Australian Government

Australian Institute of Criminology

AIC reports

Research Report 18

Impact of darknet market seizures on opioid availability

Roderic Broadhurst
Matthew Ball
Chuxuan Jiang
Joy Wang
Harshit Trivedi

Serious & Organised Crime
Research Laboratory

ISSN 2206-7280 (Online)
ISBN 978 1 925304 88 6 (Online)

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review—either through a double-blind peer review process, or through stakeholder peer review. This report was subject to double-blind peer review.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Acknowledgements

The authors thank Professor Ross Maller, Professor Peter Grabosky, Dr Rick Brown, Dr Isak Ladegaard and the anonymous reviewers for their helpful comments on earlier drafts of the report.

Acronyms and abbreviations

DDOS	distributed denial-of-service
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
FBI	Federal Bureau of Investigation
J-CODE	Joint Criminal Opioid and Darknet Enforcement
LEA	law enforcement agency
PGP	Pretty Good Privacy (encryption)

Abstract

Opioids, including the highly potent synthetic opioids fentanyl and carfentanil, are commonly sold on illicit cryptomarkets or Tor darknet markets. Data collected throughout 2019 from 12 large darknet markets that sold opioids enabled observation of the impact of law enforcement seizures and voluntary or scam market closures on the availability of fentanyl and other opioids.

Trends in opioid and fentanyl availability before and after law enforcement interventions indicate whether market operators and sellers are deterred and whether market closures lead to displacement, dispersal or substitution. Evidence of all of these outcomes was present in both descriptive and trend analyses, although most effects were short lived. Market closures, especially law enforcement seizures, reduced the availability of opioids, in particular fentanyl, as well as increasing prices and displacing vendors to other markets. Market closures also led vendors to substitute fentanyl for other opioids or other illicit drugs.

Summary

Opioids, including the highly potent synthetic opioid fentanyl and carfentanil, which has the potential to be used as a chemical weapon, are commonly sold on illicit cryptomarkets or Tor darknet markets. This report investigates the impact of darknet market closures (voluntary or exit scams) and law enforcement market seizures on the availability of fentanyl and other opioids. Quantitative methods were used to investigate the presence of potential effects of closures and seizures. We analysed these effects across four dimensions: opioid availability (as measured by unique listings), vendor or trader movement and cross-market activity, market stock value and variations in the prices of opioid products. A unique product listings time series was constructed, and the time series was then split into several sub-intervals based on the timing of market closures.

Data were collected over 352 days, from 2 January to 20 December 2019 (excluding weekends), combining 251 scrapes from initially eight darknet markets: Apollon, Empire, Dream, Nightmare, Tochka (also known as Point), Berlusconi, Valhalla (also called Silkitie), and Wall Street. In April three ‘new’ markets (Agartha, Dream Alt and Samsara) were added after Wall Street and Valhalla were seized by law enforcement and Dream voluntarily closed. In July Cryptonia was added as a substitute for Nightmare, which closed in an exit scam (where a business stops sending orders but continues to accept payment for new orders). Cryptonia operated until a planned (voluntary) closure in November.

Darknet markets have presented unique problems to law enforcement agencies (LEAs) since the inception of Farmer’s Market in 2006, and its subsequent move to the Tor hidden service in 2010. In 2011 Silk Road 1.0 emerged as a significant innovation, combining then relatively novel cryptocurrencies with the anonymity of Tor, before it was seized and its operators arrested in 2013. The Silk Road model proved enduring and darknet markets continued to evolve. Accordingly, LEA operational techniques continue to adapt to the criminal use of the Tor platform and, as with cybercrime in general, transnational policing methods have become essential.

In early 2019, a transnational law enforcement task force of US and European LEAs, the Joint Criminal Opioid and Darknet Enforcement (J-CODE) team, focused on the darknet trade in fentanyl. J-CODE's Operation SaboTor targeted Wall Street, a darknet market that was then among the most active in selling fentanyl and its derivatives. Under Operation SaboTor, Finnish Customs (with French National Police and Europol) seized Valhalla in February 2019, and then in April the German Federal Criminal Police (*Bundeskriminalamt*) arrested three Germans who operated Wall Street. Another 61 associated vendors or dealers, mostly located in the US and Europe, were also arrested. In May a major online gateway, DeepDotWeb, which linked buyers to darknet market URLs, was also seized by the J-CODE team. Throughout 2019, several other darknet markets also closed, either in exit scams (Nightmare in July, Tochka in November) or in voluntary closures (Dream Market in March, Cryptonia in November). In September 2019, as part of Operation Darknet, the Italian *Guardia di Finanza* seized Berlusconi, a market that was also active in the sale of fentanyl and other opioids.

The potential deterrence of market operators and sellers and the displacement, dispersal or product substitution that may follow such closures were explored by comparing trends in opioid and fentanyl availability before and after law enforcement interventions. Evidence of all of these outcomes was present in both descriptive and trend analyses, although effects were often short lived. Analysis also showed that market closures, especially seizures of markets by law enforcement, reduced the availability of opioids, in particular fentanyl, increased prices and displaced vendors to other markets. Market closures also led buyers to substitute fentanyl for other illicit drugs or other opioids.

Throughout 2019 a total of 2,089,694 listings, excluding duplicates, were identified, advertising a diverse range of illicit drugs and other contraband. Three percent (n=63,567) of these listings were opioids, of which roughly five percent (n=3,151) were fentanyl. Among fentanyl listings, 19 percent (n=606) were the extremely potent analogue carfentanil.

Over the observed period, Berlusconi offered the greatest number of unique listings, representing 36 percent of all listings. The items identified included illicit drugs, digital products such as malware and other contraband. Berlusconi also had the highest number of opioid listings (again at 36%) while Wall Street dominated listings of fentanyl (55%) and carfentanil (41%) until its seizure in April 2019. Tochka accounted for 21 percent of fentanyl and 30 percent of carfentanil availability until its exit scam in November of that year.

After the closure of Dream and the seizures of Valhalla and Wall Street, the April–July 2019 period saw the largest growth of opioid listings—from 5,320 at the end of April to 16,930 at the end of July. Yet this period also saw a decline in fentanyl listings: from 792 at the end of April to 531 listings by the end of July, and in December only seven listings (five of which advertised carfentanil) remained on Empire. Wall Street dominated fentanyl availability between January and April, but after its seizure Tochka took over the dominant market share until its exit scam in November. New markets also took up some market share after Tochka's closure.

Over the observed period, 4,156 opioid vendors with unique aliases were identified. Roughly three-quarters (74%) of these vendors (*n*=3,090) operated in only one market, while the remaining 26 percent of vendors (*n*=1,066) operated across two or more markets. Almost one in five opioid vendors sold fentanyl (*n*=793), with about a quarter (*n*=212) of these advertising carfentanil.

This study shows the strengths and limitations of LEA operations targeting darknet markets. The results suggest that LEA operations targeting specific high-risk products (eg fentanyl) on darknet markets have a greater impact than voluntary closures or exit scams. However, there has always been an element of self-regulation in the operation of darknet markets, such as the widespread policy of banning the listing of child exploitation material. Many markets respond to LEA interventions by implementing further self-regulation of high-risk products. Potent synthetic opioids such as fentanyl and its derivatives were widely banned by many darknet markets throughout 2018 and 2019, indicating that the darknet market economy is risk sensitive and evolving.

LEA operations targeting darknet markets require a long-term effort, with success often the consequence of user error and complacency. Darknet criminal actors are aware of LEA disruption efforts and may underestimate the risks associated with policing activities such as undercover operations and the arrests of vendors and buyers. Market displacement and dispersal as a consequence of closures (voluntary or exit scams) and police operations make buyers, sellers and market operators more adaptable and risk averse.

The implications for criminal justice policy and policing practice are discussed and the probable forms of organised crime and criminal enterprise that may comprise the darknet economy are considered. Transnational and cross-agency police cooperation is crucial in the investigation and prosecution of darknet market players. Persistent surveillance and suppression will be necessary if the availability of the most dangerous synthetic opioids is to be disrupted. The darknet economy has proven to be resilient, and the large profits to be earned from fentanyl, carfentanil and other opioids ensure that these and other products will continue to be available on some darknet markets.

Introduction

This report describes the impact of law enforcement agency (LEA) investigations and operations targeting illicit cryptomarkets or Tor darknet markets. These darknet markets can be used as a litmus test of trends in illicit drugs, malware and other digital products, as well as criminal novelty and entrepreneurship more generally. Surveys of darknet markets help track prices of narcotics and other drugs as well as surges or shortages in other contraband. Furthermore, darknet markets are an important supply–demand connection for contraband and provide a growing vector for the distribution of low mass, high value synthetic opioids and other drugs.

Cybercrime is now a universal and commonplace occurrence, often performed transnationally via sophisticated tradecraft (Australian Cyber Security Centre 2020). The continued growth of the internet has made cybercrime, often associated with underground online illicit cryptomarkets, or darknet markets, a lucrative and expanding business. The annual economic cost of cybercrime is estimated to be $1 trillion (World Economic Forum 2020), much of which is driven by a flourishing underground online black market. Digital products such as malware, phishing, stolen identities, and ransomware tools are commonly sold along with a wide range of illicit drugs and other contraband on darknet markets. This darknet economy allows consumers of contraband to connect across time and place, taking advantage of the hidden services found on encrypted Tor-like platforms and virtual private networks.

The systematic and borderless engineering of cybercrime has led to law enforcement cooperation across jurisdictions in response to a wide range of cybercrime, from ransomware to the operation of encrypted online drug markets or darknet markets. Gone are the days of the lone hacker or online drug dealer; cybercrime has become well organised on an industrial scale (Anderson et al. 2013; Australian Criminal Intelligence Commission 2019; Broadhurst et al. 2014) and darknet markets are one example of this trend.

Illicit markets

The value of darknet markets is difficult to gauge but a recent estimate based on Bitcoin and other cryptocurrency transactions indicated about US$790m was generated through about 12 million transactions in 2019—a fraction of the cryptocurrency transactions that occur on Tor for other hidden services (Chainalysis 2020). Although the overall value of darknet markets has been increasing, they remain a relatively small component of the hidden services available on Tor and an even smaller component of all illicit drug and other contraband markets. The global scale of the main conventional illicit drug markets (ie cannabis, cocaine, opiates and amphetamine-type stimulants) was estimated to be between $US426b and $US652b in 2014, of which $US75b to $US132b was attributed to opiates (EMCDDA & Europol 2019: 28; May 2017: 3). This compares to an estimated market of about US$360b a decade earlier (United Nations Office on Drugs and Crime 2005: 127). However, estimates of the value of the illicit drug economy, especially global estimates, are fraught.

RAND estimated drug revenues on darknet markets (excluding prescription drugs, alcohol and tobacco) to be between $US12m and $US21m (€10.5m to €18.5m) per month, compared to an estimated revenue of $US2.3b (€2b) per month for offline sales across the European Union (European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) & Europol 2016). Thus, darknet markets at best facilitate about one percent of the value of the retail market for illicit drugs in Europe. The EMCDDA and Europol (2019: 28–30) conservatively estimated the annual value of the European Union offline retail market for the main illicit drugs (ie cannabis, cocaine and 'crack', heroin) to be at least €30b in 2017.

In Australia the value of amphetamine, MDMA, cocaine and heroin seizures was the equivalent of a retail market valued at A$5b (Australian Criminal Intelligence Commission 2019). The National Wastewater Drug Monitoring Program gauges drug consumption by sampling and analysing sewage processed by wastewater treatment plants. It estimated that the value of these four illicit drugs was about A$11.3b (Australian Criminal Intelligence Commission 2020b). However, estimates of the value of illicit fentanyl and other synthetic opioids identified by this program are not available due to the confounding effect of prescription use of these pharmaceuticals (Australian Criminal Intelligence Commission 2019: 15, 36).

This underlines the wealth of the black economy and the scale of the illicit drug market. The tangible cost of opioid misuse, or 'extra-medical opioid use' of the estimated 104,000 dependent users in Australia (2015–2016) is about A$5.6b. Tangible costs include hospital and health services, crime, traffic accidents, and premature loss of life but exclude the decreased quality of life for families living with an opioid dependent person (Whetton et al. 2020).

We focus on the effect LEA interventions have on the availability of opioids, especially fentanyl and fentanyl analogues, on these darknet markets. We distinguish in this study fentanyl (and analogues) from other opioids such as heroin, opium, oxycodone, codeine, morphine, methadone, tramadol and buprenorphine. Synthetic opioids, especially fentanyl and its analogues, have become a major driver of drug overdoses and fatalities, notably in the in United States and Canada but also in Australia and elsewhere (Brown & Morgan 2019; Pardo et al. 2019). Due to its potency and relatively low price compared to other opioids, fentanyl has emerged as a significant source of profit for darknet dealers or vendors. Fentanyl and its even more dangerous derivative carfentanil are attractive because small quantities can be readily shipped via postal services (Broadhurst, Ball & Trivedi 2020). According to EMCDDA and Europol (2019: 17):

> High-potency synthetic opioids pose particular challenges for law enforcement and increased risks to health. They are increasingly traded online and dispatched by post, and small-volume packages can contain a large number of potential consumer doses.

Policing cooperation is essential as cybercrime is typically a transnational crime and darknet markets are a prime example of the global reach of cybercrime. In 2017, for example, the Australian Federal Police received a tip-off from the Royal Canadian Mounted Police that a shipment of the highly potent and lethal fentanyl analogue carfentanil was destined for Australia. This tip-off followed a raid of the home of a darknet market vendor in British Columbia, and in August 2017 the AFP executed a search warrant on the home of an 18 year old woman in Western Australia. The woman was found in possession of 121.76 milligrams of carfentanil (a trafficable quantity), which she had purchased from Dream Market. She was subsequently arrested and sentenced to nine months imprisonment in February 2019 for one count of importing a border-controlled drug (CDPP 2019; *Queen v Griffiths* [2019] District Court of Western Australia). This demonstrates the value of law enforcement agencies sharing information with each other to disrupt global drug trafficking, whether it is done conventionally or via anonymous darknet platforms.

Relevant legislation

In Australia, drugs are regulated at both the federal level and the state and territory level. At the federal level, serious drug offences involving the importation or exportation of controlled and border-controlled drugs, their analogues and their precursors fall under the Commonwealth *Criminal Code Act 1995*, pt 9.1 (Serious Drug Offences). Under pt 9.1, the main serious drug offences involve:

- trafficking, selling and cultivation of the prohibited drug;
- manufacturing the prohibited drug;
- importing and exporting the prohibited drug; and
- possession of the prohibited drug.

Federal drug offences are prosecuted by the Commonwealth Director of Public Prosecutions and apply to the purchasing and selling of illicit drugs via darknet markets. These offences target the supply and movement of controlled or border-controlled drugs (Brown et al. 2015). The penalty for each pt 9.1 offence depends on the quantity of the prohibited substance involved. Basic possession of a controlled or border-controlled drug could result in two years imprisonment, while importing or exporting a commercial quantity of a controlled or border-controlled drug could result in life imprisonment. The Criminal Code Regulations 2019 (Cth) sch 1 sets out the quantities for each tier (from smallest to largest): trafficable, marketable and commercial. For fentanyl, the trafficable quantity is 0.005 grams, a marketable quantity is 2.5 grams and a commercial quantity is 5 grams.

Drug offences at the state and territory level primarily deal with the domestic possession of drugs by drug users and dealers (Brown et al. 2015). State and territory drug laws contain summary offences related to the use and possession of prohibited drugs, the administration of prohibited drugs to others, and the possession of equipment for administration. They also cover indictable offences aimed at commercial drug trafficking, including the cultivation, manufacture and supply of prohibited drugs, and the possession of their precursors with intention to use them to manufacture the prohibited drug. Thus, unlike drug offences at the federal level, state and territory drug offences target users of illicit drugs and individuals who supply them to others within Australia.

LEAs face challenges prosecuting darknet market operators, traders and consumers. Electronic evidence is difficult to collect and preserve and LEAs cannot easily send a subpoena to a darknet marketplace because Tor anonymises each user's computer traffic (White et al. 2019). It can also be challenging to seize and secure cryptocurrencies such as Bitcoin as evidence and to press conspiracy or joint commission charges against suspects. US organised crime laws such as the *Racketeer Influenced Corrupt Organizations Act* emphasise the prosecution of the leaders of criminal enterprises and can apply to broad range of offences including cybercrime (Cronin 2018; White, Kakkar & Chou 2019).

The *Australian Crime Commission Act 2002* (Cth) defines serious and organised crime as requiring two or more offenders, substantial planning and the use of sophisticated methods or techniques. This legislation identified 18 serious offences (ie punishable by imprisonment for a period of 3 years or more) including cybercrime, illegal drug dealing and firearm dealing. Other offences included 'serious' theft, fraud, money laundering, currency violations, illegal gambling, obtaining financial benefit via vice, extortion, violence, bribery or corruption, perverting the course of justice, bankruptcy and company violations, harbouring criminals, forging passports, and illegal importation or exportation of fauna (Broadhurst et al. 2018). Many of these offences also have a virtual or cyber expression. Trading and advertising illicit drugs and other contraband via darknet platforms are serious and organised crimes that evoke the special powers of the *Australian Crime Commission Act*. This enables LEAs to undertake controlled operations, specialist surveillance, witness protection, and unexplained wealth investigations and asset forfeiture (Ayling & Broadhurst 2014).

Prosecutions against darknet market drug vendors may include charges at both the federal and state and territory levels; for example, if a vendor imports a marketable quantity of a border-controlled drug into Australia to sell to local buyers, they have committed both federal and state and territory drug offences. Darknet illicit drug transactions involve moving drugs across borders and also evoke Australia's international mutual legal assistance obligations under the 2004 Council of Europe Convention on Cybercrime (Budapest Convention) and the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. The Budapest Convention harmonises national laws and furthers international police and judicial cooperation in respect of cybercrime and provides for the extradition of suspects, the disclosure and preservation of computer and traffic data, real-time traffic data collection, and cross-border access to stored computer data. The Budapest Convention has been influential and has been adopted by 67 states including those outside Europe such as Australia, Japan, the United States and Canada. China, Brazil, the Russian Federation and India remain outside the convention framework.

Article 2 of the UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances— enacted in Australia by the *Crimes (Traffic in Narcotic Drugs and Psychotropic Substances) Act 1990*—states that the purpose of the convention is to 'promote co-operation among the Parties so that they may address more effectively the various aspects of illicit traffic in narcotic drugs and psychotropic substances having an international dimension'. The convention criminalises the manufacture and trafficking of narcotic drugs and psychotropic substances, which are offences under Australian law, and acts as a legal basis for extradition in respect of those offences. The convention provides for mutual legal assistance in investigations (ie the taking of evidence, execution of searches and seizures), prosecutions and judicial proceedings related to drug offences.

Many darknet market operators and traders also meet the basic definition of an organised crime group as specified in the United Nations Convention against Transnational Organized Crime (Palermo Convention), adopted in 2000. The Palermo Convention has been ratified by 147 signatories, including Australia, and was enacted to promote cooperation in the prevention and control of transnational organised crime. The Palermo Convention covers a broader spectrum of criminal activities in addition to the illicit drug trade (eg arms and human trafficking) and, importantly, provides cross-border mechanisms for the tracing of the monetary proceeds of crime. Article 2 of the Palermo Convention (United Nations Office on Drugs and Crime 2018: 5) defines an organised crime group as:

> a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit…

This general definition of 'organised crime' has limitations but is pragmatic and sufficiently theoretically open to account for the many definitions offered and the diversity of the phenomena (Edwards & Levi 2008; Fijnaut 2014; Maltz 1976). The concept of organised crime is nevertheless a contested one with little unanimity about how best to define it (Hobbs & Antonopoulos 2014; Kleemans 2014; Paoli & Beken 2014) in either the real or the virtual world (Lavorgna 2019; Leukfeldt, Lavorgna & Kleemans 2017; Lusthaus 2013).

LEA darknet market seizures and arrests point to the need for at least three criminal actors to manage and administer the basic functions of an omnibus darknet that can operate effectively for a period of several months or more in virtual black markets. Thus, darknet market criminal networks of administrators, and vendors of prohibited products such as fentanyl and other opioids, provide a virtual market for organised crime (Leukfeldt 2015; Leukfeldt et al. 2019).

The aims of this study are outlined next, followed by a description of darknet markets and LEA operations targeted at reducing the supply of opioids, especially fentanyl, and then a brief summary of the relevant literature is presented. Next, we detail the methods and data collected to analyse the impact of LEA seizures, followed by a description and discussion of the results. We conclude by considering the kinds of criminal enterprises active in the darknet drug economy and how LEAs may shape the operation of darknet markets and vendors.

Aims

This study aims to identify the impact of police seizures of darknet markets on darknet market activity, particularly the online availability of fentanyl. Market seizures due to LEA operations and other market closures over the course of 2019 present a natural quasi-experiment, allowing us to measure the impact of market closures on fentanyl availability. The findings can help assess the long-term effects of these operations, and shape future law enforcement decisions.

The assumption is that law enforcement seizures of markets and arrests of key actors lead to four possible outcomes or forms of disruption (see Johnson, Guerette & Bower 2014; Reppetto 1976): displacement, substitution, diffusion and dispersion, and deterrence. However, hidden service darknet markets operating on the Tor network are constantly evolving. A feature of contemporary darknet markets is their advanced operational security and adaptability—the darknet economy is expected to be risky, volatile and impermanent, and market actors anticipate disruption.

We drew on data captured from 12 of the largest omnibus darknet markets deemed most active and distinguished between two groups: eight original markets (with data collected from January 2019), and four new or replacement markets selected to substitute for several of the original markets that ceased operations during the course of the study (from April 2019). These markets were chosen because of their size (they each had at least 1,000 products advertised), general range of products offered, popularity (as indicated by reference in relevant market forums) and active status.

Given market closures occurred due to police operations or were initiated by market operators (either as a voluntary planned closure, or an exit scam) we explored changes in online availability or supply of opioid products, and the movement of vendors. Outcomes of market-initiated closures and law enforcement seizures could also be compared. Since darknet markets remain operational, we tested the extent to which closures and seizures reduced the availability of fentanyl and other opioids and whether displacement or substitution occurred over time.

The research questions include:

- What was the effect on the supply of fentanyl after LEA market seizures and other closures which removed key market operators and vendors?
- More generally, what are the impacts of darknet market closures on the overall market or ecosystem? Our focus is on law enforcement seizures but there may also be the confounding impact of planned closures and exit scams: for example, are exit scams triggered by other forms of closure?
- What evidence is there of substitution and/or displacement and/or dispersal/diffusion (among vendors, products/markets and prices)?
- Do market seizures and arrests deter market actors from offering specific targeted products? Did markets regulate or moderate product availability in response to LEA operations targeting fentanyl?

Darknet markets

Hidden services platforms are most commonly accessed through the Tor network but Freenet (https://freenetproject.org/author/freenet-project-inc.html) and i2p (https://geti2p.net/en/) are alternative platforms. Darknet markets account for a component of these hidden services. The Tor network hides a user's traffic through layers of networks, which makes tracing the user difficult. In a 2015 study by the Tor project, it was estimated that the Tor darknet consisted of around 30,000 unique hidden services (Kadianakis & Loesing 2015: 9). However, a 2018 study suggested this figure was dramatically inflated, due in part to the volatile lifecycle of these hidden services, concluding that Tor's hidden service darknet is roughly half the size previously reported (Owenson, Cortes & Lewman 2018: 4). Al-Nabki et al. (2019: 217) classified 20 percent of 10,367 known Tor sites as 'suspicious' or criminal and 48 percent as 'normal' (eg hosting and cryptocurrency services), while 32 percent were classified as unknown because they were unavailable, empty or locked.

From the 1990s onwards, online platforms for the sale and distribution of licit products widened the scope of e-commerce. For example, eBay was established in 1995, Amazon in 1996 and Etsy in 2005. These platforms made it relatively easy to purchase physical products online. In the late 2000s, with the birth of Bitcoin and other cryptocurrencies, anonymous online platforms called 'darknet markets' specialising in the sale and distribution of illicit products started to evolve—for example, the Farmer's Market, 2006; Silk Road 1.0, 2011 (Aldridge & Askew 2017). The Farmer's Market was the first to specialise in trading illicit products, and began operating on the internet before moving to the Tor network in 2010. Silk Road 1.0 was the first anonymous online platform to incorporate Bitcoin transactions. The evolution of darknet markets is described as unfolding in three distinct waves from Silk Road onwards, settling into an institutionalised or regularised way of conducting business (Martin, Cunliffe & Munksgaard 2019).

Just as with their licit counterparts, these anonymous platforms made it easy to purchase illicit products online. Darknet markets provide techno-criminals with a secure platform for efficient, (pseudo)anonymous, local and international trading of illicit goods and services.

The innovative 'Silk Road' model of illicit trading was built on four facilitators: Tor, cryptocurrencies, escrow, and trust established via buyer feedback. For this reason, darknet markets exemplify the notion of 'open secrecy' (Ladegaard 2019), combining efficiency with anonymity and scale—a feature they share with traditional 'secret' mafia-like groups. These markets present significant challenges to LEAs and national intelligence agencies (Bewley-Taylor 2017; Heidenreich & Westbrooks 2017), and 'forensically aware' market actors adapt to law enforcement countermeasures (Bradley & Stringhini 2019). However, advantages for criminal actors in these markets, such as impediments to cross-jurisdictional investigations and the tracing of illicit funds or transactions, are no longer sufficient to protect online illicit markets, as cross-national policing operations have evolved in response. These operations have included joint investigations across many agencies and jurisdictions. For example, the Joint Criminal Opioid and Darknet Enforcement (J-CODE) team brought together the European Union Agency for Law Enforcement Cooperation (Europol); police agencies from the United Kingdom, the Netherlands, France and Germany; and the Australian Federal Police, among others. For example, Australian LEAs frequently conduct joint operations or intelligence sharing with their overseas partners, including 'five eyes' partners—the United States, United Kingdom, New Zealand and Canada—as well as Association of Southeast Asian Nations and UN Office on Drugs and Crime partners in Asia. In the case of darknet markets this may involve a wide range of agencies, given the scope of illicit products.

Darknet markets are not immune from disruption; they are vulnerable to distributed denial-of-service (DDOS) attacks undertaken by competitors or extortionists, exit scams, voluntary closures (when an market announces a shutdown ahead of the time and allows vendors and/or buyers to complete orders and withdraw their funds from the associated escrow wallet), and occasionally hacks, de-anonymisation or seizure by law enforcement (EMCDDA & Europol 2017: 8; Moeller, Munksgaard & Demant 2017). These police ‘take-downs’ or seizures are often highly publicised by mainstream media and are also key topics in online discussion forums. Such seizures can damage trust among market actors, which is vital in the darknet market economy, and forced closures and arrests by LEAs may impact on trust in different ways to the more frequent exit scams or voluntary closures. EMCDDA and Europol (2017) identified 103 darknet markets that had been in operation since 2011 (both active and inactive) and limited growth to the darknet market ecosystem has subsequently been noted. The average lifespan of a darknet market was just over eight months (EMCDDA & Europol 2019: 70–71; EMCDDA & Europol 2017: 16) although some of the darknet markets included in our data capture had been in operation longer (eg Dream Market since 2013 and Tochka since 2015). During 2019, a number of large darknet markets ceased operation. Of the 12 markets included in this study, only four were active at the end of the study (Empire, Apollon, Dream Alt and Agartha, of which only Apollon and Empire had been in operation for over 12 months).

Law enforcement operations

Police interventions targeting traditional illicit markets may yield arrests of market players, and identification of dealers (vendors or suppliers) and buyers. Overall, these interventions are designed to disrupt the supply of illicit products. However, the online world presents a different challenge. Darknet markets are protected by difficult to trace cryptocurrencies, increased operational security (via Tor) and anonymous transnational actors. Consequently, LEA investigations capable of disrupting these online illicit markets will have different effects from operations against real world illicit markets. Regular daily data capture of illicit darknet markets’ supply patterns provides data suitable for analysis of the impact of interventions or closures.

Since the first major police operation against a darknet market in 2011, the Australian National University Cybercrime Observatory has identified, from open sources, 19 further police operations targeting Tor hidden services (including darknet markets, child sexual abuse material, and other prohibited goods or activities). As the internet is a global utility, most of these operations have been transnational investigations across multiple agencies and jurisdictions. Law enforcement investigation techniques targeting darknet drug markets have resembled international cooperative efforts to suppress child exploitation material. These techniques typically involve traditional policing methods such as undercover operations, in which law enforcement agents take over user accounts to infiltrate private chats between market traders, administrators and moderators. They also involve LEAs circumventing encryption techniques and deploying malware to de-anonymise and expose the IP addresses of darknet users (Broadhurst 2019; Ladegaard 2019). Other techniques include tracking suspects through the postal system or tracking cryptocurrency transactions (Federal Bureau of Investigation (FBI) 2019; Greenberg 2019).

Identifying and arresting suspects via intercepted parcels containing drugs is a technique often used by LEAs in Australia and elsewhere. On separate occasions in April and May 2020, two men resident in the Northern Territory but not linked were arrested after they arrived at Australia Post parcel lockers to collect seized parcels containing narcotics. This followed a joint investigation by the Northern Territory Joint Organised Crime Taskforce into an alleged criminal network that operated through the darknet and the Australian postal system, and which had parcels destined for Darwin intercepted at mail centres. These parcels contained small amounts of heroin, synthetic heroin, morphine, methamphetamine, cannabis, LSD tablets, MDMA and prescription medications. The Northern Territory Joint Organised Crime Taskforce comprised the Australian Federal Police, Australian Border Force, Northern Territory Police, the Australian Criminal Intelligence Commission and the Department of Home Affairs. Both men were charged with Northern Territory drug offences, and one was additionally charged with importing commercial quantities of border-controlled drugs under federal law (Australian Federal Police and Northern Territory Police Force 2020a, 2020b).

Similarly, Cody Ward (darknet alias 'NSWGreat') was a long-running Australian darknet market vendor behind a large darknet drug supply network in New South Wales who was also identified through postal interception and cyber-surveillance. Ward purchased and sold drugs via the darknet, and he and his co-conspirators had allegedly dealt $17m worth of drugs throughout Australia. Strike Force Royden of the NSW Police Force, which focused on drug supply, intercepted 85 parcels containing prohibited drugs with support from Australia Post, which led to the arrest of Ward and his co-conspirators in February 2019. Ward was charged in May 2019 with both state and federal drug offences (Darknetlive 2019; Dole 2019; South Coast Register 2019).

LEAs have collected valuable data from seizing darknet markets and from cooperating vendors and operators who had been arrested (van Wegberg & Verburgh 2018). Given the difficulties of investigating conspiracies to traffic or supply drugs via darknet markets, reduced charges and discounted sentences are valuable in inducing arrested darknet market staff and vendors to cooperate and provide information. A recent example involved a defendant arrested on charges of trafficking fentanyl who gave police access to his devices, darknet accounts and the vendors from whom he had purchased fentanyl (see *DPP v Martel (a pseudonym)* [2019] VCC 377) and received a substantial penalty discount. As presiding Justice Riddell noted, 'where such cooperation leads to either a prosecution being instituted or a prosecution case being strengthened by evidence against another offender, this ought result in a reduction of penalty'. The *Martel* case shows that offenders can be encouraged, with sentencing discounts, to identify co-offenders.

LEA operations targeting darknet markets often cited in the literature are Operation Onymous (2014), which closed Silk Road 2.0, and Operation Bayonet (2017), which closed AlphaBay—one of the largest markets then active (Greenberg 2018). Such investigations provide an understanding of LEA operations against darknet markets and the importance of transnational interventions and cross-jurisdictional cooperation. International cooperation in targeting serious and organised drug trafficking through the darknet has assisted Australian LEAs in arresting darknet drug vendors and buyers operating in Australia.

Globally, many capable LEAs have worked together to monitor, investigate and close darknet markets. For example, Europol fosters cross-border police investigations and task forces focused on serious and organised crime across the European Union, including darknet markets. In early 2019 J-CODE, a joint operation with Europol, US and other LEAs, specifically targeted darknet market trafficking of opioids, especially fentanyl, and monitored suspects by tracking postal packages and transactions on Bitcoin's blockchain. Between January and March 2019, J-CODE's Operation SaboTor resulted in the arrests of 61 people and the shutdown of 50 darknet accounts (FBI 2019; Greenberg 2019). Under Operation SaboTor, Valhalla, a long-running Tor darknet market operating since 2013, was seized by Finnish Customs with the assistance of the French National Police and Europol. However, its administrators eluded arrest. After Valhalla was shut down, some Finnish opioid vendors moved their listings to other hidden services on Tor, notably Wall Street (Europol 2019). This was also during a period of prolonged DDOS attacks targeting Dream that led to its voluntary closure at the end of March, pushing many vendors to move to other markets. Wall Street was seized next, in April 2019, by the J-CODE taskforce. This led to the arrest of three Germans who operated Wall Street by the German Federal Criminal Police (*Bundeskriminalamt*) with the support of European and US LEAs. By monitoring darknet market and user activity and sharing information, these agencies were able to collect valuable data, adapt their investigation and policing strategies, arrest vendors and buyers and shut down prominent darknet markets.

Two interventions took place during our monitoring of the availability of fentanyl on darknet markets: Operation SaboTor, which closed Wall Street in April 2019, as noted above (see Figure 1), and the Italian *Guardia di Finanza*'s Operation Darknet, which closed Berlusconi—then one of the largest darknet markets. Berlusconi's operational security unravelled with the arrest of one highly active vendor known as 'g00d00' in May 2019. His arrest resulted in the seizure of 2.2 kilograms of cocaine, ketamine and MDMA, as well as 163 ready-made ecstasy tablets and 78 stamps impregnated with LSD ready for post. Crucial data from his seized digital devices linked 'g00d00' to Bitcoin transactions associated with Berlusconi and a copy of Berlusconi's private key.

These links led to the seizure of Berlusconi and the arrest of three Italian nationals who operated the darknet market (all residents of the Puglia region). Two men with handles or pseudonyms managed the site and were also active vendors of a variety of contraband: 'VladimirPutin' was the site administrator and 'EmmanuelMacron' the moderator. Forensic analysis of their conversations on instant messaging applications implicated a third party, who together with them managed the proceeds of the Berlusconi platform and was the likely lead administrator. The three suspects had administrator credentials and had established a partnership, made joint management decisions and split expenses and profits (approximately €400,000 of the €2m transacted annually from Berlusconi; *Guardia di Finanza* 2019; Paganini 2019).

Figure 1: Screenshot of Wall Street after its seizure by J-CODE's Operation SaboTor

Source: Europol 2019

Figure 2: Screenshot of DeepDotWeb after its seizure by J-CODE

Established in January 2018 within the FBI's Hi-Tech Organized Crime Unit, J-CODE targeted the criminal enterprises that facilitate drug trafficking, especially of fentanyl and other opioids, on the darknet. The J-CODE team comprised the following US agencies: FBI, Drug Enforcement Administration, Postal Inspection Service, Customs and Border Protection, Immigration and Customs Enforcement's Homeland Security Investigations, Department of Defense, Financial Crimes Enforcement Network, and the Department of Justice. The DeepDotWeb case also involved French police and judicial authorities, as well as the US Postal Inspection Service, National Cyber-Forensics and Training Alliance, Internal Revenue Service Criminal Investigation, Brazilian Federal Police, Israeli National Police, Dutch National Police, Europol, German Federal Criminal Police (the *Bundeskriminalamt*), Saxon Police (Polizeidirektion Zwickau) and LEAs in the United Kingdom. The US Department of Justice's Office of International Affairs, Criminal Division's Money Laundering and Asset Recovery Section and the AlphaBay prosecution team also provided assistance (US Department of Justice 2019).

Law enforcement operations have moved beyond simply targeting the operators of hidden service darknet markets, but now also target 'information centres', such as hidden service search engines (eg Grams, Kilos, Recon). These hubs of information about darknet markets can be either accessible websites (eg DeepDotWeb, Darknetlive, dark.fail) or hidden services (eg Dread). They work as dictionaries containing links and information related to hidden services and are central to the 'darknet community' (Ladegaard 2019).

In May 2019, DeepDotWeb, a darknet news and information gateway that published links to darknet markets, was shut down by the FBI's J-CODE team (see Figure 2). Two Israeli nationals operated DeepDotWeb, one of whom ran the site from Brazil. Both were indicted for conspiracy to money launder by colluding with darknet market operators and receiving 'referral bonuses' or kickbacks for referring consumers to darknet markets. The site earned $US15m via Bitcoin transfers between November 2014 and April 2019, making money every time a purchaser used a DeepDotWeb referral link to buy illegal narcotics or other illegal goods (US Department of Justice 2019). The Dutch National Police also seized a Bitcoin laundering site that had made tracking Bitcoin transactions more difficult.

Disrupting 'information hubs' by seizure or DDOS impacts on darknet markets by restricting access to information about what sites are active, trustworthy and viable. This disruption could make it more difficult for newcomers to navigate the darknet market ecosystem and access contraband (Popper 2019).

While sometimes ending in prosecution, the results of these operations against darknet markets have largely been underwhelming—vendors and customers simply migrate to a surviving market (or a new one). Vendors sometimes migrate under a new alias and 'pretty good privacy' (PGP) key, which has a temporary disruptive effect because trust is the single most important metric for vendors on darknet markets (Van Buskirk et al. 2017). Thus, vendor migration essentially resets the displaced vendor's trust to zero. However, some newer markets have features that allow a vendor to bring their history or transaction statistics with them from a defunct market, but over the long term these 'trust credits' may restore a vendor's reputation to a limited extent. This vendor displacement appears like a game of 'whack-a-mole', and attempts to intervene in darknet market operations are often piecemeal and difficult to sustain, resulting in only temporary deterrence. We re-examine such findings and explore other potential impacts of darknet market closures.

Research has shown intervention in darknet markets causes limited disruption. The most common finding in the literature is that, following each LEA operation against darknet markets, the availability of contraband shrinks initially before rebuilding (Ladegaard 2019; Soska & Christin 2015). When Silk Road 1.0 was closed and its principal, Ross Ulbricht, was arrested by US law enforcement in 2013 (Zetter 2013), it was assumed that this would have a deterrence effect on imitators (Popper 2019). However, buyers and vendors quickly migrated to other hidden services or markets with similar infrastructure to Silk Road 1.0 (Décary-Hétu & Giommoni 2016; Popper 2019). Silk Road 2.0, for example, was launched within a month after the shutdown of Silk Road 1.0. In sum, a recent overview of the available data showed:

> …that only 17% of crypto-drug markets were closed down as a result of drug law enforcement interventions; the rest having been shut down because of exit scams, voluntary closure or hacking…only a small minority of those purchasing drugs in crypto-drug markets stopped using these markets because of drug law enforcement action – putting into question the efficacy of current drug control effort. (International Drug Policy Consortium 2018: 15)

Such a conclusion may underestimate the impact of LEA investigations and operations, particularly as these operations reinforce the self-regulatory conduct of many darknet platforms to prohibit the sale of 'unsafe' products such as child exploitation material, fentanyl (Broadhurst, Ball & Trivedi 2020), weapons (Broadhurst et al. forthcoming) and COVID-19 vaccines (Broadhurst, Ball & Jiang 2020).

Literature review

Regulation of illicit drug markets typically proceeds by targeting supply or demand. Demand control attempts to diminish drug consumption by reducing the number of users and/or the quantity of drugs consumed. Supply control attempts to reduce the availability of drugs and thereby increase prices. (The classical economic model of supply and demand in an open market predicts a reduction in use as prices rise and/or substitution of the drug in demand with an alternative; Department of Health 2017: 1.) Demand programs aim to impact drug use directly, while supply programs affect drug use indirectly. Traditional law enforcement interventions have had limited impact on the number of drug users or suppliers, or drug prices.

Previous LEA operations against drug supply on darknet markets (eg Operation Onymous in 2014 and Operation Bayonet in 2017) have been examined by several studies (Décary-Hétu & Giommoni 2016; Hull 2017; Ladegaard 2017a, 2017b, 2019, 2020; Soska & Christin 2015; Van Buskirk et al. 2017), which found short-term reductions in supply but little impact on price, with consistent evidence of actor displacement to surviving or new darknet markets (Décary-Hétu & Giommoni 2016: 67, 70–71). Hull (2017) also investigated price variation in drug listings using the same data as Décary-Hétu and Giommoni (2016) and found that interventions do not have a significant effect on drug prices in darknet markets. While listing prices did change, these changes correlated to the fluctuation in Bitcoin value and were not connected to darknet market LEA operations (Hull 2017: 10).

To explain this lack of price change, Décary-Hétu and Giommoni (2016: 71) suggest three possible reasons:

- vendors anticipate the high risk, and therefore their actions do not change as their expectations are being met;
- vendors keep their listings highly consistent but deliver a smaller quantity than advertised; and
- consumers usually dictate prices, not vendors, and thus prices stay consistent regardless of the threat to vendors.

For vendors, along with their clients, trust is central to the operation and success of darknet markets. Décary-Hétu and Giommoni (2016: 73) therefore proposed that law enforcement efforts could be tailored to disrupt the integrity of vendors on the market as opposed to shutting down markets, which inevitably reappear in new guises.

Miller (2019) used historical scrapes of darknet markets from 2014 to 2016. He also noted minimal lasting disruption following US LEA operations (eg Operation Onymous, which targeted Hydra and Cloud 9 in November 2014), but prices increased with the regulation of fentanyl and other novel psychoactive substances in China. Despite some regulatory success, fentanyl prices remained approximately 90 percent cheaper than heroin through this period.

By analysing vendor behaviour and practices, Bakken, Moeller and Sandberg (2018) described how darknet markets address the coordination problems found in traditional illicit markets—namely, the issues of competition, cooperation and validity. Darknet markets feature public information about vendors (eg vendor products and sales, vendor score or ranking, shipping profile) and the presence of multiple vendors increases the market competition in what would otherwise be a 'limited market' (Bakken, Moeller & Sandberg 2018: 446). Market 'rules' or conventions are reinforced by the vendor reputation or review system, the use of escrow and an active dispute resolution system. In short, darknet markets rely on trust instead of using threats of violence to enforce sales contracts (Bakken, Moeller & Sandberg 2018: 448). The public aspect of darknet markets mitigates the risk evaluation problems for buyers: vendors are able to publicly advertise their products, with alleged purity levels, brand names, product images, and detailed descriptions of their shipping practices (Bakken, Moeller & Sandberg 2018: 453).

Martin, Cunliffe, Décary-Hétu and Aldridge (2018) examined via a time series model the impact on the darknet opioid market of US restrictions on the prescription of the opioid hydrocodone implemented in 2014. They observed a sustained increase in the illicit trade in opioids on darknet markets, notably substitution of hydrocodone to the more potent oxycodone and fentanyl, as well as to less potent over-the-counter painkillers such as codeine. This study suggested a causal relationship between restriction in the legal supply of hydrocodone and an increase in the sale of substituted prescription opioids such as fentanyl, at least on US darknet markets. The increases in opioid sales were observed in markets that claimed to be based in the United States but not in those claiming to operate in Europe or elsewhere. This was a function of a consumer preference for purchasing from vendors who ship from the same country, also observed in related studies (Aldridge & Askew 2017; Dittus, Wright & Graham 2018).

Van Buskirk and colleagues (2017) attempted to measure the rate at which vendor numbers recover following interventions. They concluded that disruptions had a negligible effect on the rate at which vendor numbers increased. That is, disruptions had temporary but significant impacts on the overall number of vendors, yet the vendors recovered at a consistent rate—however, after a prolonged time, these numbers did not return to their peak figure. The authors suggested that disruptions, when employed in quick succession, could have a substantial impact on the ecosystem, potentially reducing the capacity of the darknet ecosystem to recover (Van Buskirk et al. 2017: 161).

Chan et al. (2019) examined the impact of LEA operations on vendor activity and sales transaction volumes in three darknet markets (Silk Road 2.0, Agora and Evolutions) during 2014 and early 2015. Using vendor listings and buyer reviews, they found that arrests of darknet participants reduced subsequent transactions, at least in the short term, and the number of active vendors declined, especially the number of short-tenure vendors. LEA operations appeared to disrupt markets also by slowing the time it takes replacement markets to reach critical mass or stasis, which reduced the volume of transactions. Buyers were sensitive to risk such as an arrest or market seizure, in particular when conducted by high-profile LEAs such as the FBI and Europol. Chan and colleagues (2019: 31–32) noted the reduction in transactions in response to policing and concluded trust may be more fragile once external risk signals were evident, despite the effectiveness of the market's protection in the past.

In general, LEA interventions see benefits immediately post-operation, but the rate of recovery and the development of new darknet markets overshadow the benefits. Furthermore, others argue that the publicity generated by police operations inadvertently makes darknet markets more active (Ladegaard 2017b; Martin 2014). If true, operations could have a net negative impact, which would help explain why some research finds an apparent lift in vendor activity and listings following major operations.

From a different angle, Ladegaard considers how the darknet market community reacts to law enforcement interventions. Analysing forum discussions, Ladegaard found that the community that forms around this ecosystem retains ideological motivations following disruption efforts. This is theoretically explained by techniques of neutralisation used by darknet players (see also Sykes & Matza 1957). This ideological context reinforces itself among new and established members and creates a feedback loop. The users of these platforms are typically educated and technologically aware. He notes that this community is, in the majority of cases, ideologically motivated (Ladegaard 2017a: 16) and educated (Ladegaard 2017b: 634). These factors are crucial to maintaining the social community following a law enforcement intervention; without the technical capabilities to create a new space for the community to interact, the whole thing would fall apart. But because these communities include capable individuals, these individuals will specialise in different topics and some will use their knowledge to assist the community without requiring monetary incentives to do so. They are part of, and contributing to, a community of like-minded individuals. The narrative adopted is akin to the common libertarian ideal of ‘society over government’—an ideal perhaps less central to market operators and vendors now than in 2014 and 2015, when Ladegaard’s data were collected. For Ladegaard a small core of actors comprised the central hub of this darknet market community. The resilience of these techno-criminal actors was only enhanced by law enforcement’s disruption techniques. By attempting to disrupt the community, LEAs actually strengthen trust within the community via collective efficacy, thus mitigating the longer term impact of police closures.

Bradley and Stringhini (2019) sought to gauge the darknet community’s response to LEA actions by observing two darknet-related forums on Reddit (/r/DarkNetMarkets and /r/dnmuk) that operated from November 2015 until both were banned in March 2018. The discussions covered Operation Hyperion, Operation GraveSac and Operation Bayonet. Operation Hyperion was an attempt by four LEAs (ie Swedish National Police, New Zealand Police, the FBI and Dutch Police) to ‘name and shame’ over 3,310 suspected darknet players in late 2016 by directly contacting suspected buyers and vendors or publicly naming them on darknet sites to discourage their further engagement. Operation Bayonet, as discussed above, involved the seizure of AlphaBay, while the preceding undercover takeover of Hansa (under Operation GraveSac) led to the exposure of vendors migrating to Hansa after the seizure of AlphaBay. From the qualitative analysis of the discussions it appeared that Operation Bayonet contributed to buyer risk awareness and had an impact on the darknet economy. Bradley and Stringhini (2019: 462) found that ‘Operation Bayonet resulted in more consequences for users being reported and that the use of Hansa as a honeypot caused serious immediate concern for the contributors who worried they had given data to the site’.

In a further study Ladegaard (2019) addressed the question of whether or not Operation Onymous and Operation Bayonet, in cracking down on concentrated online criminal activity, led to crime displacement, as offline law enforcement displaces crime to another geographical location. The key aspect to be considered is the digital reputation of vendors (Duxbury & Haynie 2018: 46; Ladegaard 2019: 113). The general displacement trend observed suggests that darknet market trading is highly resilient; counterintuitively, trade increased following media coverage in the wake of Operations Onymous (2014) and Bayonet (2017) seizures (Ladegaard 2019: 120).

Ladegaard's (2020) review of police crackdowns on the darknet economy argues that they also act as a catalyst for criminal innovation. Dread, a popular darknet forum, is illustrative. Dread experienced a prolonged and severe DDOS attack in late 2019 and early 2020, most likely an LEA operation rather than competitor disruption or blackmail, according to market observers. The effectiveness of the DDOS attack spurred the development of improved anti-DDOS tools, which have since been implemented across established markets such as White House and Empire. LEA seizures harden the operational security of darknet markets while reinforcing self-regulatory practices that further the trustworthiness and resilience of the darknet market ecosystem or economy. Reuter (1983, 2014) observed that in traditional black markets the pressure exerted by law enforcement on criminal enterprises also dispersed these criminal actors, making them 'disorganised crime'.

Method

This section outlines the procedures used to identify and analyse the effects of darknet market closures. Quantitative methods were used to investigate the potential effects of closures and seizure. We analysed the effect of market closures on product availability, especially opioid availability; vendor movement; market value; and price fluctuations. An overall product listings time series was constructed. We split the time series into several sub-intervals based on the closures of the eight markets originally selected.

To answer our research question about the effects of LEA closure, we first undertook a detailed descriptive data analysis of the trends and changes in fentanyl and other opioid availabilities over different time periods associated with closure events. Second, we made inferences based on the ARIMAX models fitted with an independent dummy variable indicating the intervention. The ARIMAX model extends the Auto-regressive Integrated Moving Average (ARIMA) model to perform multivariate (or univariate) regression analysis while also capturing the potential autocorrelation in the error term using ARIMA. Further *t*-tests were conducted to test the significance of the estimated coefficients and therefore the significance of the intervention effect. We also analysed prediction errors (defined as the difference between the predictions based on the previous period ARIMA model and the observed values) after inspecting their autocorrelation for any lag effect; and examined the intervention effect on 'standardised' listings (ie as the time periods varied, we divided the observed values by the number of trading days in each period).

This analysis allowed us to explore potential impacts of closures on darknet markets such as displacement, diffusion or dispersal, substitution and deterrence.

Displacement and diffusion were analysed in the 'spatial' sense—that is, whether the closed darknet market was replaced by another market or whether its vendors and clients moved to unidentified or new markets after the intervention. To assess this, we used ARIMAX modelling to quantify changes in the number of 'standardised' listings across all markets in different time periods to illustrate the displacement/diffusion effects in further detail. The temporal displacement/diffusion effect was also investigated by studying the lags in our constructed time series. The presence of general deterrence, given that the scope and size of the Tor universe are both unknown, is difficult to quantify. In this study, we briefly examine deterrence by inspecting the trend in total product listings and changes in the relative proportion of fentanyl available. A product substitution effect was examined by calculating the proportion of opioid/fentanyl listings across markets over different time periods.

To address the question of intervention effects, we compared the characteristics of time series after different types of market closures. This includes the measured intervention effects given ARIMAX models, autocorrelation in prediction residuals, and so on. A significant change in any of the characteristics would provide evidence that LEA seizure and other closures had different impacts.

Data collection

One of the challenges when collecting data from darknet markets is determining the true scope of the universe from which we seek to obtain a representative sample. To confidently employ representative sampling, it is necessary to know the scope and size of the universe (see Munksgaard, Demant & Branwen 2016). There are numerous markets active at any one time, and all of these need to be monitored if the impact of a closure is to be fully measured. The volatile nature of the Tor hidden service ecosystem makes this task daunting. Thus, precise measures of the impacts of closures must be qualified and may be further limited by the ability of vendors and buyers to change at will their pseudo-anonymous handles and PGP encryption, making the tracking of vendor movement across markets incomplete. This displacement of products or migration of vendors after seizures or closures may not be confined to one or two markets; market vendors and buyers, and to a lesser extent operators, can relocate to many potential market platforms or turn to small specialist or niche markets. Thus, we observed as many markets as feasible before, during and after law enforcement operations.

Estimates of the number of active markets on Tor platforms vary. EMCDDA and Europol (2019) identified 103 darknet markets which had been active between 2011 and 2017, and Ladegaard (2020) identified 126 markets active between 2011 and 2016. But only 30 markets were active in mid-2016, of which a dozen were general or omnibus markets (Gilbert & Dasgupta 2017: 162). We estimate fewer omnibus markets may be active at any one time. Defunct sources such as the online information centre DeepDotWeb listed about 40 markets as being active in early 2019, although some were limited to a particular drug (eg cannabis) or sold only drugs.

Tracking buyer and vendor cryptocurrency transactions and validating sales of particular products was not possible. The overall activity of vendors is used as a proxy measure of likely impacts on customers of darknet markets. Buyer feedback has also been useful as a proxy measure of sales transactions (see Kruithof et al. 2016), although not without limitations (Norbutas, Ruiter & Corten 2020). Estimates of actual sales may be possible for some vendors on some markets and can be used to gauge vendor value; however, we measured the available stock by observing listings or product advertisements for opioids (excluding duplicates of these listings) rather than approximate sales.

Data were collected from a dozen Tor hidden services with a focus on opioids, particularly fentanyl and fentanyl analogues. Data collection was conducted over 352 days (from 2 January to 20 December 2019, excluding weekends), combining 251 scrapes from 12 omnibus darknet markets:

- Agartha;
- Apollon;
- Empire;
- Dream;
- Samsara;
- Nightmare;
- Tochka;
- Dream Alt;
- Berlusconi;
- Valhalla;
- Wall Street; and
- Cryptonia.

Initially we collected data from eight markets (Apollon, Berlusconi, Valhalla, Wall Street, Empire, Dream, Nightmare and Tochka) but later added three 'new' markets (Agartha, Dream Alt and Samsara) in April after the shutdown of Wall Street and Valhalla by law enforcement and the voluntary closure of Dream. In July we added Cryptonia after Nightmare closed in an exit scam. Cryptonia operated until a voluntary closure in November.

The data collection process used by the Australian National University Cybercrime Observatory is further detailed in Ball, Broadhurst, Niven and Trivedi (2019), which also addresses common concerns about data collection from darknet markets (see Munksgaard, Demant & Branwen 2016). Ball et al. (2019) described the method of crawling and scraping the pages of darknet markets and subsequent classification of products, as well as estimates of prices, quantities and vendor activity. The method produces an archived record of all webpages downloaded. The 'crawl and scrape' process is undertaken in two steps (ie the raw HTML pages are retained and parsed after the data collection) and this helps validate the data capture process. The crawler is designed to over-capture webpages—for example, if the Tor website indicates six pages of listings, we capture 10 pages). That enables us to account for listings that move during the capture process and ensure a more complete data capture. Disruptions are usually handled manually; we attempt various alternative URLs until we find one that is active, but if after 10 days we cannot retrieve any meaningful data from the market we consider it inactive or closed and cease collection.

Data were entered and analysed according to the date of product listings. Weekend activities were excluded from analysis due to limitations of data collection. We count unique listings to estimate product availability and all posted listings are used to track trends.

This data collection is (naturally) split into seven periods that account for closure events, as presented in Table 1.

Table 1: Data collection periods, 2019

Period	Dates	Market closures	Duration (days)
0	2 Jan – 14 Feb	Beginning of data collection until seizure of Valhalla	43
1	15 Feb – 26 Mar	Seizure of Valhalla until closure of Dream	39
2	27 Mar – 23 Apr	Closure of Dream until seizure of Wall Street	27
3	24 Apr – 24 Jul	Seizure of Wall Street until Nightmare exit scam	91
4	25 Jul – 27 Sep	Nightmare exit scam until seizure of Berlusconi	64
5	28 Sep – 28 Nov	Seizure of Berlusconi until Tochka exit scam	61
6	29 Nov – 20 Dec	Tochka exit scam until end of data collection	21

Each period ends with a market closure, but as the time periods vary (from 21 to 91 days), we divided the number of unique listings available in each period by the number of trading days to produce a standardised number of listings. We compared the availability of fentanyl and other opioids over time as events unfolded and described the impact of closures. Each of the monitored markets posted at least 1,000 products, and changes in the presence of opioids and fentanyl were tracked. All markets experienced some downtime over the data collection period. We report only unique product listings across all markets.

Limitations

A number of limitations to this study arise due to the volatility of the Tor network and, in particular, darknet markets. Even among active markets, downtime may still occur as a result of periodic DDOS attacks by competitors or extortionists, impeding data capture. Countermeasures used by darknet markets to prevent these attacks also led to data loss and frequent changes to data capture methods. DDOS techniques were also used by law enforcement agencies to disrupt darknet markets (Europol 2019). This led to inconsistent data capture for Wall Street in particular for period 1 and incomplete or absent price data for Agartha, Samsara and Cryptonia.

Without knowing the size and scope of the Tor universe and observing only selected active markets (even if among the largest general platforms) our sample is ill-defined, and estimations are limited by the absence of the relevant denominator. As previously noted, darknet market vendors often operate across multiple markets, using multiple aliases and PGP keys, making it beyond our capability to track these vendors' movements following market closures. As is typical of studies of darknet markets, data about buyers is generally unavailable and consumer behaviour is inferred rather than observed.

The reputation and sales performance of vendors may generally be deduced from buyer feedback and records of sales transactions. These data, if available, can help gauge actual rather than potential sales. However, these data also have limitations, as feedback systems may be gamed, and not all markets report sales transactions or tie sales transactions to particular products sold by a vendor. Also, the absence of feedback cannot be interpreted as an absence of sales (Ball et al. 2019; Norbutas, Ruiter & Corten 2020).

Seven of our 12 markets provided data on the overall sales of opioid vendors sufficient to examine general correlations between listings, vendors and reported sales. About half (48.6%) of the opioid vendors in our study recorded no sales of any products. Most vendors who reported sales transactions sold opioids as well as a variety of other drugs, and few were specialist sellers of fentanyl or other opioids. As expected, the number of opioid vendors and the number of listings of opioids are strongly (and significantly) correlated (Pearson's R=0.7810; t=3.9547, degrees of freedom (df)=10, p=0.0027), as were fentanyl vendors and fentanyl listings (Pearson's R=0.8405; t=4.907, df=10, p=0.000616). However, correlations between sales and listings of either fentanyl or opioids were weak (not significant) and negative (ie for opioid listings and sales Pearson's R was –0.1339; t=–0.3.4276, df=10, p=0.6782; for fentanyl availability and sales Pearson's R was –0.3074; t=–1.026, df=10, p=0.331). Most opioid vendors are generalists and sell a variety of contraband, so a correlation between all sales and opioid or fentanyl listings was not expected. Given the absence of a uniform and complete measure of sales, this dimension was difficult to interpret and was not included in the analysis of market and vendor activity.

Our analysis therefore uses modelling techniques that examine the availability of opioids as measured by listings, but listings may not necessarily reflect actual products shipped. When analysing the effect of a market's voluntary closure, Dream Market was our only observation, and this limits our ability to arrive at a general conclusion. Cryptonia also closed voluntarily, but we had insufficient follow-up data.

In the next section we describe opioid, fentanyl and carfentanil availability and then analyse the hypothesised effects of police operations.

Results

General findings

In a preceding study (Broadhurst, Ball & Trivedi 2020) we surveyed opioid listings on six darknet markets (Berlusconi, Dream Market, Empire, Tochka, Valhalla and Wall Street) from 2 January to 27 March 2019 and found fentanyl made up a small but significant proportion of the available opioid products. Of the 259,392 unique listings then identified, five percent (*n*=13,135) were opioids, of which 8.5 percent were fentanyl or its analogues (*n*=1,118)—only 0.43 percent of all listed products. Heroin and oxycodone accounted for half all the opioids listed, followed by tramadol, fentanyl, codeine and morphine. Small quantities of opium, methadone and buprenorphine were also found (Broadhurst, Ball & Trivedi 2020: 7).

Throughout 2019 we identified 2.09 million listings across all 12 markets, including a wide variety of digital or counterfeit products and illicit drugs. Of all these listings, 63,567 were opioids (3%) and of these five percent (*n*=3,151) were fentanyl and analogues—a mere 0.15% of all product listings. The highly potent carfentanil comprised nearly one in five of all fentanyl products available (19%, *n*=606).

Table 2 summarises the number of unique listings of opioids, fentanyl and carfentanil available for sale on all markets throughout 2019. Overall, Berlusconi contributed the largest proportion of opioid listings (36%) while Wall Street dominated the listings of fentanyl (55%) and carfentanil (42%) until its seizure, and Tochka accounted for 21 percent of fentanyl and 30 percent of the available carfentanil until its exit scam in November (period 6). Opioids generally accounted for only two to four percent of all the market listings, although Dream Alt offered the least opioids—less than one percent of all its listings.

The availability of opioid and fentanyl listings over time are shown in Table 3 as impacted by the closure or seizure of markets. Tochka carried the bulk of the fentanyl listings after the seizure of Wall Street until its exit scam in November (period 6). In the *Appendix*, the standardised listings (adjusted for the time differences between periods) are detailed for opioids (Table A1), fentanyl (Table A2) and carfentanil (Table A4, with unique listings in Table A3) for each market and subperiod associated with market closure. Table 3 reports unique listings of fentanyl and opioids on all markets for each period.

Table 2: Listings of all products, opioids, fentanyl and carfentanil by market

	All listings *n* (%)	Opioids *n* (%)	Fentanyl *n* (%)	Carfentanil *n* (%)
Valhalla (seized)	6,589 (0.32)	206 (0.32)	44 (1.35)	7 (0.89)
Dream (closed)	354,426 (16.96)	8,679 (13.65)	42 (1.29)	10 (1.27)
Wall Street (seized)	92,019[a] (4.40)	4,572 (7.19)	1,782 (54.81)	326 (41.48)
Nightmare (exit scam)	261,662 (12.52)	8,981 (14.13)	146 (4.49)	17 (2.16)
Berlusconi (seized)	755,726 (36.16)	22,888 (36.00)	171 (5.26)	91 (11.58)
Tochka (exit scam)	77,865 (3.73)	2,822 (4.44)	685 (21.07)	238 (30.28)
Samsara[b] (exit scam)	33,901 (1.62)	1,272 (2.00)	10 (0.31)	3 (0.38)
Cryptonia[b] (closed)	22,849 (1.09)	1,325 (2.08)	13 (0.40)	2 (0.25)
Apollon	93,718 (4.48)	2,338 (3.68)	10 (0.31)	4 (0.51)
Empire	272,516 (13.04)	6,470 (10.18)	311 (9.57)	75 (9.54)
Agartha[b]	82,347 (3.94)	3,546 (5.58)	32 (0.98)	11 (1.40)
Dream Alt[b]	36,076 (1.73)	468 (0.74)	5 (0.15)	2 (0.25)
Total	**2,089,694 (100)**	**63,567 (100)**	**3,151 (100)**	**606 (100)**

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1; the estimated number of all listings found on Wall Street as at 23 Feb 2019 is reported here

b: Replacement market added after seizure of Wall Street

Note: Percentages add to column totals

Table 3: Opioid and fentanyl listings by markets and data collection period, 2019 (*n*)

Opioids (Fentanyl)	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Valhalla	206 (44)	Seized					
Dream	6,524 (24)	2,155 (18)	Closed				
Wall Street	1,960 (621)	450[a] (447)	2,609 (714)	Seized			
Nightmare	43 (1)	51 (0)	1,858 (7)	7,029 (138)	Exit scam		
Berlusconi	288 (57)	112 (34)	295 (23)	4,654 (30)	17,539 (27)	Seized	
Tochka	369 (33)	106 (14)	191 (46)	825 (225)	740 (200)	591 (167)	Exit scam
Samsara[b]				197 (0)	608 (9)	467 (1)	Exit scam
Cryptonia[c]					903 (4)	422 (9)	Closed
Apollon	9 (0)	0 (0)	0 (0)	191 (2)	526 (7)	963 (1)	649 (0)
Empire	116 (24)	30 (2)	367 (2)	2,978 (101)	1,904 (111)	904 (64)	171 (7)
Agartha[b]				1,056 (32)	652 (0)	1,143 (0)	695 (0)
Dream Alt[b]				224 (3)	178 (2)	63 (0)	3 (0)

a: Incomplete data capture of Wall Street occurred in period 1: opioid availability undercounted

b: Data collection for Samsara, Agartha and Dream Alt began in period 3

c: Data collection for Cryptonia began in period 4

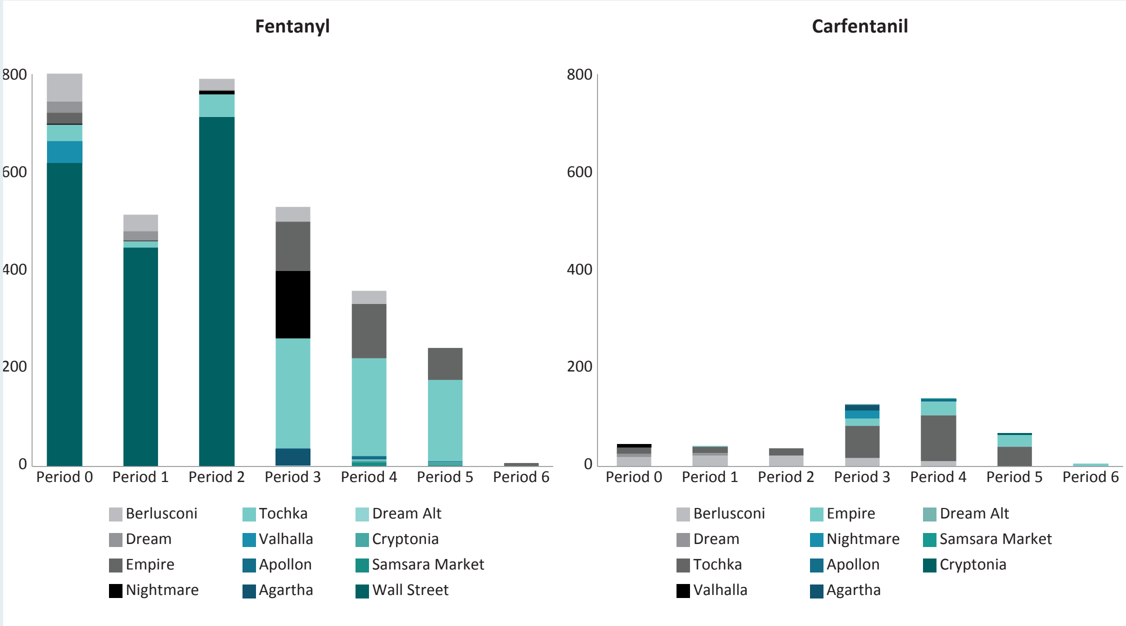
As shown in Table 3, opioid listings enjoyed strong growth across markets in March and April (period 2) after the voluntary closure of Dream and between April and July (period 3) after the LEA seizure of Wall Street. Berlusconi had the most opioid listings until its seizure in September (period 5) but also increased its opioid listings after Nightmare's exit scam. The majority of the markets offered relatively few listings of fentanyl (less than 1% of their overall listings), although fentanyl accounted for nearly two percent of all of Wall Street's listings (1.94%). Wall Street also had the largest proportion of carfentanil listings overall (0.35%), followed by Tochka (0.31%).

The proportion of fentanyl among opioid listings increased from eight percent to 21 percent after Valhalla ceased operation but dropped gradually with the closures of Dream and Wall Street. This indicates a substitution effect—with specific law enforcement operations targeting fentanyl, some vendors switched to other products, presumably to mitigate risks (see Table A7 in the *Appendix*).

Figure 3 shows the number of fentanyl and carfentanil listings across the seven data collection periods associated with market closures and visualises Table 3 (and Table A4). In both cases, Wall Street dominated the markets in the first three periods, until its seizure, after which Tochka took over the dominant market share. The entrance of new markets also made up some market share.

A common self-regulatory (or self-preserving) practice among most markets is to prohibit certain products such as child abuse images, firearms, poisons and assassination services, which are deemed likely to attract law enforcement attention. Tochka imposed no such ban on the sale of fentanyl. The majority of carfentanil listings (based on the 47.8% of listings that reported the physical form) were shipped as powder (78.18%), while others were offered in solution (11.36%), patch (7.27%) or blotter form (3.18%).

Figure 3: Number of fentanyl and carfentanil listings across darknet markets in 2019



Among all the opioids listed, carfentanil is of particular interest given its potency and higher risk of fatality. Nearly all (97.71%) of the carfentanil listings were found in the original markets. By the end of our data collection period, carfentanil listings were observed only on Empire, with only five listings identified (Figure 3; Table A4). In terms of total carfentanil listings, Wall Street held the largest market share (41.48%), followed by Tochka (30.28%) and Berlusconi (11.58%). In the replacement markets, Agartha had the most listings in period 3 but it ceased listing carfentanil thereafter, due to a self-enforced ban on the sale of fentanyl.

Opioid vendors

After accounting for duplicate pseudonyms, 4,156 unique opioid vendors were identified as actively listing in at least one period, and some listed throughout 2019. The Jaro–Winkler method (van der Loo 2014) was used to link variations in a vendor's pseudonym or handle and merge identical or similar vendor pseudonyms (Jaro–Winkler Score ≥0.90). These variations occurred more frequently for those vendors active across more than one market but also occurred occasionally over time for vendors operating in only one market.

About three-quarters of vendors (*n*=3,090, 74.3%) operated in only one market. However, this finding assumed that vendors operated with a single pseudo-identity rather than multiple identities and consequently may underestimate the actual level of cross-market activity. Four vendors were active across 10 markets and a small proportion were active across five or more markets (*n*=172, 4.1%) and a further 591 vendors (14.2%) were active across at least two markets. Similar findings on a smaller scale were observed in respect of fentanyl and carfentanil vendors. Almost one in five opioid dealers sold fentanyl (*n*=793, 19.1%) but only eight percent of these (*n*=64) listed on more than one market, heightening the impact of a key market or vendor ceasing operations. Over a quarter of the fentanyl dealers (*n*=212, 26.7%) also sold carfentanil, and 13 of these (6.1%) sold across just two markets. Most vendors appear to be generalists, listing many types of illicit drugs or other contraband. However, several vendors specialised in fentanyl and carfentanil, often selling larger quantities.

The number of active vendors varied over time in response to market closures, with the largest concentration occurring after the demise of Dream and Wall Street. Changes in the number of active vendors in each time period are summarised in Table 4. A detailed breakdown of vendors by market and period can be found in the *Appendix* (Table A8).

Table 4: Opioid, fentanyl and carfentanil vendors across all markets, by data collection period, 2019 (*n*)

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Opioid	1,764	1,084	1,550	2,663	2,283	1,551	785
Fentanyl	252	118	310	298	282	164	20
Carfentanil	45	41	37	127	138	67	5

Note: 110 pairs of vendors with Jaro–Winkler scores larger than 0.90 were merged

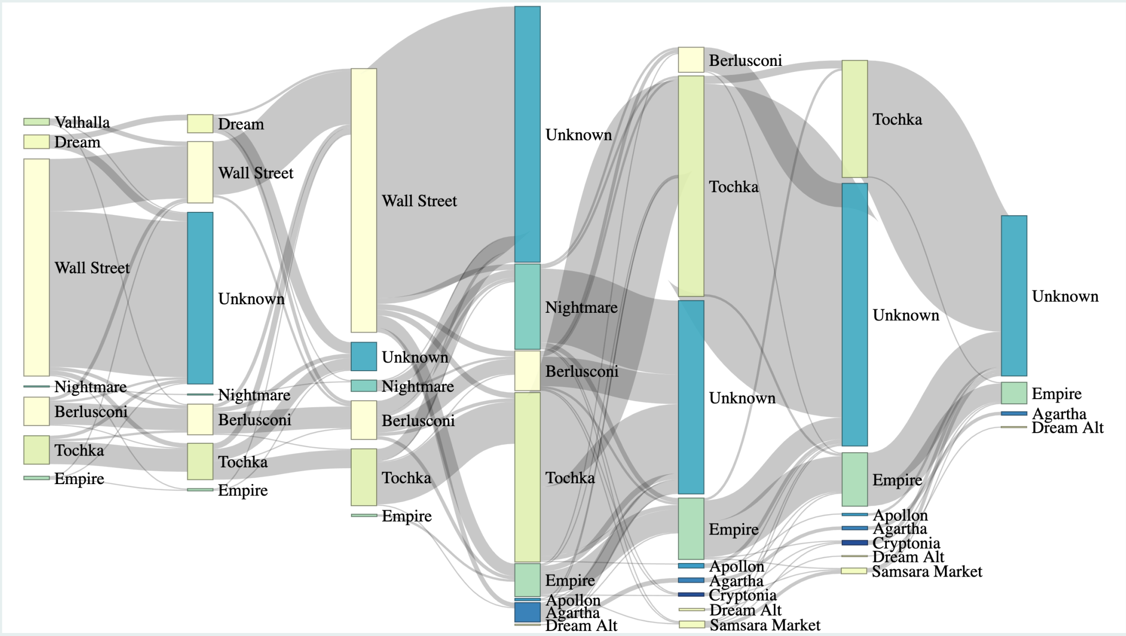
Table 4 and Table A8 show similar trends in the numbers of active vendors listing opioids, fentanyl and carfentanil—a trend also similar to that found for listings (see Table 3). The number of active vendors peaked in the middle of our collection period and then declined. The number of opioid vendors peaked in April–July (period 3) at 2,663 and thereafter declined to less than a third (*n*=785) of this number. This decline occurred because the remaining markets (Apollon, Empire, Agartha and Dream Alt) were less active and Apollon and Agartha claimed to have banned the listing of fentanyl and carfentanil. When in operation, Dream and Wall Street had the highest number of opioid vendors. After their closures, there was a significant increase in opioid vendors in the remaining markets, especially Nightmare and Berlusconi, indicating significant vendor displacement and dispersion.

The number of active fentanyl vendors peaked in March–April (period 2) at 310 and then reduced to 164 by November (period 5) following the seizure of Berlusconi. By December (period 6) the number of fentanyl vendors had fallen to 20 after the exit of Tochka, with only a handful remaining active on Empire. The number of vendors had reduced to less than a tenth (6.4%) of the peak in March–April. Wall Street was, as noted, the largest fentanyl marketplace, and after its closure we observed an increase in fentanyl vendors on both Tochka and Empire. The presence of carfentanil vendors peaked in July–September (period 4) with 138 identified. Most carfentanil vendors advertised on Tochka and Empire, which in turn became the two largest fentanyl-listing markets after Wall Street was seized by J-CODE.

Opioid vendor movements across different time periods are mapped in Figure A3. Carfentanil vendors are described in Figure A5 and fentanyl vendors are illustrated below in Figure 4. For example, six fentanyl dealers were active on Valhalla and four of them moved to Wall Street, another to Berlusconi, and one to an unknown or untracked darknet market. However, of the 232 fentanyl vendors (almost 30% of all known fentanyl vendors) active on Wall Street when it was seized by German police in April (period 2), 202 disappeared—that is, they did not reappear on any tracked market with the same pseudonym or they moved to an active but untracked market. Thirty vendors who had been on Wall Street dispersed to other active markets such as Empire (*n*=11), Berlusconi (*n*=5), Tochka (*n*=5), Nightmare (*n*=5) and Agartha (*n*=4). While the number of opioid vendors increased across each market before each closure, the number of active fentanyl vendors across all markets decreased, even though there were notable increases after Wall Street was seized. This suggests that some vendors substituted fentanyl for other opioids.

After market closures, vendors generally dispersed and scattered (diffused) to other markets—either the remaining original markets or new markets—but displacement (shifting to a popular robust market) also occurred. A significant proportion of vendors did not reappear on any of our surviving markets. This disruption could either signify deterrence (vendors stopped supplying opioids or fentanyl) or diffusion, where vendors moved outside our known darknet markets to untracked markets. Vendors may also have used new handles or pseudonyms when moving to another active market. Figure 4 is a Sankey or flow diagram of changes in the fentanyl vendor population over time and illustrates the proportional flow or shift in the numbers of vendors. Note the consistent ‘disappearance’ of vendors (mapped in Figure 4 as ‘unknowns’) after each closure, which suggests displacement or dispersal to untracked and unknown markets or perhaps desistance.

Figure 4: Fentanyl vendor movement after market closures



Note: The market decompositions are illustrated according to different market closures in each time period

Market value and prices

The prices analysed in this report are the unit listing price (in Australian dollars) after adjusting for purity, if reported, in the vendor's listing or darknet advertisement. (For details of the method used, refer to Ball et al. 2019.) Market capitalisation sums the values that are estimated from the total value of a market's relevant listings once duplicates are removed. These posted values may also be inflated with holding values and do not reflect actual sales transactions but the optimal value of a market and vendor's assets. We analyse the medians, considering the highly volatile variations in listing prices and some extreme holding prices. Table 5 presents the market values for opioids and fentanyl adjusted for variations in market duration. The adjusted values reported are the daily average value of opioid or fentanyl listings and may not reflect actual sales.

Tochka had the highest market capitalisation of A$44,480,450 for opioids, followed by Berlusconi (A$18,873,912) and Nightmare (A$11,509,653). Considering different markets operated in different time frames, 'standard' market capitalisations—the averaged market capitalisations on each business day—were calculated. Again, Tochka led with a standard market capitalisation of A$134,789. Dream was the second largest, with A$130,602, followed by Berlusconi and Nightmare. With respect to fentanyl, Tochka again ranked first with an estimated A$44,300 standard market capitalisation, followed by Wall Street, Valhalla and Dream. Prior to their closures, Tochka and Dream were also the two largest darknet markets in terms of market capitalisation (see also Table A2 in the *Appendix*).

Table 5: Market capitalisations and standard capitalisations for opioids and fentanyl

Market	Monitored operating period (days)	Opioid market capitalisation (A$)	Opioid standard market capitalisation (A$)	Fentanyl market capitalisation (A$)	Fentanyl standard market capitalisation (A$)
Tochka	330	44,480,450	134,789	14,619,038	44,300
Dream	83	8,599,003	103,602	129,375	1,559
Berlusconi	247	18,873,912	76,412	213,251	863
Nightmare	203	11,509,653	56,697	83,180	410
Wall Street	111	5,764,024	51,928	2,585,550	23,293
Empire	334	3,980,988	11,919	345,464	1,034
Valhalla	43	238,207	5,539	212,973	4,952
Apollon	334	1,496,407	4,480	12,719	409
Dream Alt	157	283,222	1,803	4,355	28

Note: All figures are rounded to whole numbers. Price data were unavailable for Agartha, Samsara and Cryptonia and they are excluded from this analysis. Estimates for Wall Street exclude missing data for all opioid listings in period 1

We also looked for changes in the price of opioids and fentanyl as markets closed or were seized. Given the presence of many outliers, the mean price of opioids or fentanyl was an unreliable measure, so we report the median price of opioids (including fentanyl) and fentanyl (including carfentanil) across the markets and respective periods in Table A9. The much lower cost of fentanyl compared to other opioids such as heroin or oxycodone is most evident in January–March (period 0, period 1), when its value was just one-twelfth of the value of other opioids. But by September–November (period 5) its relative cost had risen to nearly one-third and by December (period 6) to over half of the median price of other opioids.

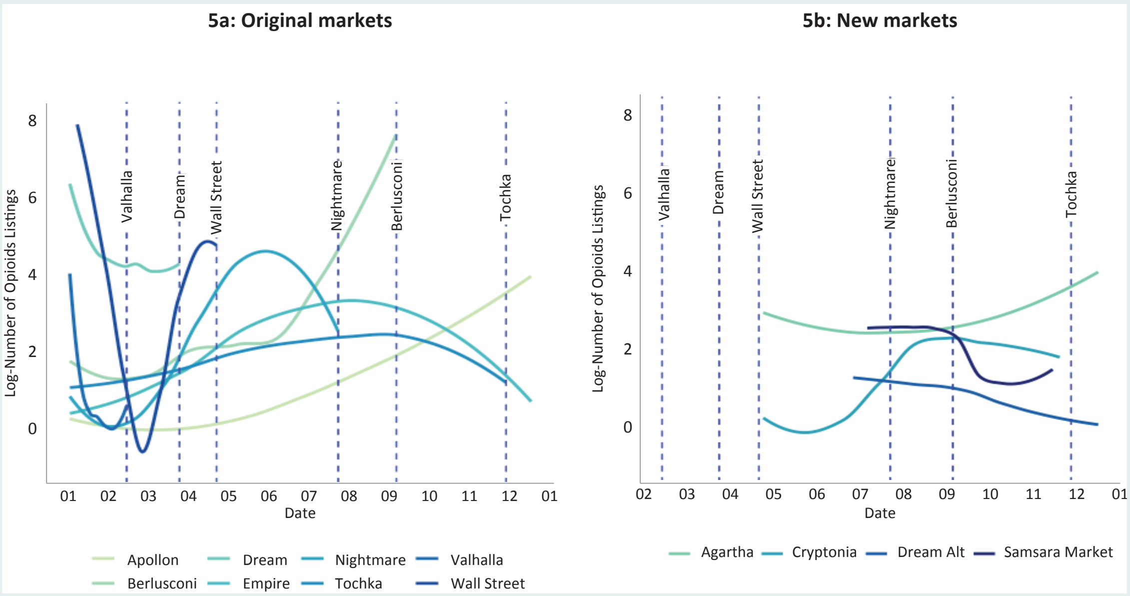
The median price of opioids declined over time but peaked at $429 (per listing/per gram) in July–September (period 4) before falling to $241 in November–December (period 6), although the overall median price across all periods was estimated to be $358. Going against this trend, Tochka increased the price of opioids to a median price of $966 per gram after Wall Street was seized. With the demise of Nightmare, Tochka's median increased to $1,167 prior to its exit scam in November. The price and availability, consistent with its leading place in the supply of opioids and fentanyl, are indicated in Table 4. The median price of fentanyl, on the other hand, increased from a low of A$25 in period 2 prior to Wall Street's seizure, to $123 in period 6 after Tochka's exit scam—significantly higher than the overall median price of $47. In short, fentanyl prices increased as both markets and dealers disappeared or substituted fentanyl for other opioids or products, with those remaining raising the price as availability decreased.

Opioid availability

The log-opioids listings are shown in Figure 5. We use log values to accommodate differences in scale across the markets and to reduce the scale of variance for analysis. The same figures with 95 percent confidence intervals are presented in Figure A1 in the *Appendix*. The confidence intervals are narrow around the fitted values, indicating relatively high estimation accuracy. However, the smoothing oversimplified the trend of Wall Street's listings after Dream's closure.

The original data showed two peaks—one before the closure of Dream and one after. As noted, four replacement markets commenced halfway through our collection. As most of our darknet markets ceased operations, Apollon and Agartha picked up the most opioid listings and showed a tendency for further growth towards the end of our data collection period.

Figure 5: Log-opioid listings for original markets and new markets over time



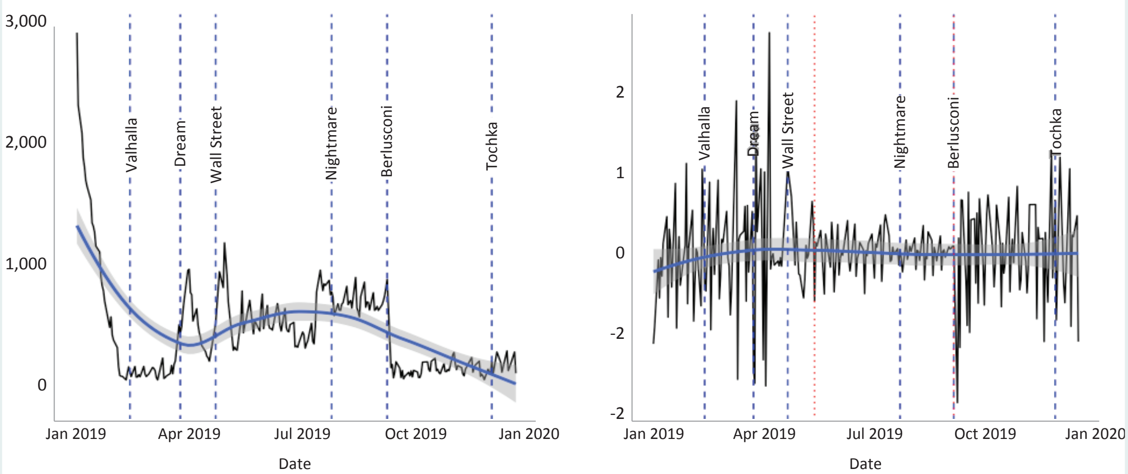
Note: All trends were smoothed using the 'local polynomial regression fitting' (Loess) method with a uniform span=0.75. The vertical dotted lines represent the dates of market closures

We observed increases in listings in most markets in periods 3 and 4, especially for Berlusconi and Nightmare. This was likely the result of the closure of two major players—Dream and Wall Street. The replacement markets also contributed some listings after the closure of Wall Street and Berlusconi. Their inclusion harmonised the trend of total listings. However, whether these increases were due solely to displacement from the closed markets remains uncertain, as some vendors may have moved to untracked markets. We describe these trends by market in Figure 5.

To observe the intervention effect, we constructed a time series of the total opioid listings across all markets and analysed the increments of the log-listings shown in Figure 6b. The number of total listings increased significantly following the closure of Dream and Wall Street and then declined to its original level after the shutdown of Berlusconi (Figure 6a). The increments show apparent non-constant variability (non-stationarity)—low volatility is, however, observed between the closures of Wall Street and Berlusconi. This was the longest period without any law enforcement closures. A change-point was detected for both the mean and variance on 15 May and 6 September 2019, prior to the closure of Berlusconi, and this supports the observation of low volatility in this period. We consider this illustrative of a stable recovery in the availability of opioids on the remaining darknet markets, which also corresponds to the rapid growth of most markets, as is detailed in Table 3 (see standardised values in Table A1). Given data limitations, the listings on Wall Street are not included in our time series.

Figure 6: Total opioid listings and change in the log of opioid listings over time

Figure 6a: Total opioid listings | **Figure 6b: Change in log-opioid listings**



Notes: Missing values occurred in Wall Street due to the difficulty of acquiring data daily. An approximation of Wall Street's opioid listings (using cubic smooth spline) is included in Figure 6a to illustrate the total trend. However, it is not included in Figure 6b because this cannot account for daily listing movements. In Figure 6b, the red dotted lines correspond to the change-points in mean and variance. The change-points are detected using the pruned exact linear time (PELT) algorithm (Killick & Eckley 2014) with normal distribution assumed for test statistics. The first observation (on 02/01/2019) is removed in Figure 6b, as duplicates from the previous period are included. The blue dashed lines represent the dates of market closures. Stineman interpolation is used to update missing values (Moritz & Bartz-Beielstein 2017)

The time series is split into seven separate periods based on closure dates of original markets. The new markets have smaller market capitalisations (see above) and fewer opioid listings, and also operated for shorter periods than the original markets. Their closures were expected to have less impact than the closure of the original markets.

We fit Auto-Regressive Integrated Moving Average (ARIMA) models with an independent variable or regressor to quantify intervention effects. The regressor is an indicator or dummy variable, which takes value 0 before intervention and value 1 thereafter. This model fits a linear relationship between total opioid listings and the presence of an intervention and describes the error terms with an ARIMA model. A non-seasonal ARIMA (*p*, *d*, *q*) consists of three components—the number of differencing transformations *d*, an autoregression (AR) term with order *p* and a moving average (MA) term with order *q*. All models are fitted in *R* using the 'auto.arima' function in the package 'forecast' (Hyndman et al. 2019). This function selects models with the lowest Akaike information criterion value. The *AR*(*p*) function captures the autocorrelation between consecutive observations and *MA*(*q*) accounts for the lagged forecast errors.

We fit such ARIMAX models on each of the two consecutive time periods with one market closure as the distinguishing event. The results are shown in Table 6. No seasonal effect was detected, and the analysis was limited by incomplete daily data for Wall Street in period 1. The closures of Wall Street, Berlusconi and Tochka were shown to have significant effects. Both Wall Street and Tochka's closures had a positive impact, which indicates diffusion (displacement to a strong established market and dispersal to other active markets). The seizure of these two markets by LEAs had the largest impact among all the market closures. Berlusconi's closure had a negative effect—evidence of possible general deterrence. However, no firm conclusion can be drawn given the restricted nature of our data collection.

Table 6: ARIMAX models on opioid listings

Market closures	Valhalla	Dream	Wall Street	Nightmare	Berlusconi	Tochka
ARIMA Error	ARIMA (1,0,1)	ARIMA (1,0,0)	ARIMA (0,0,2)	ARIMA (1,0,0)	ARIMA (0,0,1)	ARIMA (0,0,0)
Regressor	–0.4343 s.e.=0.3244	0.4035 s.e.=0.3013	1.3696 s.e.=0.2491	0.1840 s.e.=0.1416	–1.8523 s.e.=0.1031	0.3412 s.e.=0.1573
p-value[a]	0.1862	0.1875	0.0000	0.1973	0.0000	0.0338
Ljung–Box Chi-square[b]	6.0522 *p*=0.417	8.9477 *p*=0.177	9.02 *p*=0.172	6.9463 *p*=0.434	5.3402 *p*=0.618	6.9313 *p*=0.544

a: The *p*-value indicates the significance of the estimated coefficients using corresponding *t*-tests. Given a null hypothesis that the coefficient is equal to 0, we reject the null hypothesis if the *p*-value is less than 0.05

b: The Ljung–Box test examines the independence in the error terms. With the null hypothesis being that 'the errors are independently distributed', the model is considered a good fit if its *p*-value is larger than our chosen significance level of 0.05

Note: s.e.=standard error

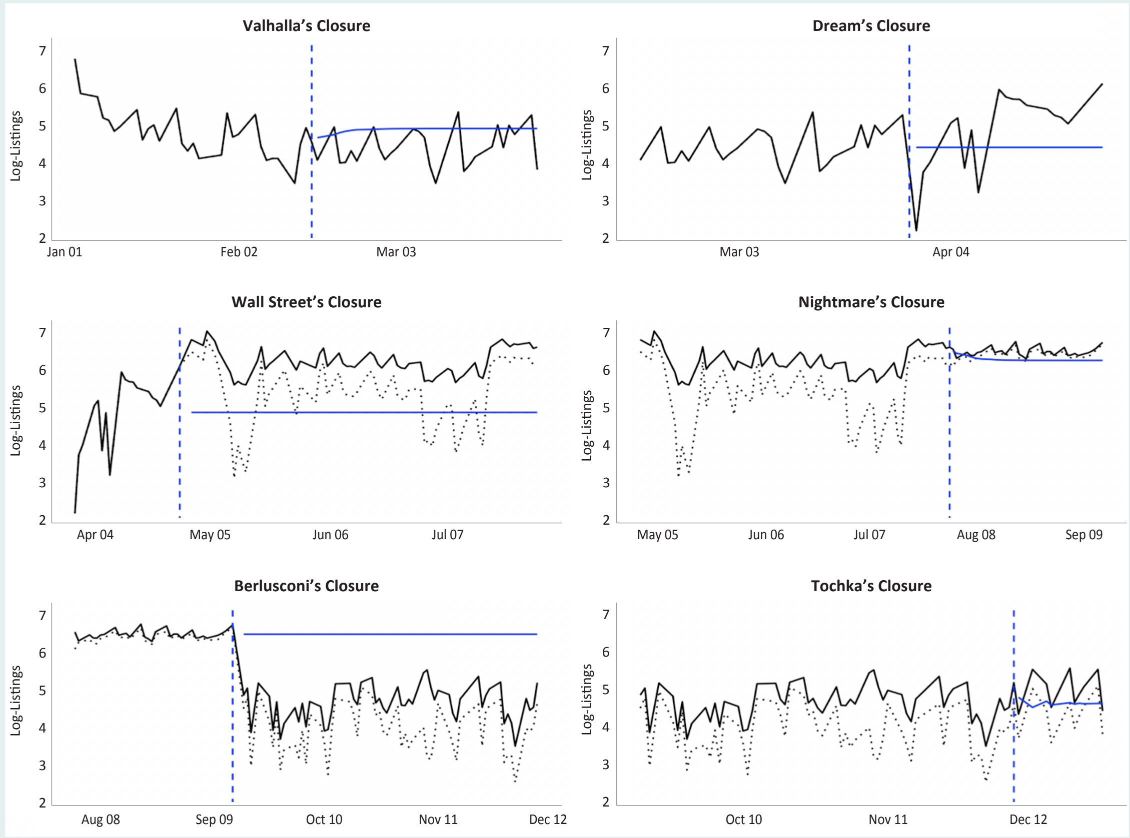
We further fit ARIMA models on each period as shown in Table A5 and A6. The forecasted log-total listings based on these ARIMA models and the observations are compared in Figure 7. Figure 7 shows that after the closure of Berlusconi the total listings dropped, with minimal recovery observed (consistent with the result in Table 6). Although no significant closure effect was detected for Dream (see Table 6), its closure appeared to have stimulated an increase in listings in other markets. However, few changes in listings were observed after Nightmare's exit scam. Valhalla's closure by Operation SaboTor and Finnish Customs was also followed by a relatively small increase in listings on other markets, although at least four vendors shifted to Wall Street.

Similar analyses were conducted on the original and new markets respectively. The total listings in new markets were extremely volatile given various market entry and cessation dates. However, the original markets displayed a more significant displacement effect following interventions, as shown in Figure 7. We suspect this was diffusion of vendors rather than displacement from original to new markets.

We compare these results with the standardised values of opioid availability in Table A1. Although we could not observe the opioid listing universe, our data showed signs of diffusion after market closures. Dream's closure accelerated the growth in opioid listings on Nightmare (5,162.3%), Empire (2,667.0%), Berlusconi (280.5%) and Tochka (160.3%). After Wall Street's closure by LEAs, we saw the emergence of new markets—Agartha, Dream Alt and Samsara. Some of the remaining original markets continued to grow. Berlusconi enjoyed rapid growth (368.1% in period 3 and 435.8% in period 4) after Wall Street's closure. Nightmare's closure was accompanied by growth in Apollon (291.6%), Berlusconi (435.9%) and Samsara (338.8%).

As a result, Wall Street's seizure by LEAs and the Tochka exit scam had the largest impact in terms of diffusion and dispersal as well as on the median price of fentanyl and other opioids. Their closures were shown to have raised the number of overall listings in our collection universe. In contrast, the closure of Berlusconi resulted in a decline in the number of total listings. Subsequent analysis showed that Dream's voluntary closure had the largest diffusion impact, resulting in a growth in listings on other markets. Apart from this dispersal, Dream's closure did not produce substitution or induce deterrence.

Figure 7: Impact of market closures on log-listings of opioids



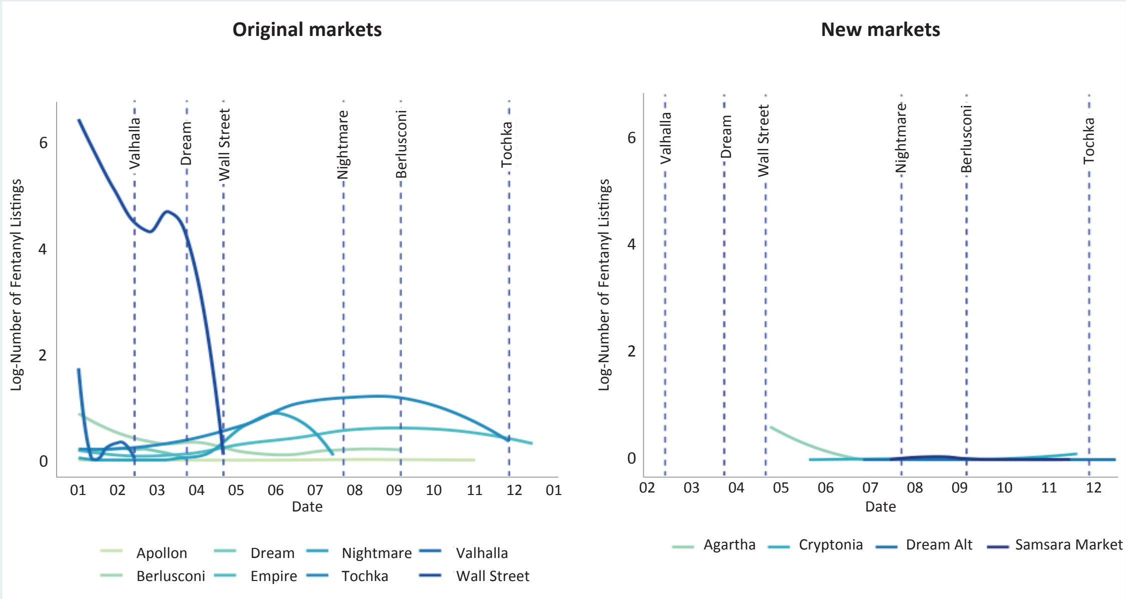
Note: The black lines represent observed values for all markets, while the dotted lines represent total log-listings for the original darknet markets. The blue lines are the forecasted log-listings for all markets based on the fitted ARIMA models

Fentanyl availability

We performed a similar analysis of fentanyl listings as we did for opioids in general. However, the declines in fentanyl availability were profound and recovery was not observed. Figure 8 displays the market breakdown of total fentanyl listings. Tochka emerged as the major player following the shutdown of Wall Street and there was little uptake of fentanyl among the replacement markets (see Table 3 and Table A2). Among the original markets, only Empire still offered fentanyl at the end of our data collection, but less was available than there had been in period 3, after the closure of Wall Street.

ARIMAX models were fitted on fentanyl listings for each of two consecutive periods. The results are reported in Table 7. Only Berlusconi's closure by police was found to have significantly reduced the overall number of fentanyl listings. The total fentanyl listings and increments are shown in Figure 8 and follow a similar pattern to those of opioids but on a smaller scale. However, the increments show more constancy. The stable period we observed for opioids was not found for fentanyl. Although the trend in fentanyl listings changes after the closure of large markets, these listings did not recover over time as rapidly as opioid listings. The median price of fentanyl also increased by 2.5 as the number of listings and dealers declined.

Figure 8: Log-listings of fentanyl across original markets and new markets in 2019



Note: All figures were smoothed using the local polynomial regression fitting (Loess) method with span=0.75. The dotted lines represent the dates of each market closure

Table 7: ARIMAX models on fentanyl listings

Market closures	Valhalla	Dream	Wall Street	Nightmare	Berlusconi	Tochka
ARIMA Error	ARIMA (2,0,0)	ARIMA (2,0,0)	ARIMA (1,0,0)	ARIMA (1,0,0)	ARIMA (1,0,0)	ARIMA (0,0,0)
Regressor	–0.0272 s.e.=0.1875	–0.1861 s.e.=0.4849	–0.8758 s.e.=0.5281	0.1991 s.e.=0.1417	–0.4951 s.e.=0.1296	–0.4415 s.e.=0.3011
p-value[a]	0.8852	0.7032	0.1015	0.1636	0.0003	0.1488
Ljung–Box Chi-square[b]	1.8708 *p*=0.931	9.3635 *p*=0.095	7.0203 *p*=0.427	11.0250 *p*=0.138	9.9231 *p*=0.193	15.1310 *p*=0.057

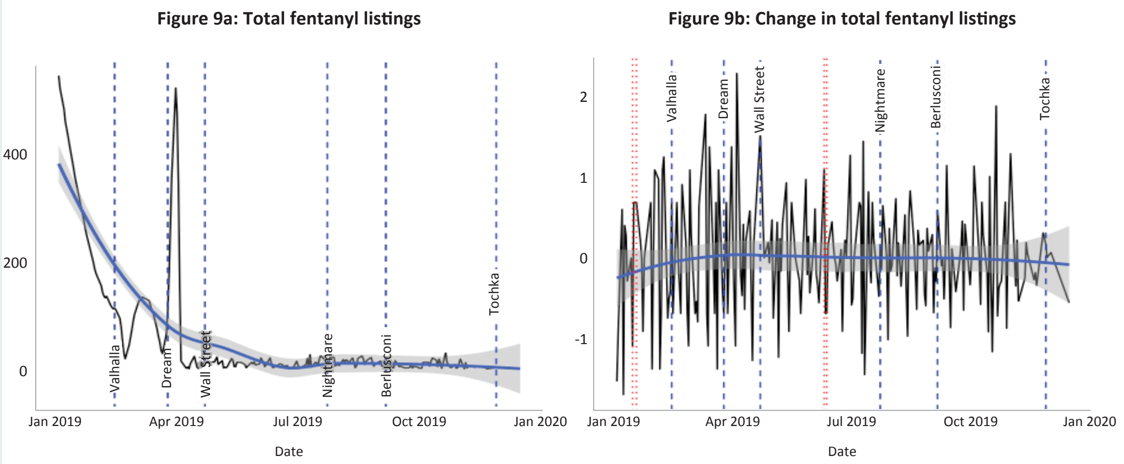
a: The *p*-value indicates the significance of the estimated coefficients using corresponding *t*-tests. Given a null hypothesis that the coefficient is equal to 0, we reject the null hypothesis if the *p*-value is less than 0.05

b: The Ljung–Box test examines the independence in the error terms. With the null hypothesis being that 'the errors are independently distributed', the model is considered a good fit if its *p*-value is larger than our chosen significance level of 0.05

Note: s.e.=standard error

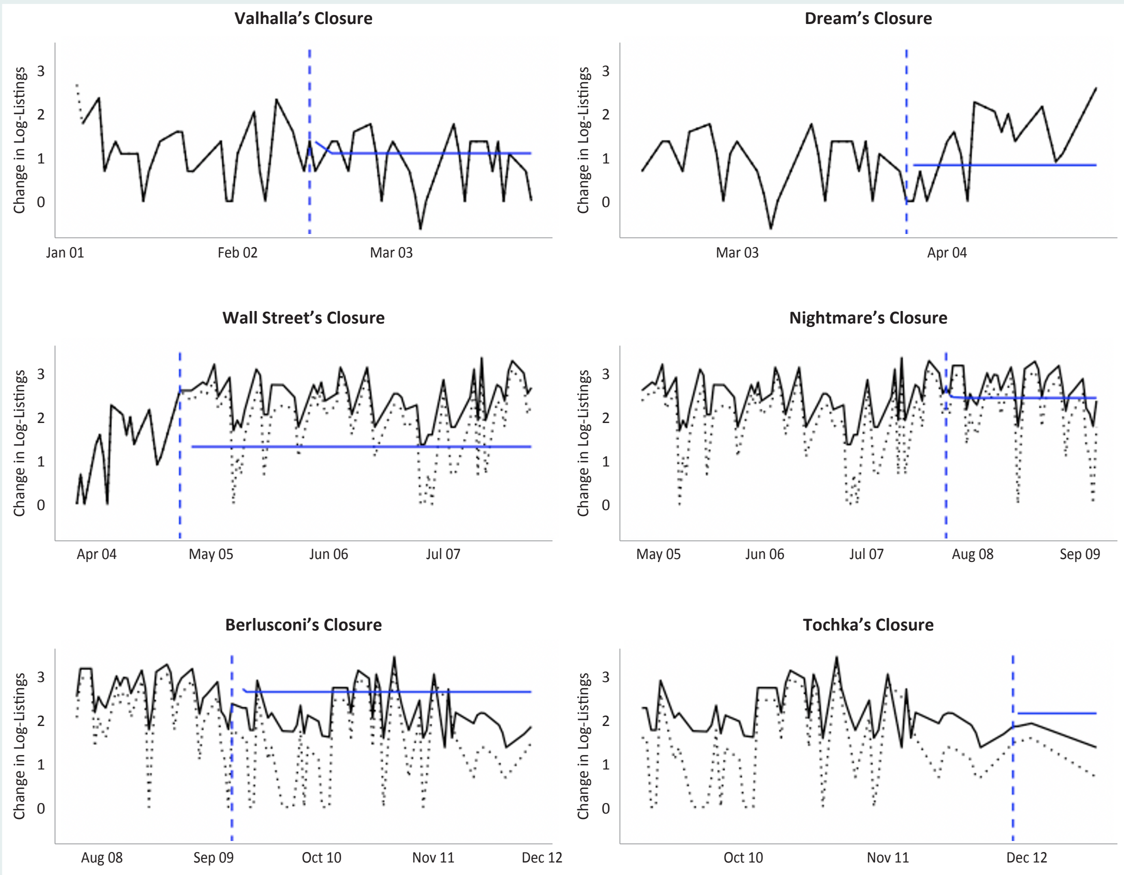
The logarithm of fentanyl listings in all markets and the original markets is shown in Figure 9. After the closure of Dream, overall fentanyl listings increased. The commencement of new markets did reduce the volatility in fentanyl listings, and this is evidence of diffusion from the original markets to new markets.

Figure 9: Fentanyl listings January to December 2019 and change in log-listings of fentanyl



Note: The dotted lines represent market closure dates; Stineman interpolation is used to update missing values; and the first observation (2 Jan 2019) was removed, as duplicates from the previous period are included. Wall Street's data is included in Figure 9a but not Figure 9b. In 9b, the red dotted lines correspond to the change-points in both mean and variance

Figure 10: Impact of market closures on log-listings of fentanyl



Note: The black lines represent observed values for all markets; the dotted lines represent total log-listings for original darknet markets, and the blue lines are the forecasted log-listings based on the ARIMA models fitted

The forecasted log-total listings based on the ARIMA models are shown in Figure 10, where listings before and after each closure are compared. A detailed description noting the rate of change is also reported in Table A2. Similar to the result for opioids, diffusion effects were observed for fentanyl on both the remaining original markets and replacement markets. Wall Street's closure had the largest impact on the growth of other markets. Since Table 5 showed Wall Street had the largest capitalisation, this result was expected.

Although no time series analysis was performed on carfentanil listings given limited observations, we constructed the same tables as for opioids and fentanyl to account descriptively for intervention effects (see Table A3 and A4). This shows a general deterioration in carfentanil availability on all our monitored markets. This may be a result of self-regulation (noting that Dream Market and Agartha had banned fentanyl), or a result of displacement and/or diffusion into the larger darknet universe. A minimal diffusion effect was also apparent after Nightmare's closure, with increases in carfentanil availability on Empire and Tochka.

Discussion

This research looked at the impact of darknet market closures on the availability of opioids—particularly fentanyl and carfentanil—in the Tor darknet economy. We observed dispersal to other markets after markets were closed. This is shown in the emergence of new markets and the growth in listings in the remaining original markets. Markets with higher market share or capitalisation tended to have a larger diffusion impact across the remaining or new (replacement) markets. Law enforcement seizures had a more significant impact than other forms of closure on the value of the markets and the reduced availability of fentanyl and the 'potential chemical weapon' carfentanil (Riches et al. 2012; Schwenk 2018).

Market operators and vendors have been conditioned by exit scams as well as frequent DDOS disruptions and have mitigated risks by moving (or dispersing) to functioning markets. The Tor darknet market milieu has adapted to volatility and this has encouraged vendors to operate across markets with similar fees, services and rules, and thus avoid the problem of 'putting all their eggs in one basket'. In short, players diversify to reduce risk. Highly active vendors operate in at least two markets, often with different pseudonyms, in anticipation of market closure. However, market-initiated closures, either scam or voluntary, usually do not heighten the risk of identification or de-anonymisation, although vendors may change handles and PGP keys when shifting to a new market.

Law enforcement operations are also likely to engender risk mitigation among surviving markets. Most markets discontinued the sale of high-risk products targeted by LEA such as fentanyl and carfentanil (along with already typically banned products such as child exploitation material, poisons and firearms), and this displacement increased listings on Tochka. Agartha (a replacement market in our study) prohibited the listing of fentanyl but not other opioids after Nightmare's July exit scam (period 4), but Tochka, apparently based in Russia, continued to offer fentanyl as a significant component of its opioid listings until its exit scam in late November (period 5). These adaptions suggest the possible role of deterrence, since perceived risks of LEA investigations targeting high-risk products combined with awareness of the changing investigative techniques and countermeasures could encourage substitution (ie an increase the availability of other opioid products instead of fentanyl) and desistance.

The forensic awareness of darknet market administrators and vendors appears to have been heightened after Operation Bayonet in 2017, which focused on AlphaBay (then the largest market), but also Hansa, a smaller market with overlapping or shared interests and actors. Netherlands police had already compromised Hansa and intercepted its encrypted digital traffic, leading to the arrest of dealers of narcotics and other contraband. Operation Bayonet was able to track some vendor and buyer migration to Hansa upon AlphaBay's takedown, flagging an increased risk in cross-market activity. Operation Bayonet increased the perceived risk of arrest among vendors and market operators, changing the way vendors managed pseudonyms and maintained continuity and trust across markets over time.

This study also described the impact of LEA market seizures and the arrest of key personnel on the supply of opioids and, in particular, on fentanyl availability. We found that law enforcement operations were linked to a reduction in the availability of fentanyl. Previous research had suggested the effect of police market seizures following Operation Onymous or Operation Bayonet was a temporary disruption and overall the Tor darknet economy recovered (Décary-Hétu & Giommoni 2016; Ladegaard 2019; Soska & Christin 2015; Van Buskirk et al. 2017). Operation SaboTor's seizure of Wall Street (then the dominant fentanyl outlet) and closure of DeepDotWeb, and Operation Darknet's seizure of Berlusconi (the dominant opioid outlet) offered a further opportunity to assess the impact of law enforcement interventions. Both closures substantially reduced the availability of fentanyl and opioids over all markets surveyed and both displacement and dispersal were observed. The reductions in the proportion of fentanyl found in the remaining markets suggest product substitution also occurred, with vendors offering oxycodone or other opioids instead of fentanyl.

As markets closed, vendors' handles or pseudonyms often switched to the remaining markets and many disappeared or discontinued (see Figure 4 and Figure A3). This was unlikely due directly to general deterrence or fear of arrest but rather changes in pseudo-identities or handles making tracking of their movement incomplete. Vendor handles are equated with a brand and become associated with trustworthiness, and seizures force vendors to re-invent themselves with a new handle and re-establish trust. However, this disruption may extend through the product supply chain. We cannot measure desistance, given the Tor darknet universe is unknown, but the data suggest some vendors also stopped selling fentanyl, perhaps deterred by a heightened perception of risk.

There was little evidence that different types of closures had different impacts or patterns of diffusion and displacement. However, we observed increases in both opioid and fentanyl listings after Dream's voluntary closure. Lags of two or three days were also detected in the prediction residuals after Dream's closure. This indicates that different vendors tended to react to Dream's closure in a similar way. One reason for the rapid dispersal was that voluntary closure allowed vendors to be informed and prepared to switch marketplace. Nevertheless, Dream was the only market whose voluntary closure we observed. (Although Cryptonia also closed voluntarily, we had insufficient follow-up to explore any displacement or dispersal to surviving or untracked markets.) Further analysis of the consequences of planned closures compared to seizures or exit scams is warranted.

A gradual decrease in fentanyl listings among all opioid listings was observed after the closures of Dream and Wall Street. Tochka's exit scam, late in our data collection period, further reduced fentanyl availability until there were only a small number of listings on only one market—Empire. The removal of markets, especially those that chose to continue making fentanyl available, greatly diminished supply, although opioid availability appeared to be recovering modestly until Berlusconi's seizure. The movement of vendors after a closure event allowed some tracking of displacement to other markets, with large numbers 'disappearing' but probably moving to unknown markets. One explanation is that the vendors had shifted to other products or other opioids (such as oxycodone) given the intense police and public health focus on fentanyl.

As noted in the *Method* section, a significant limitation to exploring the full effect of market closure is the size of the darknet universe, and thus how representative the present sample is of darknet opioid markets. We focused on general or omnibus darknet markets that offered over 1,000 listings for a wide range of contraband including opioids, although we could not verify the authenticity of the opioid products listed on the markets included in this study. Numerous single vendor or small niche drug markets and other dealers are also found on the Tor platform and so options to continue selling are plentiful. However, some surviving omnibus markets flourish and others rapidly enlarge or evolve to specialise in particular contraband such as opioids. Toolkits for creating darknet markets are available, allowing even novice vendors and market operators to set up new markets and exchange cryptocurrencies for scarce or prohibited goods (eg Eckmar's Marketplace Script 2.0 can be purchased for US$600; see https://bitcointalk.org/index.php?topic=5124640).

We also inferred from our findings that displacement and dispersal impacted on markets and vendors of targeted high-risk products such as fentanyl. With fewer vendors or markets able to supply fentanyl, prices increased as many dealers ceased selling or substituted other opioids to evade attention and remain under law enforcement's radar. Further research on the diversity and sales value of vendors, the mechanisms of product substitution (eg tramadol or oxycodone substituted for fentanyl), and the relationship between LEA operations and supply and pricing in volatile darknet market economies could help frame market and/or vendor targeting decisions. This requires a better grasp of the vendor population and the overall darknet economy.

The darknet economy and organised crime

The secrecy and efficiency of darknet markets allows this virtual black market to thrive and adjust to LEA countermeasures. The Tor platform allows for multiple illicit markets and hidden services and is ideal for creating anonymous connections and transactions across time and space and solves the secrecy versus efficiency trade-off essential to the continuity of conventional crime networks or groups (Morselli, Giguère & Petit 2007). Darknet markets reflect one growing dimension of the internationalisation of organised crime—cyber-enabled criminal services that operate across macro criminal networks (Spapens 2010) that are more or less 'dis-organised' criminal groups or enterprises without formal hierarchies or structures (Wall 2015; see also Reuter 1983).

Traditional illicit markets can be categorised as either ‘open’ or ‘closed’ markets. An open market is one where ‘anonymous sellers and buyers meet for a brief moment to exchange drugs and money at competitive prices’, while closed markets are those where social networks of peers trade drugs, hidden from law enforcement (Bakken, Moeller & Sandberg 2018: 443). The operational structure of these two types of markets is different: in the former, more emphasis is placed on customers than security, while in the latter the emphasis is on the requisite social networks which establish trust and reduce the risk of violence. The closed market format is the preferred option because a trusted supplier provides continuity and does not require buyers to seek new supply sources (Bakken, Moeller & Sandberg 2018: 444). Darknet markets exhibit properties of both open and closed markets. Firstly, as an open market, darknet markets are essentially public, as the only barrier to entry is the possession of the skills required to use the Tor browser and access darknet markets (Bakken, Moeller & Sandberg 2018: 444). Secondly, as a closed market, the review system (in which vendors build reputations) helps create a trusted network, with ‘the reputation system [formalising] the trustworthiness of participants’ (Bakken, Moeller & Sandberg 2018: 445). Ultimately, darknet markets ‘have achieved a balance of low risk and high level of traffic that appeals to both sellers and buyers’ (Bakken, Moeller & Sandberg 2018: 445).

We can speculate that these illicit markets function as small or medium sized criminal enterprises in a loose confederacy within a shared but decentralised infrastructure that allows collusion across markets and between vendors, which is further fostered by darknet forums and information centres. This differs from traditional illicit markets, which are often less efficient because secrecy acts as a barrier as well as a facilitator, unlike the ‘open’ forms of encryption in the digital marketplace. Darknet markets and forums are ideal ‘offender convergence settings’ (Kleemans, Soudijn & Weenink 2012). Kleemans (2014: 35; see also Reuter 1983) noted that the activities of criminal enterprises or networks share remarkable similarities with legal activities, and criminal actors can be ‘viewed as normal, rational, profit-oriented entrepreneurs who are involved in activities that, though illegal, are driven by the same laws of supply and demand as legal activities’. Nevertheless, the historical perspective dictates that ‘organized crime can be tackled effectively only by unified, decisive, incorruptible government’ (Fijnaut 2014: 354). This may be feasible in some jurisdictions—but safe havens for cybercriminals may be more plentiful than corruption-free policing agencies.

Illicit markets in the real world usually require protection by mafia-like groups or corrupt police to enforce illicit contracts using the threat of violence and are usually geographically confined, at least at the retail level. Darknet markets, on the other hand, rely on cybersecurity specialists, cryptocurrencies and Tor protocols to protect them from extortion, aggressive competitors and hostile takeovers. Conventional illicit markets are often vulnerable to well-organised LEA countermeasures aimed at a particular criminal enterprise, place or jurisdiction. Generally, constraints of illegality predict that most criminal enterprises will be small and short-lived (Kleemans 2014; Reuter 1983). This appears to be so for markets in the darknet economy.

An apparently endless consumer demand for illicit products of all kinds, however, sustains the darknet economy. Moreover, restrictions on supply do not eradicate demand; instead, they change the market conditions for criminal entrepreneurs (Kleemans 2014). Overall, darknet retail drug markets appear to avoid external constraints but 'without central and effective corrupt government involvement, drug markets are likely to be fragmented and competitive' (Reuter 2014: 376). Monopolies over darknet markets or particular products are consequently relatively uncommon. As with illicit markets in the real world, without collusion or symbiosis with LEAs, darknet markets are observed to be fragmented, risky (due to exit scams and seizures) and competitive. Small and large darknet enterprises, vendors and market providers create a retail hub that enables resellers and consumers to buy prohibited goods or services, while markets come and go.

Conclusion

The darknet market economy may be less susceptible than traditional illicit markets to LEA countermeasures such as undercover operations. Indeed, most successful LEA seizures of markets and arrests have been the result of happenstance, often errors on the part of vendors or administrators. Darknet markets are sustained by the maintenance of personal or trusted ties, a shared (virtual) space, secure communications, and relevant skills provided by darknet market administrators and community forums (Felson & Clarke 2012). Nevertheless, there is always an offline practical delivery component to any online transaction that allows the contraband to be intercepted by law enforcement (Aldridge & Askew 2017; Newman & Clarke 2003; Soska & Christin 2015: 45).

Previous research has suggested that the seizure of markets is disruptive to the supply of contraband such as drugs but that over the long term they recover and the effects on supply fade. This study has shown both the strengths and limitations of LEA operations, but interventions targeting particular products such as fentanyl and the markets most active in their sale can be effective. In this sense, interventions are more like a glass half full than half empty, since they also reinforce the risk aversion of both vendors and market operators, encouraging the banning of the sale of high-risk products such as fentanyl. Although bans are not always effectively moderated by market administrators, and vendors use obscure product descriptions, overall bans reduce availability. We observed many vendors describing opioid products as 'not fentanyl', and throughout 2019 the number of markets making fentanyl available decreased. Darknet markets are not entirely lawless or irrational but operate according to rules and conventions. These include the prohibition by many markets of some profitable but high-risk products. These prohibitions lead to the subsequent displacement of high-value, high-risk products to 'bulletproof' markets—for example, robust omnibus markets such as Tochka, which allegedly operates from servers inside the Russian Federation and outside the reach of transnational LEA operations, or niche markets too small to attract concerted LEA attention.

Operation SaboTor focused on opioids, especially fentanyl, and targeted markets like Wall Street, which were significant suppliers, and was successful in reducing supply and dispersing dealers. Operation Darknet seized the large and diverse Berlusconi market, pushing opioid (but not fentanyl) vendors to Apollon, Agartha and Empire and strengthening the role of these markets in the supply of opioids. This shows that displacement and substitution occurs at both the market and product level and both should feature in future targeted LEA operations. Recovery of the opioid market, and to a lesser extent the fentanyl market, was evident. New markets have since emerged that may also offer fentanyl and carfentanil on an unknown scale. Among our sample of darknet markets operating in 2019, only Empire and Agartha remain active at the time of writing (June 2020). Five Empire vendors continued to list fentanyl but no listings for carfentanil were identified. Agartha, however, did list numerous carfentanil and fentanyl products, reneging on its claim to have banned fentanyl and its analogues. The price of fentanyl also appeared to have increased, with vendors advertising one gram of fentanyl for $200 or more. However, new markets such as White House, Monopoly, Versus and Darkmarket appear to have self-regulated to reduce risk and have banned fentanyl listings.

The results show that LEA seizures are disruptive to darknet markets, forcing vendors to disperse or displace to an active market that may soon close (via an exit scam) or that may become the target of another LEA operation. Accordingly, vendors and market operators are adaptable and resilient, anticipating the volatility and risks inherent in the darknet market economy. A significant core of vendors and market specialists operate across markets, offering a diverse range of products, and are capable of starting over after closures or seizures. For the greatest disruption and impact on supply, law enforcement operations should focus on particular illicit products and their likely substitutes, the key dealers and markets involved, as well as the markets poised to replace the dominant markets and the high-value vendors operating across markets. LEA operations may stimulate innovation in these markets (Ladegaard 2020; Reuter 2014; Schelling 1965) but also put pressure on darknet markets to self-regulate and ban the most harmful products and services.

References

URLs correct as at August 2020

Aldridge J & 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. https://dx.doi.org/10.1016/j.drugpo.2016.10.010

Al-Nabki MW, Fidalgo E, Alegre E & Fernández-Robles L 2019. ToRank: Identifying the most influential suspicious domains in the Tor networks. *Expert Systems with Applications* 123: 212–26. https://dx.doi.org/10.1016/j.eswa.2019.01.029

Anderson R, Barton C, Böhme R, Clayton R, van Eeten MJG, Levi M, Moore T & Savage S 2013. Measuring the cost of cybercrime. In R Böhme (ed), *The economics of information security and privacy*. Berlin & Heidelberg: Springer: 265–300

Australian Criminal Intelligence Commission 2020a. Cybercrime. https://www.acic.gov.au/about-crime/organised-crime-groups/cybercrime

Australian Criminal Intelligence Commission 2020b. *National Wastewater Drug Monitoring Program Report no 9*. Canberra: ACIC. https://www.acic.gov.au/publications/reports/national-wastewater-drug-monitoring-program-reports

Australian Criminal Intelligence Commission 2019. *Illicit drug data report 2017–18*. Canberra: ACIC. https://www.acic.gov.au/publications/reports/illicit-drug-data-report

Australian Cyber Security Centre (ACSC) 2020. *ACSC Annual cyber threat report: July 2019 to June 2020.* Canberra: ACSC. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

Australian Federal Police & Northern Territory Police Force 2020a. *Darwin man charged with drug offences following joint police investigation*. Media release, 29 April. https://www.afp.gov.au/news-media/media-releases/darwin-man-charged-drug-offences-following-joint-police-investigation

Australian Federal Police & Northern Territory Police Force 2020b. Second Darwin man arrested with alleged links to dark web criminal network. Media release, 14 May. https://www.afp.gov.au/news-media/media-releases/second-darwin-man-arrested-alleged-links-dark-web-criminal-network

Ayling J & Broadhurst R 2014. Organized crime control in Australia and New Zealand. In L Paoli (ed) *The Oxford handbook of organized crime*. Oxford: Oxford University Press: 612–633

Bakken SA, Moeller K & Sandberg S 2018. Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology* 15(4): 442–460

Ball M, Broadhurst R, Niven A & Trivedi H 2019. *Data capture and analysis of darknet markets.* https://dx.doi.org/10.2139/ssrn.3344936

Bewley-Taylor D 2017. Narcotics Anonymous: Crypto-drug markets adapt to law enforcement intervention. *Jane's Intelligence Review* 29(6): 50–53. https://cronfa.swan.ac.uk/Record/cronfa36802

Bradley C & Stringhini G 2019. A qualitative evaluation of two different law enforcement approaches on dark net markets. *2019 IEEE European Symposium on Security and Privacy Workshops*, Stockholm, Sweden, 2019, pp 453–463. DOI: 10.1109/EuroSPW.2019.00057

Broadhurst R 2019. Child sex abuse images and exploitation materials. In R Leukfeldt & T Holt (eds), *Cybercrime: The human factor.* Routledge. https://ssrn.com/abstract=3384499

Broadhurst R, Grabosky P, Alazab M, Bouhours B & Chon S 2014. An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8(1): 1–20

Broadhurst R, Ball M, Foye J, Jiang C & Trivedi H forthcoming. Illicit firearms and weapons on darknet markets. *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology

Broadhurst R, Ball M & J Jiang 2020. *Availability of COVID-19 related products on Tor darknet markets.* Statistical Bulletin no. 24. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sb/sb24

Broadhurst R, Ball M & Trivedi H 2020. Fentanyl availability on darknet markets. *Trends & issues in crime and criminal justice* no. 590. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi590

Broadhurst R, Masters A, Smith RG & Brown R 2018. The state of organised crime research in Australia. In RG Smith (ed), *Organised crime research in Australia 2018.* Research Report no. 10. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/rr/rr10

Brown D, Farrier D, McNamara L, Steel A, Grewcock M, Quilter J & Schwartz M 2015. *Criminal Laws: Materials and commentary on criminal laws and process of New South Wales*, 6th ed. Federation Press

Brown R & Morgan A 2019. The opioid epidemic in North America: Implications for Australia. *Trends & issues in crime and criminal justice* no. 578. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi578

Chan J, He S, Qiao D & Whinston AB 2019. Shedding light on the dark: The impact of legal enforcement on darknet transactions. http://dx.doi.org/10.2139/ssrn.3468426

Chainalysis 2020. *The 2020 state of crypto crime.* https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

Commonwealth Director of Public Prosecutions (CDPP) 2019. *Case report: Jewel Victoria Griffiths – Drug importation.* https://www.cdpp.gov.au/case-reports/jewel-victoria-griffiths-drug-importation

Cornish DB & Clarke RV 1987. Understanding crime displacement: An application of rational choice theory. *Criminology* 25(4): 933–948. http://dx.doi.org/10.1111/j.1745-9125.1987.tb00826.x

Cronin MJ 2018. Hunting in the dark: Prosecutor's guide to the dark net and cryptocurrencies. *United States Attorneys' Bulletin* 66(4): 65–78

DarknetLive 2019. Australian police bust prolific darkweb vendor "NSWGreat". https://darknetlive.com/post/australian-police-bust-prolific-darkweb-vendor-nswgreat/

Décary-Hétu D & Giommoni L 2016. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change* 67(1): 55–75. http://dx.doi.org/10.1007/s10611-016-9644-4

Department of Health 2017. *National Drug Strategy 2017–2026*. Canberra: Department of Health. https://www.health.gov.au/resources/publications/national-drug-strategy-2017-2026

Dittus M, Wright J & Graham M 2018. Platform criminalism: The 'last-mile' geography of the darknet market supply chain. *Proceedings of the 2018 World Wide Web Conference on World Wide Web.* https://doi.org/10.1145/3178876.3186094

Dole J 2019. Police penetrate dark web, find $17m of drugs 'disguised as candy'. *ABC News,* 15 February. https://www.abc.net.au/news/2019-02-15/nsw-police-penetrate-dark-web-drugs-syndicate/10814548

Duxbury SW & Haynie DL 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

Edwards A & Levi M 2008. Researching the organization of serious crimes. *Criminology and Criminal Justice* 8(4): 363–388

EMCDDA—see European Monitoring Centre for Drugs and Drug Addiction

European Monitoring Centre for Drugs and Drug Addiction 2016. *The internet and drug markets.* https://www.emcdda.europa.eu/publications/insights/internet-drug-markets_en

European Monitoring Centre for Drugs and Drug Addiction & Europol 2019. *EU drug markets report 2019.* Luxembourg: Publications Office of the European Union

European Monitoring Centre for Drugs and Drug Addiction & Europol 2017. *Drugs and the darknet: Perspectives for enforcement, research and policy.* Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy

European Monitoring Centre for Drugs and Drug Addiction & Europol 2016. *EU drug markets report: In-depth analysis*. Luxembourg: Publications Office of the European Union

Europol 2019. Double blow to dark web marketplaces. Media release, 3 May. https://www.europol.europa.eu/print/newsroom/news/double-blow-to-dark-web-marketplaces

Federal Bureau of Investigation 2019. Operation SaboTOR: Federal partnerships key to dismantling online drug markets. https://www.fbi.gov/news/stories/j-code-operation-sabotor-032619

Felson M & Clarke RV 2012. Comments on the special issue. *Trends in Organised Crime* 15: 215–221. https://doi.org/10.1007/s12117-012-9165-1

Fijnaut C 2014. Searching for organized crime in history. In L Paoli (ed), *The Oxford handbook of organized crime*. New York: Oxford University Press: 53–95

Gilbert M & Dasgupta N 2017. Silicon to syringe: Cryptomarkets and disruptive innovation in opioid supply chains. *International Journal of Drug Policy* 46: 160–67

Greenberg A 2019. Feds dismantled the dark-web drug trade—but it's already rebuilding. *Wired*. https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/

Greenberg A 2018. Operation Bayonet: Inside the sting that hijacked an entire dark web drug market. *Wired*. https://www.wired.com/story/hansa-dutch-police-sting-operation/

Guardia di Finanza 2019. Three administrators of the black market called Berlusconi market, active in the dark web, arrested. *Guardia di Finanza inseima per la legalita*. https://www.gdf.gov.it/stampa/ultime-notizie/anno-2019/novembre/arrestati-tre-amministratori-del-black-market-denominato-berlusconi-market-attivo-nel-dark-web

Heidenreich S & Westbrooks DA 2017. Darknet markets: A modern day enigma for law enforcement and the intelligence community. *American Intelligence Journal* 34(1): 38–44. https://www.jstor.org/stable/26497115

Hobbs D & Antonopoulos GA 2014. How to research organized crime. In L Paoli (ed), *Oxford handbook of organised crime*. New York: Oxford University Press

Hull G 2017. *The effects of police interventions on darknet market drug prices* (Senior Theses). Claremont McKenna College. https://scholarship.claremont.edu/cmc_theses/1596/

Hyndman R, Athanasopoulos G, Bergmeir C, Caceres G, Chhay L, O'Hara-Wild M et al. 2019. Forecast: Forecasting functions for time series and linear models. *R package* version 8.7. http://pkg.robjhyndman.com/forecast

International Drug Policy Consortium 2018. *Taking stock: A decade of drug policy.* https://idpc.net/publications/2018/10/taking-stock-a-decade-of-drug-policy-a-civil-society-shadow-report

Johnson SD, Guerette RT & Bowers K 2014. Crime displacement: What we know, what we don't know, and what it means for crime reduction. *Journal of Experimental Criminology* 10(4): 549–571

Kadianakis G & Loesing K 2015. *Extrapolating network totals from hidden-service statistics.* https://research.torproject.org/techreports/extrapolating-hidserv-stats-2015-01-31.pdf

Killick R & Eckley IA 2014. Changepoint: An R package for changepoint analysis. *Journal of Statistical Software* 58(3): 1–19. https://www.jstatsoft.org/v58/i03/

Kleemans ER 2014. Theoretical perspectives on organized crime. In L Paoli (ed), *Oxford handbook of organised crime.* New York: Oxford University Press

Kleemans ER, Soudijn MRJ & Weenink AW 2012. Organized crime, situational crime prevention and routine activity theory. *Trends in Organised Crime* 15: 87–92. https://doi.org/10.1007/s12117-012-9173-1

Kruithof K, Aldridge J, Décary-Hétu D, Sim M, Dujso E & Hoorens S 2016. *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands*. Santa Monica: RAND Corporation. https://www.rand.org/pubs/research_reports/RR1607.html

Ladegaard I 2020. Open secrecy: How police crackdowns and creative problem-solving brought illegal markets out of the shadows. *Social Forces*. https://doi.org/10.1093/sf/soz140

Ladegaard I 2019. Crime displacement in digital drug markets. *International Journal of Drug Policy* 63: 113–121. https://doi.org/10.1016/j.drugpo.2018.09.013

Ladegaard I 2017a. We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *British Journal of Criminology* 58(2): 414–433. https://doi.org/10.1093/bjc/azx021

Ladegaard I 2017b. I pray that we will find a way to carry on this dream: How a law enforcement crackdown united an online community. *Critical Sociology* 45(4–5): 631–646. https://doi.org/10.1177/0896920517735670

Lavorgna A 2019. Cyber-organised crime: A case of moral panic? *Trends in Organized Crime* 22: 357–374

Leukfeldt ER 2015. Organised cybercrime and social opportunity structures: A proposal for future research directions. *European Review of Organised Crime* 2(2): 91–103

Leukfeldt ER, Kleemans ER, Kruisbergen EW & Roks RA 2019. Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime* 22: 324–345

Leukfeldt ER, Lavorgna A & Kleemans ER 2017. Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research* 23: 287–300

Lusthaus J 2013. How organised is organised cybercrime? *Global Crime* 14(1): 52–60

Maltz MD 1976. On defining “organized crime”: The development of a definition and a typology. *Crime & Delinquency* 22(3): 338–346

Martin J 2014. *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Palgrave McMillan

Martin J, Cunliffe J, Décary-Hétu D & Aldridge J 2018. Effect of restricting the legal supply of prescription opioids on buying through online illicit marketplaces: Interrupted time series analysis. *BMJ* (Clinical research ed). https://doi.org/10.1136/bmj.k2270

Martin J, Cunliffe J & Munksgaard R 2019. *Cryptomarkets: A research companion.* Emerald Group Publishing

May C 2017. *Transnational crime and the developing world*. Washington, DC: Global Financial Integrity. https://gfintegrity.org/report/transnational-crime-and-the- developing-world

Miller JN 2019. The war on drugs 2.0: Darknet fentanyl’s rise and the effects of regulatory and law enforcement action. *Contemporary Economic Policy* 38(2): 246–257. https://doi.org/10.1111/coep.12447

Moeller K, Munksgaard R & 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): 1427–1450

Moritz S & Bartz-Beielstein T 2017. imputeTS: Time series missing value imputation in R. *The R Journal* 9(1): 207–218. https://doi.org/10.32614/RJ-2017-009

Morselli C, Giguère C & Petit K 2007. The efficiency/security trade-off in criminal networks. *Social Networks* 29(1): 143–153

Munksgaard R, Demant J & Branwen G 2016. A replication and methodological critique of the study "Evaluating drug trafficking on the Tor Network". *International Journal of Drug Policy* 35: 92–96

Newman G & Clarke R 2003. *Superhighway robbery: Preventing e-commerce crime*. Cullompton: Willan

Norbutas L, Ruiter S & Corten R 2020. Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets. *International Journal of Drug Policy* 76. https://doi.org/10.1016/j.drugpo.2019.102635

Owenson G, Cortes S & Lewman A 2018. The darknet's smaller than we thought: The life cycle of Tor Hidden Services. *Digital Investigation* 27: 17–22. https://doi.org/10.1016/j.diin.2018.09.005

Paganini P 2019. Italian law enforcement shut down the 'Berlusconi market' black market and arrested three suspected of being its administrators, *Security Affairs*, 8 November. https://securityaffairs.co/wordpress/93603/cyber-crime/berlusconi-market-darkweb.html

Paoli L & Beken TV 2014. Organized crime: A contested concept. In L Paoli (ed), *The Oxford handbook of organised crime*. New York: Oxford University Press

Pardo B, Taylor J, Caulkins JP, Kilmer B, Reuter P & Stein BD 2019. *The future of fentanyl and other synthetic opioids.* Santa Monica: RAND Corporation. https://www.rand.org/pubs/research_reports/RR3117.html

Popper N 2019. Dark web drug sellers dodge police crackdowns. *New York Times,* 11 June. https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html

Reppetto TA 1976. Crime prevention and the displacement phenomenon. *Crime & Delinquency* 22(2): 166–177. https://doi.org/10.1177/001112877602200204

Reuter P 2014. Drug markets and organised crime. In L Paoli (ed), *The Oxford handbook of organised crime.* New York: Oxford University Press

Reuter P 1983. *Disorganized crime: The economics of the visible hand.* Cambridge, MA: MIT Press

Riches JR, Read RW, Black RM, Cooper NJ & Timperley CM 2012. Analysis of clothing and urine from Moscow theatre siege casualties reveals carfentanil and remifentanil use. *Journal of Analytical Toxicology* 36(9): 647–656

Schelling T 1965. Economics and criminal enterprise. *Public Interest* 7: 61–78

Schwenk M 2018. Chemical warfare agents: Classes and targets. *Toxicology Letters* 293: 253–263

Soska K & Christin N 2015. *Measuring the longitudinal evolution of the online anonymous marketplace ecosystem.* Proceedings of the 24th USENIX Security Symposium. Washington, DC: USENIX: 33–48

South Coast Register 2019. Police lay 22 additional charges against Cody Ward and Shanese Koullias over alleged Callala drug ring. *South Coast Register,* 31 May. https://www.southcoastregister.com.au/story/6193788/police-lay-additional-charges-over-callala-dark-web-drug-ring/

Spapens T 2010. Macro networks, collectives, and business processes: An integrated approach to organized crime. *European Journal of Crime Criminal Law & Criminal Justice* 18: 185–215

Sykes G & Matza D 1957. Techniques of neutralization: A theory of delinquency. *American Sociological Review* 22(6): 664–670. https://www.jstor.org/stable/2089195

United Nations Office on Drugs and Crime 2018. *United Nations Convention against Transnational Organized Crime and the Protocols Thereto* (July 2018). https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html

United Nations Office of Drugs and Crime 2005. *World drug report 2005*. New York: United Nations Publications. https://www.unodc.org/unodc/en/data-and-analysis/WDR-2005.html

US Department of Justice 2019. Administrators of DeepDotWeb indicted for money laundering conspiracy, relating to kickbacks for sales of fentanyl, heroin and other illegal goods on the darknet. Justice News, 8 May. https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales

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 der Loo M 2014. The stringdist package for approximate string matching. *The R Journal* 6: 111–122. https://CRAN.R-project.org/package=stringdist

van Wegberg R & Verburgh T 2018. Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In *Evolution of the Darknet Workshop at the Web Science Conference (WebSci 18)*: 1–5

Wall DS 2015. Dis-organised Crime: Towards a distributed model of the organization of cybercrime. *European Review of Organised Crime* 2(2): 71–90

Whetton S, Tait RJ, Chrzanowska A, Donnelly N, McEntee A, Muhktar A et al. 2020. *Quantifying the Social Costs of Pharmaceutical Opioid Misuse and Illicit Opioid Use to Australia in 2015/16.* Perth: National Drug Research Institute, Curtin University

White R, Kakkar PV & Chou V 2019. Prosecuting darknet marketplaces: Challenges and approaches. *United States Attorneys' Bulletin* 67(1): 65–80

World Economic Forum 2020. *The global risks report 2020.* https://www.weforum.org/reports/the-global-risks-report-2020

Zetter K 2013. How the feds took down the Silk Road drug wonderland. *Wired*, 18 November. https://www.wired.com/2013/11/silk-road/

Appendix

Table A1: Standardised opioid listings and change over time by market, 2019

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Valhalla	4.79	Seized					
Dream	151.72	55.26	Closed				
		−63.6%					
Wall Street[a]	45.58	11.54	96.63	Seized			
		−74.6%	737.3%				
Nightmare	1	1.31	68.81	77.24	Exit scam		
		30.8%	5,162.3%	12.2%			
Berlusconi	6.7	2.87	10.93	51.14	274.05	Seized	
		−57.1%	280.5%	368.1%	435.8%		
Tochka	8.58	2.72	7.07	9.07	11.56	9.69	Exit scam
		−68.3%	160.3%	28.2%	27.5%	−16.2%	
Samsara[b]				2.16	9.5	7.66	Exit scam
					338.8%	−19.4%	
Cryptonia[c]					14.11	6.92	Closed
						−51.0%	
Apollon	0.21	0	0	2.1	8.22	15.79	30.9
		−100%	–	–	291.5%	92.1%	95.8%
Empire	2.7	0.77	13.59	32.73	29.75	14.82	8.14
		−71.5%	1,667.0%	140.8%	−9.1%	−50.2%	−45.0%
Agartha[b]				11.6	10.19	18.74	33.1
					−12.2%	83.9%	76.6%
Dream Alt[b]				2.46	2.78	1.03	0.14
					13.0%	−62.9%	−86.2%

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

Note: Percentages rounded to one decimal place

Table A2: Standardised fentanyl listings and change over time by market, 2019

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Valhalla	1.02	Seized					
Dream	0.56	0.46	Closed				
		−17.3%					
Wall Street[a]	14.44	11.46	26.44	Seized			
		−20.6%	130.7%				
Nightmare	0.02	0	0.26	1.52	Exit scam		
		−100%	–	484.9%			
Berlusconi	1.33	0.87	0.85	0.33	0.42	Seized	
		−34.2%	−2.3%	−61.3%	30.0%		
Tochka	0.77	0.36	1.7	2.47	3.12	2.74	Exit scam
		−53.2%	374.6%	45.1%	−6.4%	12.4%	
Samsara[b]				0	0.14	0.02	Exit scam
					–	−88.3%	
Cryptonia[c]					0.06	0.15	Closed
						136.1%	
Apollon	0	0	0	0.02	0.11	0.02	0
		–	–	–	397.66%	−85.0%	−100%
Empire	0.56	0.05	0.07	1.11	1.73	1.05	0.33
		−90.8%	44.4%	1,398.3%	56.3%	−39.5%	−68.2%
Agartha[b]				0.35	0	0	0
					−100%	–	–
Dream Alt[b]				0.03	0.03	0	0
					−5.2%	−100%	–

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

Note: Percentages rounded to one decimal place

Table A3: Carfentanil listings by market over time, 2019 (*n*)

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Valhalla	7	Seized					
Dream	6	4	Closed				
Wall Street[a]	127	50	149	Seized			
Nightmare	0	0	0	17	Exit scam		
Berlusconi	19	0	0	17	11	Seized	
Tochka	13	14	15	65	92	39	Exit scam
Samsara[b]				0	2	1	Exit scam
Cryptonia[c]					0	2	Closed
Apollon	0	0	0	0	4	0	0
Empire	0	1	0	15	29	25	5
Agartha[b]				11	0	0	0
Dream Alt[b]				2	0	0	0

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

Table A4: Standardised carfentanil listings and change over time by market, 2019

	Period 0	Period 1	Period 2	Period 3	Period 4	Period 5	Period 6
Valhalla	0.16	Seized					
Dream	0.14	0.1	Closed				
		–26.5%					
Wall Street[a]	2.95	1.28	5.52	Seized			
		–54.6%	330.4%				
Nightmare	0	0	0	0.19	Exit scam		
		–	–	–			
Berlusconi	0.44	0	0	0.19	0.17	Seized	
		–100%	–	–	–8.0%		
Tochka	0.3	0.36	0.56	0.71	1.44	0.64	Exit scam
		–8.7%	54.8%	28.6%	101.2%	–55.5%	
Samsara[b]				0	0.03	0.02	Exit scam
					–	–47.5%	
Cryptonia[c]					0	0.03	Closed
						–	
Apollon	0	0	0	0	0.06	0	0
		–	–	–	–	–100%	–
Empire	0	0.03	0	0.16	0.45	0.41	0.24
		–	–100%	–	–174.9%	–9.5%	–41.9%
Agartha[b]				0.12	0	0	0
					–100%	–	–
Dream Alt[b]				0.02	0	0	0
					–100%	–	–

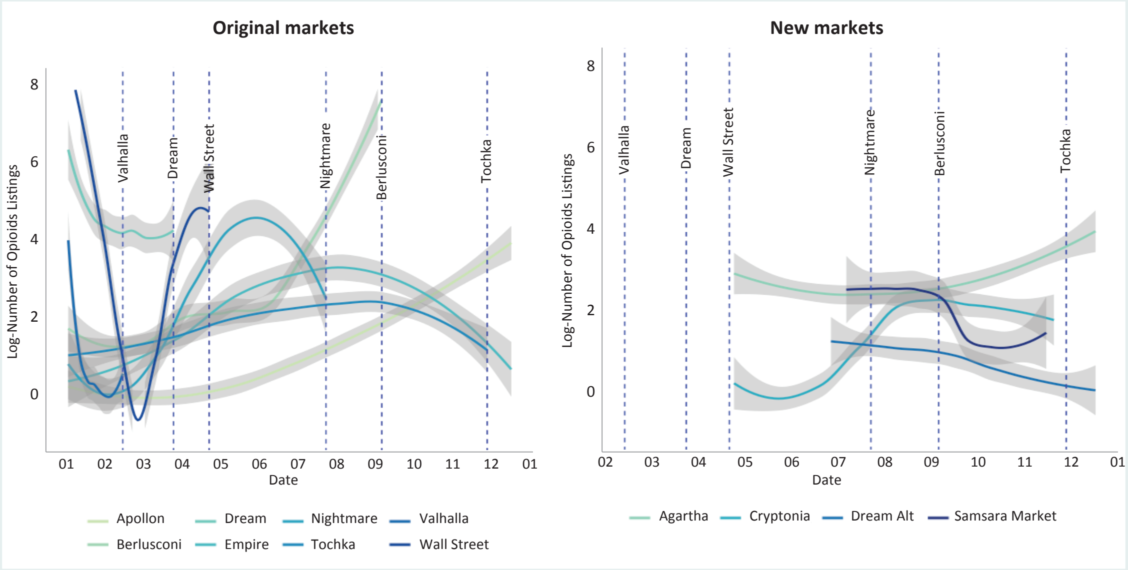
a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

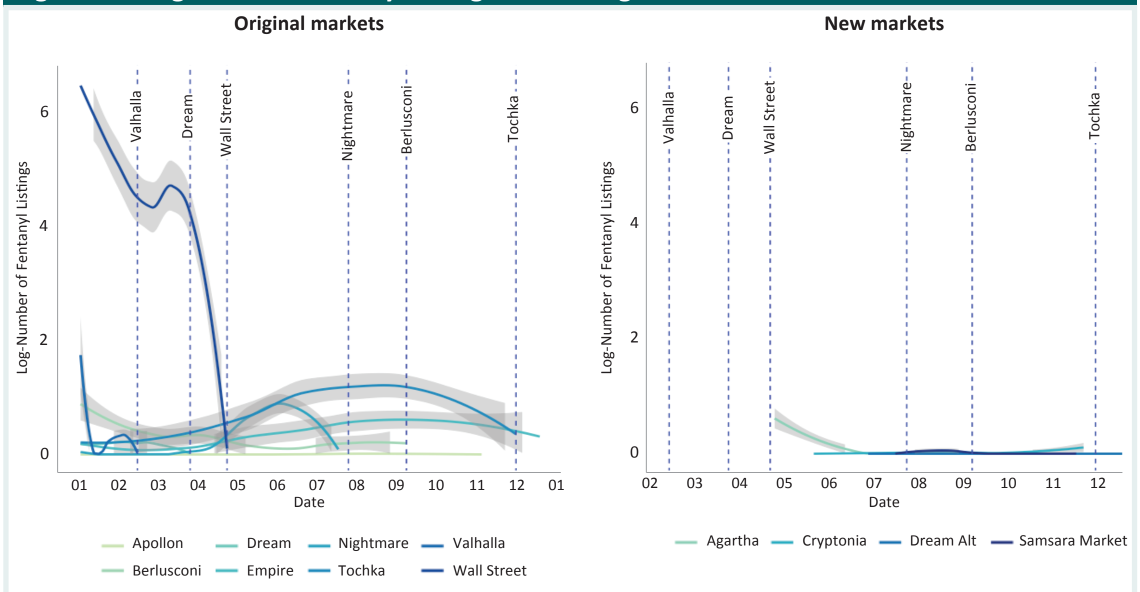
Note: Percentages rounded to one decimal place

Figure A1: Logarithm of opioid listings across original markets and new markets



Note: The vertical dotted lines represent the dates of market closures. All trends are smoothed using the 'local polynomial regression fitting' (Loess) method with a uniform span=0.75. The shading around the fitted lines represents the 95% confidence intervals and are identical to those in Figure 5

Figure A2: Logarithm of fentanyl listings across original markets and new markets



Note: The vertical dotted lines represent the dates of market closures. Trends are smoothed using the 'local polynomial regression fitting" (Loess) method with a uniform span=0.75. The shading around the fitted lines represents the 95% confidence intervals and are identical to those in Figure 8

Table A5: ARIMA models on log-listings of opioids

Overall time period	ARIMA	Coefficients
	ARIMA(1, 1, 1)	ar1=0.2510 ma1=–0.7211
	Ljung–Box chi-square=13.5780	*p*=0.0592
Period 0	ARIMA(0, 1, 1)	ma1=–0.4074
	Ljung–Box chi-square=9.1854	*p*=0.1019
Period 1	ARIMA(0, 0, 0) with mean=4.4253	–
	Ljung–Box chi-square=9.1854019	*p*=0.1
Period 2	ARIMA(1, 1, 0)	ar1=–0.4904
	Ljung–Box chi-square=5.1604	*p*=0.1604
Period 3	ARIMA(1, 0, 0) with mean=6.2809	ar1=0.7274
	Ljung–Box chi-square=6.0027	*p*=0.6469
Period 4	ARIMA(0,0,0) with mean=6.5157	–
	Ljung–Box chi-square=5.9396	*p*=0.3121
Period 5	ARIMA(1,1,2)	ar1=–0.6699 ma1=0.0453 ma2=–0.8408
	Ljung–Box chi-square=3.7785	*p*=0.8049

Note: No model is fitted on period 6 given insufficient data. Ar1 represents the coefficient of the autoregression component in the ARIMAX model after 1 differencing transformation. Ma1 or ma2 represent the coefficient of the moving average component in the ARIMAX model after 1 or 2 differencing transformations

Table A6: ARIMA models on log-listings of fentanyl

Overall time period	ARIMA	Coefficients
Overall time period	ARIMA(1,1,1)	ar1=0.1442 ma1=–0.8070
	Ljung–Box chi-square=6.9641	*p*=0.4326
Period 0	ARIMA(0,0,1) with mean=1.1881	ma1=0.4231
	Ljung–Box chi-square=7.8544	*p*=0.0971
Period 1	ARIMA(0,0,0) with mean=0.8350	–
	Ljung–Box chi-square=3.3343	*p*=0.5035
Period 2	ARIMA(0,1,0)	–
	Ljung–Box chi-square=5.2043	*p*=0.1574
Period 3	ARIMA(1,0,0) with mean=2.4665	ar1=0.2826
	Ljung–Box chi-square=8.7081	*p*=0.3675
Period 4	ARIMA(0,0,1) with mean=2.6769	ma1=0.5462
	Ljung–Box chi-square=4.0207	*p*=0.4032
Period 5	ARIMA(0,0,0) with mean=2.195	–
	Ljung–Box chi-square=14.5130	*p*=0.1052

Note: No model is fitted on period 6 given insufficient data. Ar1 represents the coefficient of the autoregression component in the ARIMAX model after 1 differencing transformation. Ma1 represents the coefficient of the moving average component in the ARIMAX model after 1 differencing transformation

Table A7: Proportion of fentanyl (including analogues) among all opioid listings, by market and period (%)

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Valhalla	21	Seized					
Dream	0	1	Closed				
Wall Street[a]	32	–	27	Seized			
Nightmare	2	0	0	2	Exit scam		
Berlusconi	20	30	8	1	0	Seized	
Tochka	9	13	24	27	27	28	Exit scam
Samsara[b]				0	1	0	Exit scam
Cryptonia[c]					0	2	Closed
Apollon	0	0	0	1	1	0	0
Empire	21	7	1	3	6	7	4
Agartha[b]				3	0	0	0
Dream Alt[b]				1	1	0	0
Total	**8**	**21**	**15**	**3**	**2**	**5**	**0**

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

Table A8: Active opioid, fentanyl and carfentanil vendors across markets by closure event (*n*)

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
All markets							
Opioids	1,764	1,084	1,550	2,663	2,283	1,551	785
Fentanyl	252	118	310	298	282	164	20
Carfentanil	45	41	37	127	138	67	5
Valhalla							
Opioids	27						
Fentanyl	5	Seized					
Carfentanil	7						
Dream							
Opioids	749	755					
Fentanyl	12	14	Closed				
Carfentanil	6	4					
Wall Street[a]							
Opioids	695	–	796				
Fentanyl	187	47	225	Seized			
Carfentanil	–	–	–				
Nightmare							

Table A8: Active opioid, fentanyl and carfentanil vendors across markets by closure event (*n*) (cont.)

	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
Opioids	14	22	330	1,083			
Fentanyl	1	1	8	72	Exit scam		
Carfentanil	0	0	0	17			
Berlusconi							
Opioids	83	89	132	577	793		
Fentanyl	21	24	27	32	22	Seized	
Carfentanil	19	22	22	17	11		
Tochka							
Opioids	161	180	193	348	434	339	
Fentanyl	24	30	48	149	194	103	Exit scam
Carfentanil	13	14	15	65	92	39	
Samsara[b]							
Opioids				25	107	111	
Fentanyl				0	4	4	Exit scam
Carfentanil				0	2	1	
Cryptonia[c]							
Opioids					164	208	
Fentanyl					1	4	Closed
Carfentanil					0	2	
Apollon							
Opioids	4	2	3	41	82	176	204
Fentanyl	0	0	0	2	4	2	0
Carfentanil	0	0	0	4	0	0	0
Empire							
Opioids	31	33	96	382	458	445	321
Fentanyl	2	2	2	25	51	47	16
Carfentanil	0	1	0	15	29	25	5
Agartha[b]							
Opioids				160	172	215	224
Fentanyl				17	4	3	3
Carfentanil				11	0	0	0
Dream Alt[b]							
Opioids				47	73	57	36
Fentanyl				1	2	1	1
Carfentanil				2	1	0	0

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1

b: Data collection from Samsara, Agartha and Dream Alt began in period 3

c: Data collection from Cryptonia began in period 4

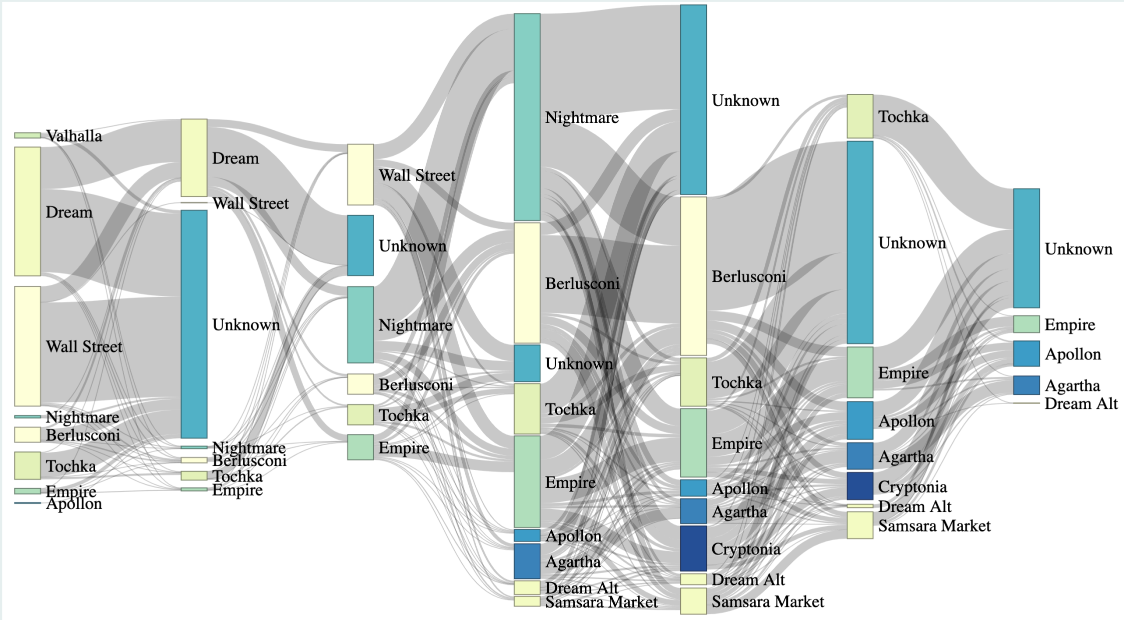
Table A9: Median price per gram of opioids and fentanyl by market and period (A$)

Opioids (Fentanyl)	Period 0 Jan–Feb	Period 1 Feb–Mar	Period 2 Mar–Apr	Period 3 Apr–Jul	Period 4 Jul–Sep	Period 5 Sep–Nov	Period 6 Nov–Dec
All markets	399	356	243	367	429	258	241
	(28)	(30)	(25)	(52)	(75)	(97)	(123)
Valhalla	168	Seized					
	(243)						
Dream	460	373	Closed				
	(67)	(73)					
Wall Street[a]	240		267	Seized			
	(28)	(30)	(25)				
Nightmare	120	54	240	392	Exit scam		
	(2)	(2)	(72)	(28)			
Berlusconi	202	171	194	372	449	Seized	
	(13)	(26)	(40)	(38)	(29)		
Tochka	738	691	562	966	1177	1167	Exit scam
	(21)	(66)	(26)	(49)	(60)	(77)	
Apollon	700	46	59	486	314	242	249
	(0)	(0)	(0)	(129)	(78)	(11)	(0)
Empire	340	33	96	382	458	445	321
	(44)	(outlier)	(outlier)	(229)	(228)	(145)	(106)
Dream Alt[b]				307	251	113	36
				(1,437)	(807)	(889)	(886)

a: Daily data collection of all opioid listings incomplete for Wall Street in period 1 and price data for this period were not reliable

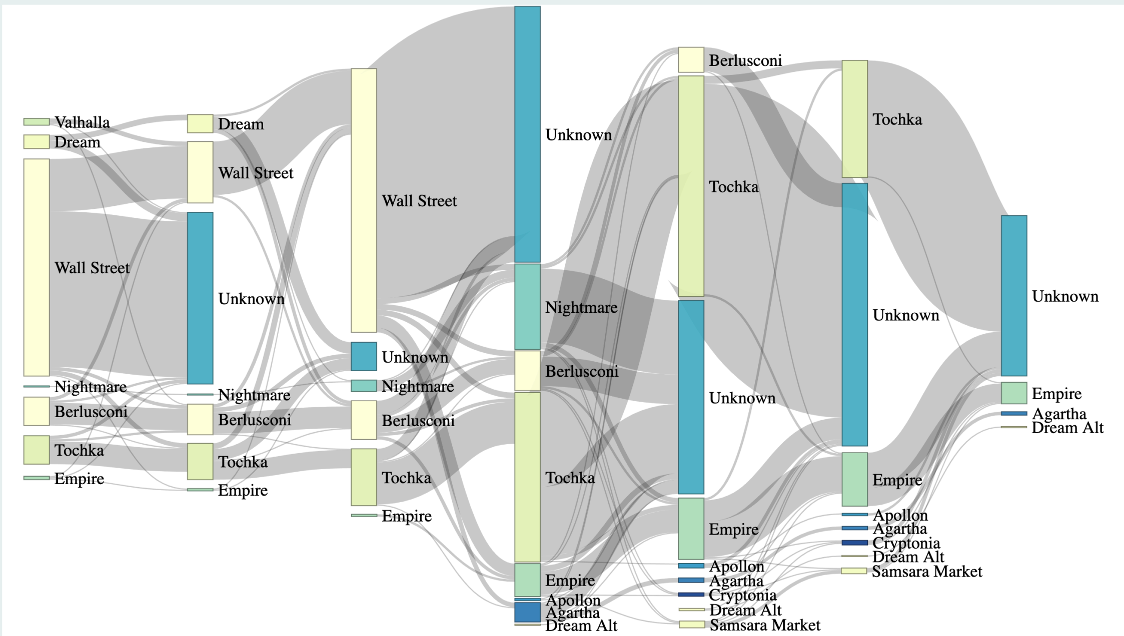
Note: Price data not available from Samsara, Cryptonia or Agartha

Figure A3: Opioid vendor movements across closure events



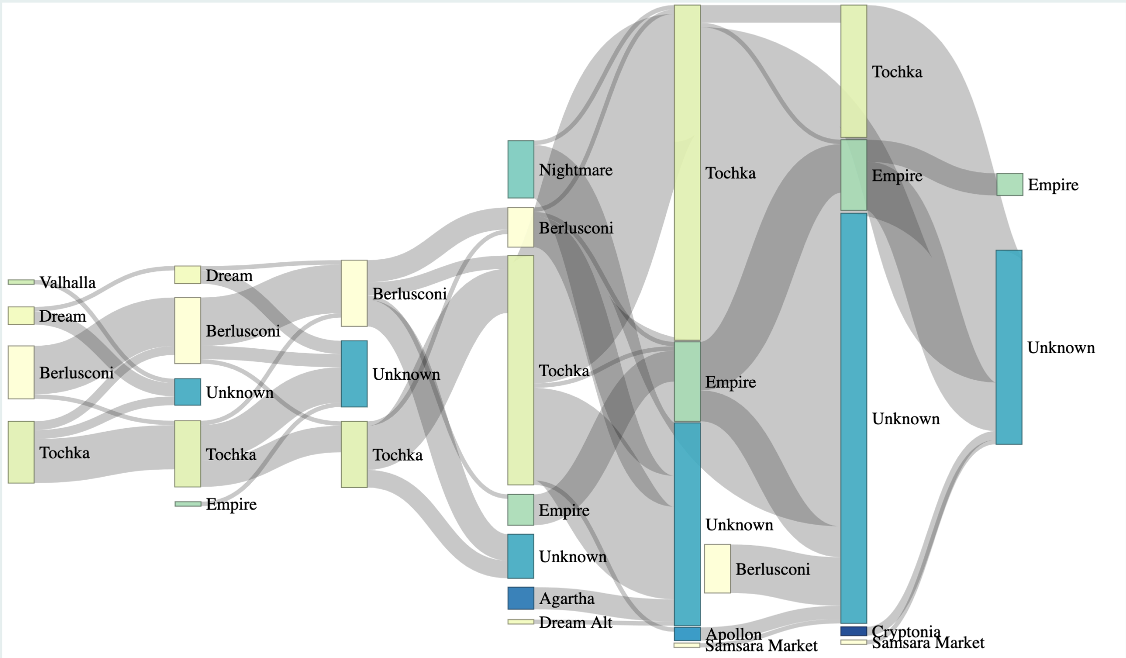
Note: The market decompositions are illustrated according to different closure events in each respective time period

Figure A4: Fentanyl vendor movements across closure events



Note: The market decompositions are illustrated according to different closure events in each respective time period

Figure A5: Carfentanil vendor movements across closure events



Note: The market decompositions are illustrated according to different closure events in each respective time period

AIC reports
Research Report

Roderic Broadhurst is a Professor of Criminology at the Australian National University.

Matthew Ball is the Laboratory Coordinator of the Australian National University's Cybercrime Observatory.

Chuxuan Jessie Jiang is a Research Assistant at the Australian National University's Cybercrime Observatory and the Research School of Finance, Actuarial Studies and Applied Statistics.

Joy Wang is a Research Assistant at the Australian National University's Cybercrime Observatory.

Harshit Trivedi is a data scientist at Fifth Domain and a Research Assistant at the Australian National University's Cybercrime Observatory.

Australia's national research and
knowledge centre on crime and justice

aic.gov.au