the Darknet markets Evolution and Agora (Ladegaard, 2018).

Sitting at the intersection of technology and crime, media coverage of Darknet market closures might be motivated by more than simply the dry presentation of the facts contained within the official law enforcement press statements surrounding such events. For instance, the British press tend to portray the "Dark Web" in profoundly negative terms, often characterizing the technology as inherently linked to criminal activities (De-Oliveira-Sarda, 2020). Such portrayals link to older patterns of social and journalistic moral panics, which are especially prevalent in the case of stories regarding crime (Jewkes & Linnemann, 2017; Mawby & Gisby, 2009; Welch et al., 2002). They also fit well with the incentive structure of click-driven media, web-based analytics, and online advertisement, where sensational headings, content, and portrayals of events can maximize revenue, journalist status gain, and media product dissemination (Tandoc Jr, 2019). In keeping with these patterns, it might be reasonable to assume that the media would emphasize patterns that showcase the sensational elements of Darknet market closures, potentially even more than official press statements (amplification of the original narrative).

Plausibly, then, while Darknet takedowns per se might work against an expansion of the Darknet market ecosystem through removal and deterrence signaling, media coverage of these events might have the opposite effect in some measure, at least in some settings. And while some literature suggests that the increased attention focused on Darknet markets during the time of a police-driven shutdown might encourage market growth (Buxton & Bingham, 2015; Ladegaard, 2018; Van Buskirk et al., 2014), investigation of market-level features during a single law enforcement operation (i.e., Operation Onymous) has not unearthed much support for this type of publicity-driven effect over the short run (Décary-Hétu & Giommoni, 2017).

Past literature, however, has yet to adequately parse several potentially important dimensions of the takedown/coverage/and effect nexus. These facets have both descriptive elements and effect-based implications.

First, *in a descriptive sense*, it is unclear what types of deterrence and publicity signals are sent by official press statements and media coverage of law enforcement takedown events. Second, the comparative strength of these signals is unknown, both overall, across outlet types, and over time. Third, the ratio of deterrence-to-publicity signals within press releases and media coverage both by takedown and over time is not well documented nor understood.

Finally, in a more effects-based sense, it is unclear if the balance of media coverage of Darknet market takedowns matters for aggregate outcomes. Comparatively high publicity signal events, for example, may or may not lead to more demonstrable Dark Web-related activity and comparatively high deterrent signaling events might lead to a comparatively low level of post-event interest or activity. Outcomes such as these would suggest that media coverage of these events acts similar to stories of suicides (Ishii, 1991, Gould et al., 2003, Romer et al., 2006, Sinyor et al., 2018, mass shootings (Johnston & Joy, 2016; Towers et al., 2015), murder (Cantor et al., 1999) and drug use behaviors (Ma et al., 2017; Primack et al., 2009), all of which increase the prevalence of such events in the future.

Data and methods

To determine the disposition of media coverage of Darknet market closures by law enforcement, we constructed a new dataset inclusive of all fifteen Darknet markets that were known to be closed by law enforcement between October of 2013, when Silk Road 1.0 was taken offline, and the end of 2019.[1] In broad terms, the data include 54,382 (27,195 unique) sentiment-expressive sentences nested within

[1] These markets include: Alpaca, AlphaBay, Berlusconi, Cloud9, Hansa, Hydra, Pandora, Silk Road, Silk Road 2, Topix, Tor Bazaar, Utopia, Valhalla, and Wall Street Market. This list was partially extracted from the European Monitoring Center for Drugs and Drug Addition's *Darknet Markets Ecosystem* report: https://www.emcdda.europa.eu/system/files/publications/8347/Darknet2018_posterFINAL.pdf

406 media stories and 47 law enforcement press statements, all nested within six takedown operations.[2] Sentiment-expressive sentences in this case are whole lines that contain meaning relative to either deterrent or publicity effects. For example, a quote from law enforcement saying, “We will find offenders on the Dark Web,” is a sentiment-expressive sentence, capturing a deterrent signal. Filler lines or those that made purely descriptive claims, such as “Ross Ulbricht was from Austin, TX,” are not sentiment-expressive sentences and were not included in the dataset.

Data collection

The research team collected the initial corpus of media story URLs and law enforcement press releases. Media stories were collected via Google News. The team members collecting the articles had not previously researched the Dark Web or cryptomarkets and completed all searches while incognito, minimizing the risk of algorithmic sorting of stories by pre-existing profiles. To locate media stories, the research team date restricted the time range for returns to within 90 days of the takedown event and searched using the following generic search strings: “NAME market” AND “takedown” AND “Dark Web” OR “Darknet”; “NAME market” AND “police close” AND “Dark Web” OR “Darknet”; “NAME market” AND “police closure” AND “Dark Web” OR “Darknet”; “NAME market” AND “police shut down” AND “Dark Web” OR “Darknet.” The same search strings were also entered into Factiva; however, the returned articles were not sensitive to market name (the articles returned were the same regardless of market name) and contained many irrelevant articles (e.g., “AFM: Sharon Stone Joins ‘Darknet’ Ensemble”). As such, the data collection proceeded with those stories found on Google News as this source provided better coverage than other available alternatives.

From the resulting pool of returned media stories per search string, the research team pulled the top ten returns (unique per market) into the dataset. Only the top ten returns were chosen as 1) this is the default number of returns for Google News, 2) Google users rarely venture onto the second page of search results, and 3) a manual examination of the page 2 returns and beyond revealed many irrelevant articles and no articles from major new outlets, suggesting that the top ten returns provided a fairly high degree of completeness. These procedures resulted in a total of 406 unique media articles.[3] Official law enforcement press releases for the various operations were collected via a targeted search for the operation name and major law enforcement agency titles, such as the Federal Bureau of Investigations (FBI) or Europol, as well as key word searches of major law enforcement agency databases using operation names and date ranges. Forty-seven unique press releases covering all six law enforcement takedowns were collected via the process. Data were

[2] The major operations in the dataset are Operation Marco Polo, Operation Commodore, Operation Onymous, Operation Bayonet/GraveSac, Operation Darknet, and Operation SaboTor.

[3] Since some markets had fewer than ten relevant stories returned via the search procedures and some searches returned the same article for multiple markets, the total corpus of media accounts is less than the 600-story maximum that would result from selecting ten unique articles per market per search string.

collected between May 29, 2020 to August 12, 2021. Google News searches were repeated near the end of the data collection period to ensure that the top ten returns did not differ based on updates to Google's algorithm.

Data coding

After collecting the corpus of media articles and official press releases, the research team coded the expressed sentence-level sentiments within all 406 media stories and 47 official press releases. Media stories consisted of articles from major news outlets (e.g., The Guardian, n = 213), tech journalism (e.g., Wired, n = 165), and blogs/other (e.g., KrebsOnSecurity, n = 28). In total, the dataset consists of 54,382 non-unique sentiment-expressive sentences within the media coverage and 2,303 entries within the official press releases (see Table 1 for examples). Many of the sentiment-expressive sentences were non-unique, as they occurred across multiple different media articles and press releases, such as direct quotes from law enforcement officials or subject-matter experts. The data consist of only sentiment-expressive sentences, in the sense that the included lines convey some plausible deterrent or publicity meaning and were not merely connecting sentences or descriptive claims such as "Ross Ulbricht was from Austin, TX."

The data coding process consisted of two stages: 1) an initial categorization of a sentence as a specific deterrence or publicity signal type and 2) an assessment of the signal's strength on an ordinal scale from 1 (weakest) to 5 (strongest). Two members of the research team independently coded each article, extracting sentiment-expressive sentences, thematically categorizing this content, and coding each for expressed signal strength (see below for diagnostics). During the initial data categorization process, sentence-level signals were coded into either a) prefabricated deterrence or publicity signal buckets or b) generic "other deterrence" or "other publicity" categories, each of which was later parsed for thematic content until theoretical saturation was reached (Breckenridge & Jones, 2009).

The prefabricated deterrence categories included expressions of the 1) severity, 2) certainty, or 3) celerity of punishment, and were drawn from the classical criminological model of deterrence (Apel & Nagin, 2011; Kleck & Barnes, 2014; Kleck et al., 2005). The pre-set publicity categories included details on 1) how to access Tor/the Dark Web, 2) financial gains to be had in the Darknet ecosystem, 3) the low odds of getting caught when using Tor or Bitcoin/cryptocurrency, and 4) interesting available content/sensationalism. These categories were initially populated by the research team after a preliminary, non-systematic review of media coverage of the Darknet market takedowns. Following the initial categorization of the sentiment-expressive sentences into themes, the research team then scored each expressive morsel on an ordinal scale from 1–5.

The inclusion of other signal type categories for both deterrence and publicity allowed for additional inductive coding of the expressed sentence-level sentiments contained within the media coverage and official press releases in the dataset. Sentences that expressed some deterrent or publicity meaning but did not fall into one of the prefabricated categories were initially categorized by the research team as

Table 1 Example sentiment-expressive signal categorizations and signal strength coding

Signal Type	Strength Score (1–5)	Example
Select Deterrence Signals		
Severity of punishment	5	"Ulbricht has since been convicted to a double life sentence plus 40 years in prison."
Certainty of punishment	2	"They were identified via more traditional means and their activities linked to the market in such a way that defense seems a lost cause."
Celerity	4	"Authorities swept in quickly after the platform was switched into a "maintenance mode" on April 23, and the suspects allegedly began transferring funds used on the platform to themselves in a so-called "exit scam", Mr Ungefuk said."
Select Publicity Signals		
Financial Opportunity	5	"A conservative estimation of USD 1 billion was transacted in the market since its creation in 2014."
Libertarian principles	3	"This is so f…ed up man, we have the right to do whatever we want to our bodies."
Interesting Content/Sensationalism	5	"It offered interfaces in six languages – English, French, German, Italian, Portuguese and Spanish – and numerous separate categories for merchandise, including drugs, jewellery, equipment and support for credit card fraud, software and malware, among others."

"other" and given a signal strength score. Once data collection was complete, the research team later parsed these data to formulate six additional deterrent signals that might inhibit people from exploring the Dark Web or using drug cryptomarkets (e.g., Opsec errors; Personal risk; Exit scams; Links to opioid epidemic and the war on drugs; Not user friendly; and Immoral or poor-quality goods and services). The research team likewise induced four publicity-related themes that could plausibly encourage people to use Tor, the Dark Web, or Darknet markets (e.g., A tech savvy community; Dark Web markets follow libertarian principles; Market ecosystem resiliency; and the Positive, rights-based uses of Tor). Table 1 summarizes some non-exhaustive examples of various expressed sentiments and their respective signal strength coding (see the Qualitative Themes section below for more details).

The two research team members who collected and thematically coded the data were extensively trained on the coding procedures prior to beginning their work. Before beginning the final data analysis, the coders also met and reconciled the categorization of each signal. This reconciliation process involved a discussion between the research team members of each discrepant coding decision relative to the initial coding guidelines. In each case, the discussion continued until a consensus view was obtained. The result of this process is that the percent agreement for each initial thematic categorization (e.g., "severity" under the deterrence umbrella) was 100%. The coders then randomly selected 10% of the total articles and reconciled any differences in the assigned signal strength by deliberating until consensus was reached. Interrater reliability was calculated per category; kappa ranged from 0.40 to 0.88, indicating fair to almost perfect agreement. Given the consensus procedures and high overall agreement between the coders, the scores across the two research team members were averaged to produce a single final sentiment-expressive sentiment score.

Finally, to assess the potential material impacts of takedowns and coverage on Tor/Dark Web-related activities within the United States, the research team collected two additional sets of data. The first data type is query search volume data from Google Trends, which is a population normalized measure of search interest in a particular term or topic (Chen et al., 2022; Jardine & Lindner, 2020; Lindner et al., 2020; Lindner & Xiao, 2020). In particular, we collected data on the search topic "Dark Web", which is an opaque bundle of correlated Dark Web-related search terms as defined by Google. These data were standardized relative to the global peak for the 2013–2019 period in order to adjust for changing underlying patterns of absolute search volume over the study period (Jardine & Lindner, 2020). The second data type is Tor relay client numbers for the United States, collected from the Tor Project user metrics page (Project, 2018). Both sets of data were collected for a total of 90 days on either side of a particular Darknet market shutdown date.

Data collection to measure potential behavioral changes in response to takedowns/coverage was restricted to the US for three primary reasons. First, most of the media outlets in the sample are English speaking papers and online blogs. This feature of the sample should suggest that resonance and uptake of the narratives being presented should be strongest in English speaking locations, such as the United States. Second, US law enforcement, especially the FBI, often played a major role in most Darknet market closures in the data. This implies that most Darknet market closures would have some relevant US angle to them. Third, the US is often a major player in Darknet drug related activities (Aldridge & Décary-Hétu, 2016; Décary-Hétu et al., 2016; Demant et al., 2018; Soska & Christin, 2015; Van Buskirk et al., 2016). These geographically specific features suggest that if coverage of Darknet market takedowns have an observable effect on people's behavior, they are most likely to be easily observed within the United States, given its centrality to the Darknet market/takedown dynamics at play.

Results

We analyze the data in five ways. First, as the original sentiment-expressive sentences are textual, we present an initial thematic analysis of these data as qualitative statements, anchored in a comparative sense of their median signal strength. Second, as little is known about the actual descriptive parameters of media coverage of Darknet market takedowns in quantitative terms, we aggregate and tabulate the data into market, takedown operation, and population totals. Third, we plot the signal type (e.g., type equals celerity of punishment) percentage share of the cumulative total for each sentiment-expressive signal category (e.g., category equals deterrence) for both media coverage and official press releases. This process allows us to see how the balance of coverage both a) changes over time and b) varies between unofficial and official sources. Fourth, we construct a standardized and logged deterrence-to-publicity ratio and plot this value over time across the full population of takedown events. This measure shows whether deterrence or publicity predominates in the coverage surrounding any given takedown operation and whether the preponderance of coverage/signals sent varies over time. Finally, we present two measures to assess whether the balance of coverage might have an effect on revealed interest in the Dark Web (via Google Trends) and revealed engagement with the Tor anonymity network (via US Tor relay client connections). We plot an interrupted time series for each measure of Dark Web-related activity to show the effect of a takedown on each type of activity across each discrete law enforcement operation, though the small number of takedown operations strongly suggests that this analysis needs to be interpreted with caution.

Qualitative themes

A number of interesting thematic findings emerged from the review of the sentiment-expressive sentences contained within the data. One interesting place to start is with the "other signal type" category, which was an initial broad bundle of sentiment-expressive terms that did not fit into any of the pre-established categories. When examining these classifications as they relate to deterrent signals, subthemes emerged for each of the larger bucketed categories. For example, the broader "Personal Risk" category encompasses a multitude of risks users might experience when accessing the Darknet generally or cryptomarkets more specifically. These risks include worries such as having their devices hacked, the risk of Bitcoin theft, and extortion attempts by nefarious actors within the Darknet ecosystem, including other market participants.

The emergent "Opsec Errors" category includes signals that describe poor operational security measures by cryptomarket administrators, such as specific slights ("He continued: Ross was an absolute cement-head, when it came to security" [Strength Score = 3]) or descriptions of how their mistakes led to their downfall (e.g., improperly configured VPNs, or registering servers under a personal email address). This sort of expressed sentiment also substantiates ecosystem-wide events. For example, the identity of Ross Ulbricht, the founder of Silk Road, was ultimately discovered due to his use of a Gmail email account on a Bitcoin market forum in the earliest days of the marketplace (Jardine, 2021).

Signals concerning the practice of administrators "absconding" with cryptomarkets users' bitcoins were included in the "Exit Scams" category ("In fact, its competition has largely collapsed over the last week: Over the past weekend the administrators of the Sheep Marketplace absconded with as much as $100 million of its users' bitcoins and took their site offline." [Exit scam: Strength Score = 3]). The "Links to the opioid epidemic and war on drugs" category contained signals decrying the War on Drugs as a failure ("Cryptography and cryptocurrency are out of the bottle, and the war on drugs is even more hopeless than it always was." [Strength Score = 3]) or the description of tragic deaths that occurred due to the purchase of illegal narcotics on cryptomarkets and the need for intervention ("Additional victims included Bryan B., a 25-year old from Boston, Massachusetts, and Scott W., a 36-year old from Australia, who both died as a result of heroin purchased from Silk Road, and Jacob B., a 22-year old from Australia, who died from health complications that were aggravated by the use of drugs purchased from Silk Road." [Opioid epidemic: Strength Score = 5). Interestingly, these expressed sentiments are at variance with the views of most Darknet drug market users, who tend to find drug exchange via these sites to be far preferable than alternative modalities of drug procurement (Barratt et al., 2016).

Difficulties with cryptocurrency, the transient nature of many Tor sites ("It was observed that the vast majority of Tor sites exist for only a matter of days or weeks before vanishing." [Not User Friendly: Strength Score = 3]), or the poor design and confusing URLs of Darknet markets sites ("Using their website feels like I'm playing around on some 15 year olds MySpace page." [Not User Friendly: Strength Score = 3]) characterized signals in the "Not user friendly" bucket. Many articles also mentioned items for sale on the Dark Web that most American readers would shy away from accessing, such as child pornography ("By monitoring dark web activity over six months, it was found that 80% of traffic was to websites hosting images of child abuse, although the most popular category by page volume was the sale of illegal drugs." [Interesting content/Sensationalism: Strength Score = 1]), murder-for-hire, and terrorism.

Beyond the parsed deterrent "other signal type" categories described above, additional publicity-related categories emerged from the corpus of text as well. Contrasting the "Opsec Error" category, some stories suggested that the Dark Web could provide individuals with access to a "Tech savvy community" (e.g., "tech savvy drug enthusiasts actively discuss the drug markets through dedicated subreddits and other online forums, asking for dealer recommendations, hammering vendors with bad reviews and discussing security concerns" [Strength Score = 2]). Users and administrators of cryptomarkets also express "Libertarian principles," with Silk Road creator Ross Ulbricht describing the site as an "economic simulation to give people a first-hand experience of what it would be like to live in a world without the systemic use of force" [Strength Score = 3]. In both instances, expressed sentiments could create the perception of an alluring counter-culture to mainstream politics, economics, and society, potentially stimulating interest in the Dark Web and drug markets in particular, though the occurrence of this sort of political dialogue on these sites has declined over time (Munksgaard & Demant, 2016).

Despite the takedowns as outlined in the media coverage and press releases, many signals suggested "Market ecosystem resiliency," with law enforcement stating after a takedown that "despite this positive achievement, those involved in the online drug trade appear to be resilient to such disruption and able to re-organise rapidly." These expressed sentiments mirror empirical investigations into Darknet market activity following major law enforcement actions, which tend to show a rapid recovery in total vendors, sales, and listing across the ecosystem following the closure of one or more markets (Décary-Hétu & Giommoni, 2017; Van Buskirk et al., 2014, 2017).

Lastly, some articles described the history of Tor and its development by the U.S. government, leading into its modern "Rights-based uses." These rights-based functions include those that allow dissidents and citizens “to circumvent the censorship of certain countries” and to protect “journalist and activists…from repressive regimes and intrusive intelligence agencies.” As with many of the other emergent thematic categories that came out of the corpus of sentiment-expressive terms, the detailing of these positive use cases of the Dark Web fits with the findings of country-level empirical investigations into how political repression associates with the use of the Tor network (Jardine et al., 2020; Jardine, 2018b).

The quotes provided for each of the “other deterrent” and “other publicity” categories come from each of the four coverage types included in the dataset. In examining articles from the two broad categories wholistically, the media coverage and official press releases reporting on darknet market takedowns differed stylistically, with press releases tending to be shorter in length and focused on the “facts” (e.g., specific charges and sentences, dollar amounts and lists of items seized, etc.), while the media coverage contained specific narratives (e.g., how the authorities were able to gather the evidence and perform their takedown operations, or reports of the “courtroom drama” type). Stylistic differences also occurred within the three different subcategories of media coverage. Articles from tech journalism outlets tended to be the longest and most detailed, while the “other” (e.g., blogs) reports might mention a takedown tangentially and focus instead on personal experiences on the Dark Web or provide “how to” guides to accessing the deep vs. Dark Web.

These stylistic differences impacted both the kinds of signal each type of article sent as well as the strength with which certain sentiments were conveyed (see Fig. 1). When contrasting media stories and press releases, on the primary prefabricated deterrence categories (i.e., severity, certainty, and celerity of punishment), there are few notable differences in the strength and balance of the scores. For “severity of punishment,” signals from both media coverage and press releases discussed specific charges and sentencing; for example, a press release about the Silk Road takedown stated, “In addition to the life sentence prison term, ULBRICHT was ordered to forfeit $183,961,921” [Severity of Punished: Strength Score = 5]. Media coverage largely included quotes from law enforcement to convey “certainty of punishment” (“No matter where they live, we will investigate and prosecute criminals who create, maintain, and promote dark web marketplaces to sell illegal drugs and other contraband” [Certainty of Punishment: Strength Score = 4]), while press releases provided metrics related to their operations (“Overall more than 38 000 transactions have been identified and Europol sent more than 600 communications.” [Certainty of Punishment: Strength Score = 3]). To express “celerity of punishment,” both media coverage and press releases emphasized the speed of law enforcement action, though media coverage tended to dramatize this swiftness (e.g., “But a series of arrests this month, including the bust of the black market site Silk Road, shows the G-men have infiltrated the Internet’s back alley.” [Celerity of Punishment: Strength Score = 3]).

While the deterrence categories had very similar tone and signal strength, some of the publicity-related and “other signal type” categories had wider variation between outlet types. Within the prefabricated publicity-related categories, “Accessibility” was similar in terms of the median strength of the depiction of events, but the media tended to have more strongly worded outliers than official press statements.

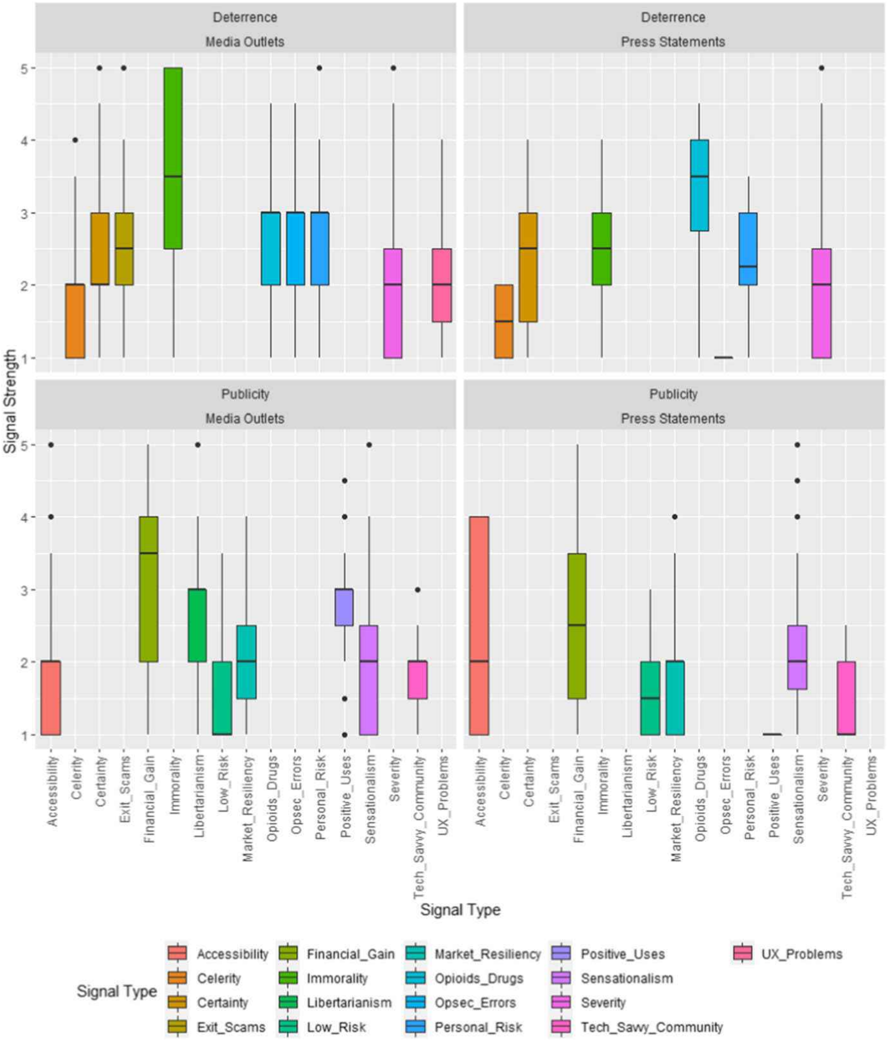

Fig. 1 Signal strength by type, category and outlet type

Comments within this category include descriptions of Tor's functionality or even specific URLs (e.g., "Addresses on the Tor network follow the form of a random string of letters followed by the.onion suffix, like this link to a Deep Web directory: allyour4nert7pkh.onion." [Accessibility: Strength Score = 5]). Press releases express "Low risk" only mildly and often in past tense to emphasize a sense of neutralization, "Silk Road enabled its users to buy and sell drugs and other illegal goods and services anonymously and outside the reach of law enforcement" [Low Risk: Strength Score = 1]. However, media coverage often describes why and how using Tor and cryptocurrency is low risk more commonly in the present tense, such as in this signal from a tech journalism outlet: "Even the NSA can't break the technology, though they've tried, according to new documents revealed by the Guardian" [Low Risk: Strength Score = 4]. Press releases mention "financial gain" from Darknet cryptomarkets tangentially, only including monetary values to emphasize the scale of the operation: "A conservative estimation of USD 1 billion was transacted in the market since its creation in 2014" [Financial Gain: Strength Score = 5]. Media coverage sensationalized both the amount of money to be made ("Yes, that's 'billion' with a 'b,' and all those sales allegedly generated 600,00 Bitcoins for Silk Road itself." [Financial Gain: Strength Score = 4]) and the luxurious lifestyles of administrators ("Alexandre Cazes was just 25, but according to U.S. government documents he was the alleged mastermind behind AlphaBay, the most profitable dark web marketplace in the world, and a millionaire who owned luxury cars and multiple properties in Thailand, Cyprus and Antigua." [Financial Gain: Strength Score = 4]). As with "financial gain," press releases mention "interesting content" available on cryptomarkets only to emphasize scale: "For example, as of September 23, 2013, there were: 159 listings under the category "Services," most of which offered computer hacking services, such as a listing by a vendor offering to hack into social networking accounts of the customer's choosing; 801 listings under the category "Digital goods," including malicious software, hacked accounts at various online services, and pirated media content; and 169 listings under the category "Forgeries," including offers to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of false identification documents" [Interesting/Sensational Content: Strength Score = 5]. Media coverage also frequently contained these kinds of laundry lists of available items ("Launched in early 2014, Evolution is now considered the largest dark web market; at the time of publication it had more than 15,000 items for sale, including 11,600 drugs, 540 counterfeit documents such as passports and driving licenses, 213 weapons—including an Uzi submachine gun with ammunition—and 34 listings for laboratory supplies such as chloroform, and a machine capable of manufacturing 3,000 pills per hour." [Interesting/Sensational Content: Strength Score = 5]), but imbue excitement into their descriptions.

Within the "other deterrent" and "other publicity" signal categories, there are some categories not discussed at all in press releases, but which occur frequently in media coverage. These are: 1) Dark web markets follow libertarian principles; 2) Tor is not user friendly; and 3) exit scams. The exclusion of any mention of difficulties using the Dark Web or the occurrence of exit scams in press statement may be surprising given their plausible deterrent nature, but the tone of the press releases emphasizes active law enforcement efforts and their success. The mention of additional impediments to Dark Web use may dilute this messaging. Additionally, law enforcement is likely unconcerned with the principles driving those involved with illegal drug exchange, so the lack of mention of libertarianism is expected.

Of the remaining "other" signal categories, discrepancies between media coverage and press releases are most noticeable for "Links to the opioid epidemic and war on drugs" and "Positive, rights-based uses of Tor." As mentioned above, signals for the "Links to the opioid epidemic and war on drugs" category took two forms, 1) criticism of the War on Drugs and 2) descriptions of tragic overdoses and the need for continued intervention. Mainstream media coverage often includes quotes from politicians and law enforcement about the necessity of the War on Drugs: "Attorney General Jeff Sessions said, 'The ability of these drugs to so instantaneously end these promising lives is reminder to us of just how incredibly dangerous these synthetic opioids are, especially when purchased anonymously from dark spaces on internet, and this is likely one of the most important criminal investigations of this entire year'" [Opioids: Strength Score = 3]. Tech journalism and other media types like blogs were more varied in their perspectives: tech journalism acknowledged the risks associated with synthetic opioids, but like with the other media genres, often included quotes from Darknet market users who disparage the efforts and effects of the War on Drugs.

Regarding the "Positive, rights-based uses of Tor" category, only one press release contained any mention of this ("Tor is used by a variety of people for both illicit and licit purposes, a fact that has also been acknowledged in the complaint against Ross William Ulbricht, accused of being the main administrator of the original Silk Road." [Positive Uses of Tor: Signal Strength 2]). In contrast, all forms of media coverage provided examples of legal and potential rights-based motivations to access the Dark Web. In this sense, media coverage tends to emphasize aspects of the Dark Web that are broader in both domain (wider than just crime or drugs) and geography (use cases that apply more in countries that are highly repressive as opposed to democratic) (Jardine et al., 2020).

These qualitative themes can also be considered in quantitative and aggregate terms. Table 2 presents basic descriptive statistics for the data, with signals aggregated into the largest sentiment-expressive category levels (i.e., deterrence or publicity) and all outlet types combined together. The table includes descriptive statistics for both the whole sample as a pooled cross-section and discrete metrics for each takedown operation ($n = 6$). Overall, both the full sample and each respective takedown tend to have similar measures of central tendency and variance on both deterrence and publicity, clustering near to a mean score of between 1.75–2.21 on the 5-point scale and a standard deviation of between 0.76 and 1.05.

For both the full sample and in the coverage surrounding each respective takedown, the total sum of the deterrence signals sent by media coverage are greater than the publicity signals, suggesting a generally dissuasive overall tone to the coverage. There is, however, a significant amount of variation between the respective takedown operations in terms of the total sum of signals by sentiment-expressive category. Since the total sum of each sentiment-expressive signal category is sensitive to the number of markets taken offline, the last column in Table 2 presents a simple normalization of the total sum per signal category divided by the number of markets shuttered in each takedown operation. This data transformation helps to facilitate comparison between single market and multimarket events. Generally speaking, even after accounting for the number of markets closed, takedowns that target single, smaller-scale markets, such as Operations Commodore and Darknet, generate fewer signals overall than those targeting two or more markets (Operations Onymous, Bayonet/GraceSac, SaboTor). The first takedown, Operation Marco Polo, is a clear outlier as it involves only a single market closure (i.e., Silk Road) and has the highest normalized volume of signals for both of the deterrence and publicity categories. This result is suggestive of the idea that early coverage during the cryptomarket era was potentially more expressive than later coverage.

Table 2 Descriptive parameters of the aggregate data overall and by takedown

	N	Min	Max	Mean	SD	Total Sum	Market N Weighted Total Sum
Overall (Deterrence /Publicity*)	15,647 11,548	1 1	5 5	2.18 2.00	0.93 0.93	34,034 23,052	2,268.93 1,536.80
Descriptive Statistics by Takedown							
Operation Marco Polo	1,884 1,429	1 1	5 5	2.21 1.99	0.88 0.96	4,162 2,839	4,162 2,839
Operation Commodore	330 246	1 1	5 4	1.86 1.75	0.76 0.79	614 430	614 430
Operation Onymous	6,940 6,005	1 1	5 5	2.21 1.95	0.93 0.89	15,366 11,690	1,920.75 1,461.25
Operation Bayonet/GraveSac	2,953 1,596	1 1	5 5	2.21 2.09	1.00 0.98	6532 3328	3,266 1,664
Operation SaboTor	2,987 1,808	1 1	5 5	2.10 2.10	0.87 0.97	6,272 3,804	3,136 1,902
Operation Darknet	553 464	1 1	5 5	1.96 2.07	0.90 1.05	1,086 962	1,086 962

* A note on table interpretation. The upper left quadrant of each cell is the deterrence score for each descriptive parameter, while the bottom right quadrant is the publicity signal score for each

Relative share of signals by time, type, and outlet

Figure 2 presents the trend in the relative density of signal types over time by both outlet (media vs. press statement) and signal category (deterrence vs. publicity). A few trends are notable. First, within official press statements, the presentation of the three component parts of deterrence (severity, certainty, and celerity) have markedly changed over time. Interestingly, in the earlier years of the data (up until about 2015), severity and certainty were referenced with comparative frequency. Over time, however, references to celerity of punishment have steadily increased and seem to have come at the expense of references to severity and certainty. This metamorphosis might imply a narrative shift, from oblique references to catching and punishing offenders toward statements that emphasize the immanence of law enforcement action. It is also notable that this pattern from within official press statement is not represented within media coverage, where the relative proportion of all three components of the traditional deterrence equation are both less frequent overall and follow more idiosyncratic patterns.

It is also interesting to note how media coverage tends to both reify the content of official releases and add additional contextual dimensions, across both the publicity and deterrence thematic categories. Within the publicity category, for example, media coverage

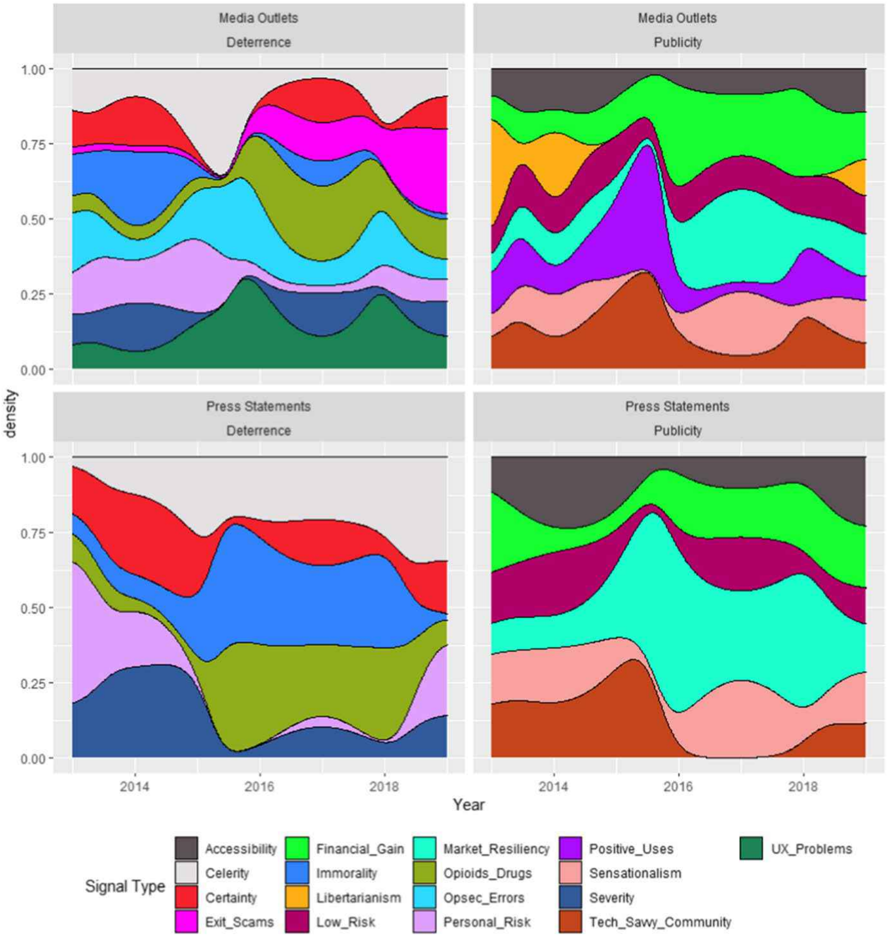

Fig. 2 Relative proportion of signals over time by type and outlet

clearly adds contextual overlays on top of the informational content of official releases. Most notably, media tends to heavily discuss (as seen above) both the positive uses of Tor and the linkage between libertarian political philosophy and Darknet cryptomarkets, neither of which appear within the corpus of text from official releases. Likewise, the media adds new potential deterrent elements, such as operation security errors, general UX (user experience) failures, and exit scams, to the narrative arch of the closure of these markets.

A standardized logged deterrence-to-publicity ratio over time

The trends over time presented above show how the presentational elements of Darknet market closures have changed from the first closure in 2013 through 2019. However, these numbers cannot express what the balance of coverage happens to be. Figure 3 presents an aggregated standardized log deterrence-to-publicity ratio by

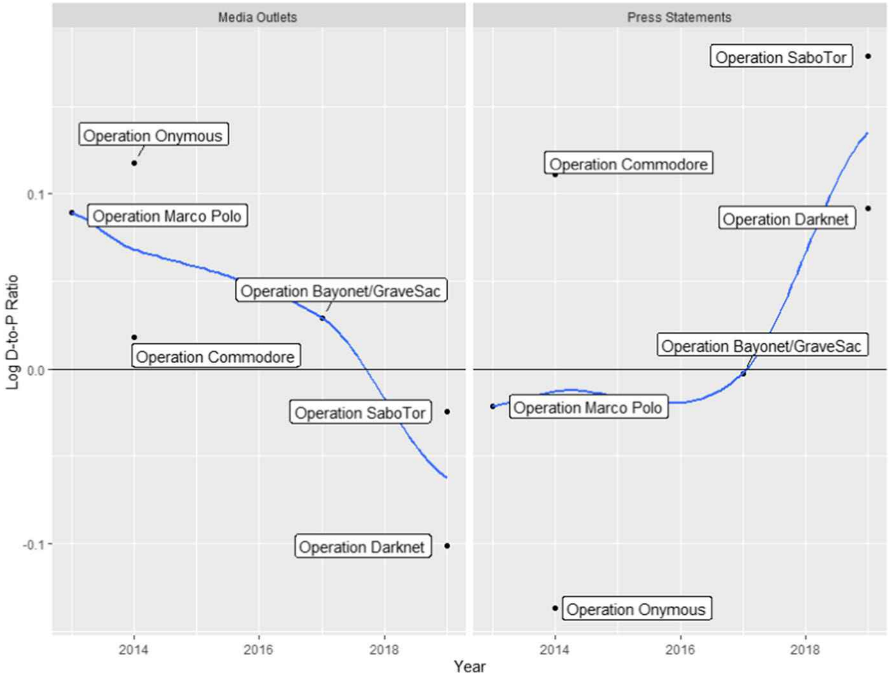

Fig. 3 Log deterrence-to-publicity ratio over time/media type

law enforcement takedown operation. These data indicate the standardized relative prevalence of deterrence or publicity signaling over time and by takedown for all available modes of coverage. Standardization was completed by dividing the sum of assigned signal scores by the sum of the maximum scores possible. This procedure helps to accommodate for the fact that some closures (e.g., Silk Road during Operation Marco Polo) are very well covered, while others (such as Operation Darknet) have fewer media accounts written about them. The logged ratio transforms the data so that a zero indicates equal signaling strength.

Figure 3 depict the standardized log deterrence-to-publicity ratio for each takedown operation separated by coverage type, with media coverage represented in the left pane and official press releases shown on the right. This disaggregation demonstrates that media coverage and press releases have sent a discrepant balance of signals about these operations. Media coverage of Operation Marco Polo favored deterrence (0.09), while official press releases trended slightly towards publicity (-0.02). This discrepancy was most pronounced for Operation Onymous, with media coverage favoring deterrence (0.12) and press releases favoring publicity (-0.14). However, the coverage for Operations SaboTor and Darknet demonstrated an opposite pattern of divergence, with media outlets sending a preponderance of publicity signals (-0.02, -0.10) and official statements stressing deterrence (0.18, 0.09, respectively). For Operation Bayonet/GraveSac, media coverage sent marginally more deterrence signals (0.03), while press releases sent an approximately equal balance of deterrence and publicity signals (-0.002). Only for coverage of Operation Commodore did media outlets and press statements converge in the sending of primarily deterrent signals; however, press statements displayed a greater ratio of deterrence to publicity signals (0.11) than media outlets (0.02).

It is also notable in Fig. 3 that the trend in the ratio of sentiment-expressive terms have trended in opposite directions. Media coverage has grown increasingly publicity oriented, with the two most recent closures (Darknet and SaboTor) having the strongest balance of publicity signals. In contrast, official press releases by law enforcement have exhibited the opposite trend, coming far more expressive of a preponderance of deterrent signals over time. This divergence might reflect media becoming more enmeshed in click-drive ad incentives (Tandoc Jr, 2019), leading to more attention on the sensational elements of these markets and their closure, and law enforcement getting increasingly confident that they can effectively police these sites (Jardine, 2021), resulting in more stringent statements about punishment and arrest.

Measuring impact (Google Trends)

Figure 4 plots the trend in a standardized Google Trends score for 45 days on either side of each respective takedown to investigate the potential material impact of law enforcement takedown operations on revealed interest in the Dark Web within the United States. Google Trends can be used as predictive metric in a number of circumstances (Ayers et al,, 2009; Chen et al., 2022; Choi & Varian, 2012; Jardine & Lindner, 2020; Nuti et al., 2014; Seifter et al., 2010). The GT scores are standardized to accommodate for the fact that underlying search volume for terms related to the broader topic of the Dark Web have increased over time.

The closure of Darknet markets does seem to generate additional Google Search activity within the US in many cases, but these increases tend to follow the events with the highest aggregate log deterrence-to-publicity ratios (see pane 1 in Fig. 3). Operations Marco Polo in October of 2013 (Silk Road market), Commodore in February of 2014 (Utopia market), Onymous in November of 2014 (Multiple Markets), and Bayonet/GraveSac in July 2017 all exhibit sizeable and discrete jumps in search activity, but are also those takedowns with the highest log deterrence-to-publicity ratios. Some of the later takedowns exhibit a different pattern, with either no discernible change in search behaviors (e.g., Operation Darknet in Sept. 2019) or even a reduction in interest (e.g., Operation SaboTor in March 2019). In the case of Operation SaboTor, the takedown actually corresponds with discrete drop in US based search query volume for the Dark Web.

Generally, these data suggest that Google search activity is not sensitive to the relative balance of coverage and is, instead, subject to a high degree of periodicity. The oldest takedowns exhibited the largest jumps in US-based search activity associated with the topic of the Dark Web. That novelty effect seems to have lasted for about four takedowns, following which additional takedowns generate less new interest in the wide topic of the Dark Web compared to the preceding 45 days.

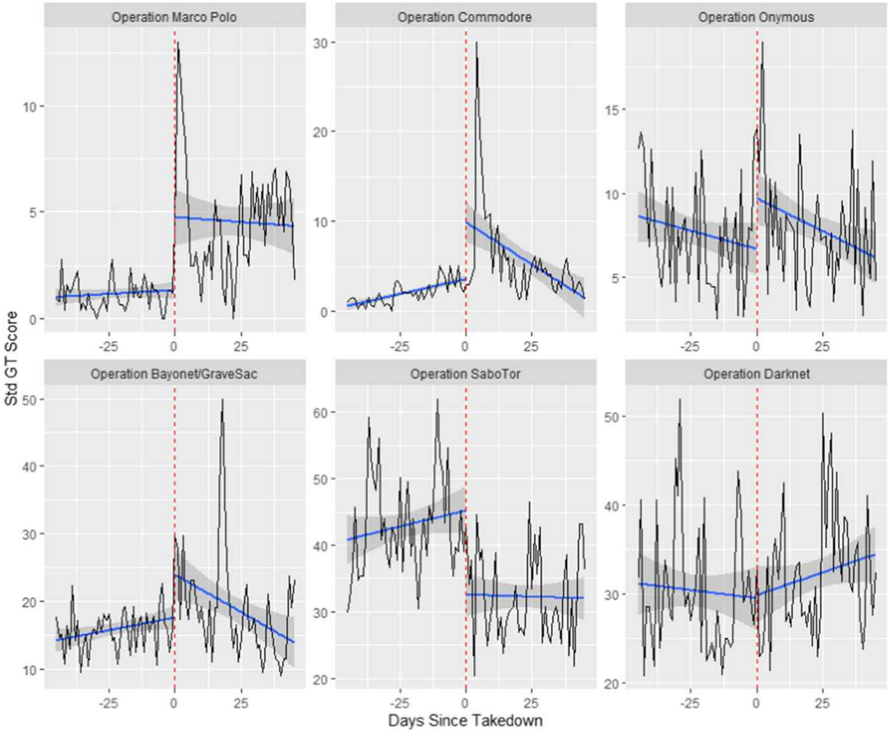

Fig. 4 Google trends scores by takedown operation (45 day intervals) standardized GT scores with 0.9 confidence intervals

Measuring impact through US Tor relay clients volume

Figure 5 plots daily US Tor anonymity network client data, centered around the publicly known date of each respective Darknet takedown operation by law enforcement. A couple of closures (e.g., Operations Macro Polo, Onymous, and Darknet) exhibit a clear discrete drop downward in US Tor client connections. The pattern in the other takedown operations in the dataset, however, is less clear, with three interventions (i.e., Operations Commodore, Bayonet/GraveSac and SaboTor) actually leading to a modest increase in the number of US Tor network clients.

The core prediction from a balance of coverage framework would be that closures with a high logged deterrence-to-publicity ratio should see a reduction in Tor network connections, while the opposite could be true of relatively low scores on this measure. Interestingly, media coverage and press statements have divergent patterns on the log ratio, granting an opportunity to, with caution due to the small number of cases, see whether media coverage or official statements are correlating with outcomes in this case. As seen in Fig. 3, media coverage suggests that the two closures with the highest log ratios are Operations Onymous and Operation Onymous. The log ratio within press coverage presents an opposing picture, with these two interventions having the highest relative publicity score in the dataset. As shown in

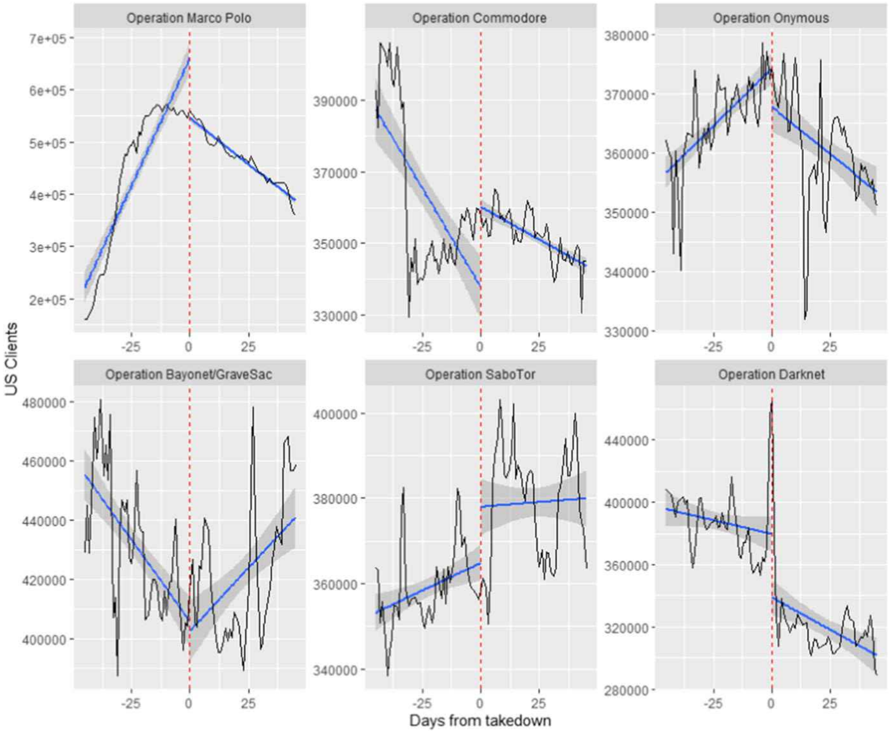

Fig. 5 US Tor use by takedown (45 day intervals) standardized GT scores with 0.9 confidence intervals

Fig. 5, both of these closures actually see reductions subsequent reductions in Tor network connections, suggesting the disposition of media coverage might be more determinative of outcomes than the content of press statements. Media coverage also suggests that SaboTor and Darknet have the highest relative balance of publicity, and, in one of the two, Tor network connections do indeed spike upwards after the closure. Overall, however, the small number of cases limits any inferences that can be made here and, in any event, the score on the logged ratio only really fits expectations in two cases, with Tor network activity exhibiting more idiosyncratic patterns in the other four.

Discussion

The current results illuminate several facets of the nexus between cryptomarket closures, media coverage and the response of the public in the US. The Darknet market ecosystem tends to be highly resilient to takedowns, recovering the majority of user and activity levels within a few weeks-to-months after the closure of any given market or set of markets (Décary-Hétu & Giommoni, 2017), even in the wake of high profile sentencing events surrounding the Dread Pirate Roberts (Ladegaard, 2018). The baseline findings suggest that law enforcement efforts to close Darknet markets are potentially effective crime management approaches (Jardine, 2015, 2021), but have potentially less utility as a deterrent instrument.

The current data and results nuance these findings in several ways. First, potential Darknet market users have clear informational needs, such as learning how to download Tor, unearthing cryptomarket addresses, and determining which market to visit for what purpose (Chen et al., 2021; Haasio et al., 2020; Jardine, 2021). The finding of increased US-based search interest in the topic of the Dark Web could be interpreted as at least partial support for the idea that closures, especially more historical ones like during Operations Marco Polo and Commodore, raise the publicity of Tor and the Darknet market ecosystem in a way that could potentially expand the pool of latent or potential Darknet market users. Over time, as new potential users collect more information through search and engagement with social media forums on platforms such as Reddit, it is possible that some fraction of this previously unaware population would then convert into new Darknet market users. The precise conversion rate is unclear and the strong counterfactual (i.e., that people would not have become Darknet market users absent exposure to coverage about a closure) might be too restrictive. A gentler version of the idea would be that coverage of Darknet market closures might increase the speed with which motivated offenders would walk through the initial information dimensions of the Darknet market crime script to become cryptomarket participants (Jardine, 2021). In either case, closures are associated with spikes in Web search in many cases and would likely increase the informational awareness of the population, suggesting that part of the reason why the Darknet market ecosystem remains resilient is that it is in fact anti-fragile due to an information propagation mechanism.

The data also suggest that some closures cause a spike in search interest overall, but that this pattern is largely driven by earlier takedowns such as Operations Marco Polo, Commodore, Onymous and Bayonet/GraveSac. This emergent pattern suggests some clear periodicity to the data and might suggest that the US population's general informational needs with regards to Darknet markets have become saturated over time. Such a saturation may imply that Google search as a novel discovery mode has become potentially redundant or at least of less value after 2017, when Darknet markets started to become more well known. This nuance implies that early closures would have rapidly raised the public profile of the Dark Web and drug cryptomarkets in particular, but that the effect has modulated into the present in such a way that additional coverage or publicity surrounding takedowns does little to foster new public interest in the ecosystem.

Another interesting finding with myriad implications is that closure of Darknet markets by law enforcement tend to suppress US Tor network usage in some cases. Of course, the total population of law enforcement operations during the study period remains small ($n = 6$) and care in interpretation is warranted. Nevertheless, it might be telling that the two takedown operations with the highest log deterrence-to-publicity ratios within media coverage both resulted in discrete reductions in US Tor client connections. Interestingly, too, unlike the rapid recovery of the Darknet ecosystem per se (Décary-Hétu & Giommoni, 2017; Soska & Christin, 2015), US Tor client connections do not recover to pre-takedown levels even after 45 days post-closure in these two cases.

One potential mechanism that might be at play is a generalized deterrent effect that could be reaching beyond the narrower confines of real and potential cryptomarket users. Presenting an image of certain punishment, severe sentences, swift justice, and a host of other deterrent dimensions may generally dissuade people from using Tor in the US. However, just because daily US Tor use declines after a given Darknet market closure, does not necessarily entail that those who are being deterred from connecting to Tor would be the same as those who would be inclined to use a Darknet cryptomarket. Indeed, the co-occurrence of both the rapid recovery of activity in the Darknet market ecosystem (Décary-Hétu & Giommoni, 2017; Soska & Christin, 2015; Van Buskirk et al., 2017) and the persistent reduction in US Tor network usage following high deterrence signaling events suggest that those who drop out of the Tor system may not in fact be the primary Darknet market using population.

Two other broad potential blocks of Tor users might make up the population that is being dissuaded from use post-closure. The first would be a group of largely benign users, who might leverage Tor as a tool for privacy-protection, censorship circumvention, or free expression (Jardine, 2018a, b). The Tor anonymity network is not itself illegal, nor was it necessarily designed with illicit functions in mind—though the designers were also keenly aware that rigorous anonymity would protect putatively good and bad activity in equal measure (Gehl, 2016, 2018). Recent empirical estimates suggest that more Tor users in liberal democracies such as the US are likely using the technology for illicit purposes than in repressive regimes, but still a vast majority (greater than 90 percent of the average daily total) still use the Tor network as a hyper private browser with which to visit surface web sites in place of Onion/Hidden Services (Jardine et al., 2020). This block of benign users might be sensitive to the disposition of coverage and could choose to avoid the risk of potentially being caught up in law enforcement activity by substituting to other services in the place of Tor, such as commercial VPNs or DuckDuckGo, in the wake of a takedown.

A second, highly malicious block of Tor users that are potentially unconnected to cryptomarkets might also be generally deterred from connecting to the Tor anonymity network following the takedown of Darknet drug markets. One empirical investigation suggestions that upward of 80 percent of Hidden Service site visits in 2015 went to sites dedicated to child abuse imagery distribution (Owen & Savage, 2015). Such a disproportionate usage rate of available Hidden Service content suggests that child abuse imagery consumption patterns are likely more compulsive and frequent on an intraday basis than drug procurement behaviors on Darknet markets and could make up a larger share of US Tor network connections on an average day. To the extent that Darknet market closures send a clear deterrent signal generally indicting the potential effectiveness of law enforcement to police Darknet sites (an eventuality that is supported by the increasing certainty of punishment language in official press statements), then Tor users who are engaged in criminal activities beyond drug exchange on cryptomarkets might be dissuaded from using Tor and might leave for a longer duration than is evident within the drug market ecosystem.

Conclusion

This paper leverages a new dataset of qualitatively coded sentiments surrounding law enforcement closure of Darknet cryptomarkets. Sentiments expressed in media coverage and official releases can send either deterrent or publicity signals to the public, and often will even within the same corpus of text. After tracing the nature of these expressed sentiments both qualitatively and quantitatively, this article documented how coverage might be giving rise to part of the "anti-fragility" of the Darknet ecosystem (Taleb, 2012). Tor network use within the US sometimes dips in the wake of events that are covered in comparatively strong deterrence terms by media outlets. Tor network use tends to actually increase marginally in events that are comparatively high in terms of publicity signals. Older closures are associated with sizable jumps in US-based Google search activity surrounding the topic of the Dark Web, but this effect has declined over time.

Declarations

Research for this project was provided by the Institute for Society, Culture, and the Environment at Virginia Tech. The Authors have no financial or non-financial interests related to this article.

References

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

Apel, R., & Nagin, D. S. (2011). General deterrence: A review of recent evidence. *Crime and Public Policy, 4*, 411–436.

Arthur, C. (2013). Silk road: Suspicions grow that server was hacked ahead of arrests. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/oct/08/silk-road-hack-suspicion-fbi-server

Ayers, J. W., Ribisl, K., & Brownstein, J. S. (2011). Using search query surveillance to monitor tax avoidance and smoking cessation following the United States' 2009 "SCHIP" cigarette tax increase. *PLoS ONE, 6*(3), e16777. https://doi.org/10.1371/journal.pone.0016777

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016). 'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy, 35*(Supplement C), 50–57. https://doi.org/10.1016/j.drugpo.2016.04.006

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

Bradley, C. (2019). *On the resilience of the dark net market ecosystem to law enforcement intervention*. UCL (University College London). Retrieved from https://discovery.ucl.ac.uk/id/eprint/10080409/8/Bradley_10080409_thesis.pdf

Breckenridge, J., & Jones, D. (2009). Demystifying theoretical sampling in grounded theory research. *Grounded Theory Review, 8*(2). Retrieved from https://groundedtheoryreview.com/2009/06/30/847/

Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy Brief, 7*. Retrieved from https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf

Cantor, C. H., Sheehan, P., Alpers, P., & Mullen, P. (1999). Media and mass homicides. *Archives of Suicide Research, 5*(4), 285–292.

Chen, A. (2013). Silk Road's Downfall Killed the Dream of the Dark Net. *Gawker*. Retrieved from https://gawker.com/silk-roads-downfall-killed-the-dream-of-the-dark-net-1441310875

Chen, Z., Jardine, E., & Liu, X. (2021). *Examining the Information Pathways Leading to the Darknet: A Cross-National Analysis.* Paper presented at the 71st Annual International Communication Association Conference (ICA21).

Chen, Z., Jardine, E., Fan Liu, X., & Zhu, J. J. H. (2022). Seeking anonymity on the internet: The knowledge accumulation process and global usage of the Tor network. *New Media & Society*, 14614448211072201. https://doi.org/10.1177/14614448211072201

Choi, H., & Varian, H. (2012). Predicting the present with google trends. *Economic Record, 88*(s1), 2–9. https://doi.org/10.1111/j.1475-4932.2012.00809.x

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

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change, 67*(1), 55–75. https://doi.org/10.1007/s10611-016-9644-4

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy, 35*(Supplement C), 69–76. https://doi.org/10.1016/j.drugpo.2016.06.003

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime. *International Criminal Justice Review, 28*(3), 255–274. https://doi.org/10.1177/1057567718769719

De-Oliveira-Sarda, T. (2020). *The dark side of the internet: A study about representations of the deep web and the Tor network in the British press.* Loughborough University.

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

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

FBI. (2017). *Darknet Takedown.* In Authorities Shutter Online Criminal Market AlphaBay. Federal Bureau of Investigation.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 18*(7), 1219–1235. https://doi.org/10.1177/1461444814554900

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

Glover, C. (2022). Dark web marketplace Hydra has been shut down. What will take its place? Retrieved from https://techmonitor.ai/technology/cybersecurity/hydra-marketplace-shut-down-ransomware

Gould, M., Jamieson, P., & Romer, D. (2003). Media contagion and suicide among the young. *American Behavioral Scientist, 46*(9), 1269–1284. https://doi.org/10.1177/0002764202250670

Greenberg, A. (2017). The Biggest Dark Web Takedown Yet Sends Black Markets Reeling. *Wired.* Retrieved from https://www.wired.com/story/alphabay-takedown-dark-web-chaos/

Haasio, A., Harviainen, J. T., & Savolainen, R. (2020). Information needs of drug users on a local dark Web marketplace. *Information Processing & Management, 57*(2), 102080. https://doi.org/10.1016/j.ipm.2019.102080

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

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

Ishii, Ki. (1991). Measuring mutual causation: Effects of suicide news on suicides in Japan. *Social Science Research, 20*(2), 188–195. https://doi.org/10.1016/0049-089X(91)90016-V

Jardine, E. (2015). The dark web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series* (21), 1–24. Retrieved from https://www.cigionline.org/sites/default/files/no.21.pdf

Jardine, E. (2018a). Privacy, censorship, data breaches and Internet freedom: The drivers of support and opposition to Dark Web technologies. *New Media & Society, 20*(8), 2824–2843. https://doi.org/10.1177/1461444817733134

Jardine, E. (2018b). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New Media & Society, 20*(2), 435–452. https://doi.org/10.1177/1461444816639976

Jardine, E. (2021). Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention. *American Journal of Criminal Justice, 46*(6), 980–1005.

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

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

Jewkes, Y., & Linnemann, T. (2017). *Media and crime in the US*. Sage Publications.

Johnston, J., & Joy, A. (2016). *Mass shootings and the media contagion effect.* Paper presented at the American Psychological Association's 124th Annual Convention, Denver, CO. Retrieved from https://www.apa.org/news/press/releases/2016/08/media-contagion-effect.pdf

Kleck, G., & Barnes, J. C. (2014). Do more police lead to more crime deterrence? *Crime & Delinquency, 60*(5), 716–738. https://doi.org/10.1177/0011128710382263

Kleck, G., Sever, B., Li, S., & Gertz, M. (2005). The missing link in general deterrence research. *Criminology, 43*(3), 623–660. https://doi.org/10.1111/j.0011-1348.2005.00019.x

Kovach, S. (2013). FBI Says Illegal Drugs Marketplace Silk Road Generated $1.2 Billion In Sales Revenue. *Business Insider*. Retrieved from https://www.businessinsider.com/silk-road-revenue-2013-10#:~:text=The%20FBI%20says%20Silk%20Road,%2480%20million%20in%20sales%20commissions

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), 414–433.

Leger, D. L. (2013). How FBI brought down cyber-underworld site Silk Road. *USA Today*. Retrieved from https://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/

Lindner, A. M., Elsner, J., & Pryciak, G. (2020). Tor and the City: MSA-level Correlates of Interest in Anonymous Web Browsing.

Lindner, A. M., & Xiao, T. (2020). Subverting surveillance or accessing the Dark Web? Interest in the Tor anonymity network in U.S. states, 2006–2015. *Social Currents, 7*(4), 352–370. https://doi.org/10.1177/2329496520919165

Ma, M., Liu, S., & Li, J. (2017). Does media coverage influence the spread of drug addiction? *Communications in Nonlinear Science and Numerical Simulation, 50*, 169–179. https://doi.org/10.1016/j.cnsns.2017.03.002

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

Masson, K., & Bancroft, A. (2018). 'Nice people doing shady things': Drugs and the morality of exchange in the darknet cryptomarkets. *International Journal of Drug Policy, 58*, 78–84. https://doi.org/10.1016/j.drugpo.2018.05.008

Mawby, R. C., & Gisby, W. (2009). Crime, media and moral panic in an expanding European Union. *The Howard Journal of Criminal Justice, 48*(1), 37–51.

Munksgaard, R., & Demant, J. (2016). Mixing politics and crime–The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy, 35*, 77–83.

Nuti, S. V., Wayda, B., Ranasinghe, I., Wang, S., Dreyer, R. P., Chen, S. I., & Murugiah, K. (2014). The use of google trends in health care research: A systematic review. *PLoS ONE, 9*(10), e109583. https://doi.org/10.1371/journal.pone.0109583

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

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

Primack, B. A., Kraemer, K. L., Fine, M. J., & Dalton, M. A. (2009). Media exposure and marijuana and alcohol use among adolescents. *Substance Use & Misuse, 44*(5), 722–739. https://doi.org/10.1080/10826080802490097

Project, T. (2018). Users. Retrieved from https://metrics.torproject.org/userstats-relay-country.html?start=2018-03-20&end=2018-03-22&country=all&events=points

Romer, D., Jamieson, P. E., & Jamieson, K. H. (2006). Are news reports of suicide contagious? A stringent test in six US cities. *Journal of Communication, 56*(2), 253–270.

Seifter, A., Schwarzwalder, A., Geis, K., & Aucott, J. (2010). The utility of "Google Trends" for epidemiological research: Lyme disease as an example. *Geospatial Health, 4*(2), 135–137. https://doi.org/10.4081/gh.2010.195

Sinyor, M., Schaffer, A., Nishikawa, Y., Redelmeier, D. A., Niederkrotenthaler, T., Sareen, J., . . ., & Pirkis, J. (2018). The association between suicide deaths and putatively harmful and protective factors in media reports. *CMAJ, 190*(30), E900-E907.

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

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder* (vol. 3): Random House Incorporated.

Tandoc, E. C., Jr. (2019). *Analyzing analytics: Disrupting journalism one click at a time*. Routledge.

Towers, S., Gomez-Lievano, A., Khan, M., Mubayi, A., & Castillo-Chavez, C. (2015). Contagion in mass killings and school shootings. *PLoS ONE, 10*(7), e0117259. https://doi.org/10.1371/journal.pone.0117259

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

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., & Burns, L. (2016). Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *International Journal of Drug Policy, 35*(Supplement C), 16–23. https://doi.org/10.1016/j.drugpo.2016.07.004

Van Buskirk, J., Roxburgh, A., Farrell, M., & Burns, L. (2014). The closure of the Silk Road: What has this meant for online drug trading? *Addiction, 109*(4), 517–518. https://doi.org/10.1111/add.12422

Van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy, 25*(2), 183–189. https://doi.org/10.1016/j.drugpo.2013.10.009

Welch, M., Price, E. A., & Yankey, N. (2002). Moral panic over youth violence: Wilding and the manufacture of menace in the media. *Youth & Society, 34*(1), 3–30. https://doi.org/10.1177/0044118X02034001001

Zetter, K. (2013). How the Feds Took Down the Silk Road Drug Wonderland. *Wired.* Retrieved from https://www.wired.com/2013/11/silk-road/

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

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.