DOI: 10.1111/1745-9133.12642

CRIMINOLOGY & Public Policy

SPECIAL ISSUE ARTICLE

CYBERCRIME AND CYBERSECURITY

# "Like aspirin for arthritis": A qualitative study of conditional cyber-deterrence associated with police crackdowns on the dark web

**David Décary-Hétu**[1] | **Camille Faubert**[2] | **Julien Chopin**[3] | **Aili Malm**[4] | **Jerry Ratcliffe**[5] | **Benoît Dupont**[6]

[1]School of Criminology, Université de Montréal, Montréal, Quebec, Canada

[2]École nationale de police du Québec, Nicolet, Quebec, Canada

[3]School of Criminology, Université de Montréal, Montréal, Quebec, Canada

[4]School of Criminology, Criminal Justice and Emergency Management, California State University – Long Beach, Long Beach, California, USA

[5]Department of Criminal Justice, Temple University, Philadelphia, Pennsylvania, USA

[6]School of Criminology, Université de Montréal, Montréal, Quebec, Canada

**Correspondence**
David Décary-Hétu, School of Criminology, Université de Montréal, Montréal, Quebec, Canada. Email: david.decary-hetu@umontreal.ca

"Like aspirin for arthritis" in the article title is quoted from Sherman et al. (1995: 777).

**Funding information**
PMI Impact

## Abstract

**Research summary:** Crackdowns are law enforcement strategies based on the principles of deterrence theory, which stipulates that offenders are rational actors who will refrain from crime if perceived risks are higher than perceived benefits. Studies have shown that the effects of police street drug crackdowns are mostly short termed and followed by considerable displacement. In the early 2010s, an important part of illicit drug trades moved online to cryptomarkets, and law enforcement agencies have responded by engaging in online drug crackdowns. In this study, we focus on the perceptions of dark web users in order to determine, from a qualitative "data-driven" perspective, whether police online crackdowns may have a cyber-deterrent effect by analyzing 1796 forum posts. Our results show that these events trigger psychological and practical consequences that participants claim to have a conditional, although minor, deterrent effect. In the majority of cases, dark web users claimed to engage in several forms of spatial and tactical displacement.

**Policy implications:** Our study suggests that police crackdowns on the dark web have limited, short-term effectiveness in curbing illicit activities. It proposes that innovative policing approaches such as problem-

  

oriented policing and "pulling levers/focused deterrence" strategies, which involve identifying key actors and engaging with them, be potentially extended to the dark web. While this approach is promising, it emphasizes the need for further research to assess its efficacy in the online realm, as it is a largely uncharted territory for law enforcement.

**KEYWORDS**
conditional effect, cryptomarkets, deterrence theory, displacement, drugs, police crackdown

Cryptomarkets are "online marketplace platforms bringing together multiple vendors and listing mostly illegal and illicit goods and services for sale" (Aldridge & Décary-Hétu, 2016: 23). These merchant websites, similar in their design and user experience to Amazon Marketplace or eBay, make it possible to mail order a wide array of goods such as illicit drugs, firearms, counterfeit credit cards, currencies, and passports; cryptomarkets also make available hacking and fraud services (Hiramoto & Tsuchiya, 2023). Cryptomarkets first appeared in 2011 and immediately attracted the attention of law enforcement agencies due to the anonymity and security they afforded to their participants. This attention translated to the first cryptomarket seizure by the Federal Bureau of Investigation in October 2013 (Aldridge & Décary-Hétu, 2016), followed by several others[1] in the years since (Bhaskar et al., 2019; Department of Justice, 2014; Europol, 2020).

Cryptomarket seizures mirror police crackdowns and are designed around deterrence (Décary-Hétu and Giommoni, 2017). While many studies have shown that police crackdowns are rarely effective in preventing offline/street drug crimes in the long term (Cohen et al., 2003; Cooper et al., 2005; Eck, 1993; Fader, 2016; Lawton et al., 2005; Mazerolle et al., 2007; Sherman et al., 1995), few studies have investigated this question for online drug sales. The aim of this study is to understand the attitudes and beliefs of cryptomarket participants regarding the impacts of police crackdowns on cryptomarkets and other platforms that facilitate their activities. Specifically, this study focuses on a qualitative analysis of online forums that discuss police crackdowns on cryptomarkets and other platforms that facilitate their activities following two police operations (i.e., Operation East River and Operation DeepDotWeb). Findings from this study contribute to the debate on the applicability of criminological theories to the online environment, as well as on the role of law enforcement agencies' operations in countering online drug trafficking. We propose a model that predicts deterrence based on the virtuality of environments and the opportunistic nature of crimes.

## 1 | DETERRENCE THEORY: A RATIONAL CHOICE PERSPECTIVE

According to Akers (1990), deterrence theory and the rational choice perspective constitute the core of classical criminological doctrine. These approaches, which are interrelated, are both derived from an economic analysis of crime (see Pratt et al., 2017; Ward et al., 2006) and state that individuals' actions are based on rational decisions following a cost–benefit analysis. The rational

choice approach (Cornish & Clarke, 1986, 1987) provides a theoretical framework to understand how offenders make decisions and proposes that rationality and self-interest are fundamental principles of offending (Clarke & Cornish, 1985; Piquero & Tibbetts, 2002). This theoretical perspective states that offenders make decisions to gain more than what it costs to commit offenses (Cornish & Clarke, 1986, 1987).

Building on rational choice theory, deterrence theory posits that the rational calculation of the costs associated with law enforcement negatively impacts the motivation of individuals and leads to a decrease in criminal activity when deterrence is put in place (Akers, 1990). Studies have further explored this concept by developing the restrictive deterrence perspective (J. P. Gibbs, 1975; Jacobs, 1996a, 1996b, 2010; see Moeller et al., 2021 for a review). This perspective proposes that some individuals have the ability to forgo or reduce their criminal activities in order to limit the risks and the suffering they may cause (e.g., prison sentence, see J. P. Gibbs, 1975). In a conceptualization work, Jacobs (1996a, 1996b) proposes to dichotomize restrictive deterrence with (1) probabilistic restrictive deterrence and (2) particularistic restrictive deterrence. The probabilistic restrictive deterrence consists of individuals reducing the frequency of crimes which mathematically reduces the risk of suffering its consequences (Jacobs, 1996a, 1996b, 2010). Particularistic deterrence consists of reducing the visibility of the crimes committed by decreasing the severity and detection, or by displacing the criminal activity (Jacobs, 1996a, 1996b, 2010).

Several studies have tested deterrence theory in different contexts and found mixed empirical support (see the review by Pratt et al., 2017). Specifically, deterrence can be achieved through increased police activity (i.e., in specific locations or situations), punishment, and threats in the media (Kopper, 1995). Such an approach, which is labeled as a police crackdown, is an operation intended to increase the (perceived or objective) certainty and severity of detection or arrest following illegal activities (Cohen et al., 2003; Sherman, 1990). Unintended and negative consequences are also associated with deterrence when criminal activities are displaced instead of reduced.

It is generally accepted that the first use of the idea of displacement was in the pioneering work of Reppetto (1976), and the concept has been increasingly used since the 1970s, especially regarding drug markets (Caulkins, 1992). Caulkins (1992: 17) defined displacement as "the phenomenon of illicit drug markets adapting to police enforcement pressure rather than being eliminated by that pressure." Five different types of displacement of crime are discussed in the literature: (1) spatial displacement (i.e., police operations cause crime to move to nearby locations), (2) temporal displacement (i.e., crime takes place at another time), (3) tactical displacement (i.e., targeted individuals adapt their criminal behavior), (4) target displacement (i.e., targets change), and (5) functional displacement (i.e., offenders change the type(s) of crime they commit) (Eck, 1993; Green, 1995; Ratcliffe & Breen, 2011; Reppetto, 1976). It has been suggested that the less opportunistic the crime, the more likely it was to show displacement (Leong, 2014).

## 2 | POLICE DRUG CRACKDOWNS, DETERRENCE THEORY, AND CRIMINAL DISPLACEMENT

Police crackdowns have been used by law enforcement to address street drug markets since the 1980s (Sherman, 1990). They are rooted in deterrence theory; drug offenders are assumed to be rational actors who decide to limit their illicit activities if an increase in perceived detection and arrest risk associated with police crackdowns surpasses their perceived benefits of offending (Fader, 2016; J. P. Gibbs, 1975; Jacobs, 1996b). As mentioned previously, one of the effects associated with restrictive deterrence is the displacement of criminal activity (Hodgkinson et al.,

2020). The implementation of police operations causes an increase in the perception of the risks of being identified and arrested among individuals involved in criminal activities. In line with the particularistic deterrence dimension, individuals who can recognize a risky situational context for themselves will displace their activities in order to limit their exposure and visibility (Jacobs, 2010; Jacobs and Cherbonneau, 2014). Illicit drug sales are rarely opportunistic and therefore prone to displacement.

Several studies have found that in line with restrictive deterrence, drug dealers understand the risks to be arrested and use both police avoidance detection strategies and displacements to extend the lifespan of their criminal activities (Ekland-Olson et al., 1984; Jacobs, 1996a, 1996b; Johnson & Natarajan, 1995). Spatial displacement has been the most common form of displacement studied in connection with police crackdowns (Ratcliffe & Breen, 2011; Windle & Farrell, 2012). It translates to street dealers and users moving to other neighborhoods or from the street to indoor settings to better hide their drug transactions (Cooper et al., 2005; Fader, 2016; Lawton et al., 2005; Maher & Dixon, 1999). Tactical displacement involves the diffusion of warnings when police officers approach drug dealing settings, the adoption of jargon that is difficult to understand by outsiders, and restricting transactions to known customers (Jacques & Reynald, 2012; Johnson & Natarajan, 1995; Van Nostrand & Tewksbury, 1999). Temporal displacement refers to drug dealers varying their operation hours, and they will reorganize their sale time to coincide with police shift changes (Johnson & Natarajan, 1995). Finally, functional displacement occurs when drug users switch the products they use (e.g., heroin users moving to pharmaceuticals) (Reuter et al., 2021), or when drug dealers take a break from dealing (Fader, 2016). Whether deterrence or displacement occurs as a response to increased risks of detection or arrest, it reflects a process of decision making and rationality, which is crucial to understanding the development of efficient strategies to counter illicit trades (Holt et al., 2008).

More recent research has sought to include emotions, in addition to rationality, in models that define and explain deterrence (Pickett et al., 2017). Police crackdowns would increase the perceived risk of apprehension in the short term and would as a result strike fear among offenders. This fear would be the driver of their decision not to re-offend. As it is human nature to seek regression to a normal state of mind, even in the aftermath of a traumatic event, the fear that derives from deterrence would be short lived, which would explain the limited impact of most police crackdown operations. Offenders would simply learn to live with the higher risks of apprehension, and not react as much to those risks when exposed to them in the long term. The need to take into account the emotional aspects of deterrence was highlighted in other works (Pickett, 2018; Roche et al., 2020; Yim, 2021) which found fear was a strong predictor of criminal propensities in most cases. Yim (2021) raised doubts about the mediating role of fear, though he did describe many methodological issues that could explain this contradictory finding.

## 3 | DETERRENCE IN CYBERSPACE

A growing number of academics are investigating the application of deterrence theory in cyberspace toward law enforcement interventions (Denning, 2015; Ladegaard, 2018; Ledberg, 2015; Maimon, 2020; Moeller et al., 2021; Pineau et al., 2016; Wilson et al., 2015). As has been the case for applying routine activities theory to a virtual environment (see, e.g., Yar, 2005), several studies have focused on the transposition of deterrence theory to a virtual environment. A few recent studies on surveillance have found evidence for deterrence in cyberspace (Maimon et al., 2014; Wilson et al., 2015).

Specifically, results showed that the publication of a banner warning computer hackers that their activities were monitored reduced their offense duration and, at times, severity (Maimon et al., 2014). This result suggests, unsurprisingly, that online offenders are not that different from offline offenders, and therefore that deterrence theory also applies to the same extent to them (Maimon et al., 2019). The deterrence of online offenders has also been studied through the study of the impacts of online police crackdowns (Décary-Hétu & Giommoni, 2017; Ladegaard, 2019b; Soska & Christin, 2015; Van Buskirk et al., 2017; Van Buskirk et al., 2014). Cryptomarket crackdowns have triggered rapid vendor relocation to other dark web[2] platforms and generated exponential increases of active vendors on them (Ladegaard, 2019b; Van Buskirk et al., 2014). Studies have shown that after law enforcement shut down a cryptomarket, activities resumed back to their initial levels on another platform in the span of 2–3 months (Soska & Christin, 2015) or grew even beyond (Bhaskar et al., 2019), which could be indicative that the deterrent effect of these crackdowns is short lived.

Aside from cryptomarket metrics, some authors have studied the impacts of police online operations on cryptomarket drug activities through the perceptions of actors involved in this trade. In their interviews with cryptomarket drug vendors, Martin et al. (2020) noticed that in concordance with theories of offender rationality, the calculation between perceived risks and benefits was a major part of their decision-making process. This was because cryptomarkets provide a context that allows one to substantially increase profit while decreasing risks. Additionally, through qualitative analyses of online posts, studies have uncovered that police crackdowns can change the general feel of cryptomarkets from relaxed to suspicious and stressful. They however managed to convince only a few users to abandon their illicit activities; most users would look extensively for strategies to adapt (Barratt et al., 2016; Bradley & Stringhini, 2019; Horton-Eddison & Di Cristofaro, 2017; Ladegaard, 2019a; Porter, 2018).

While some posts addressed minor disruption in flows of money, products, reputation, and contacts, a greater part of the discussions was devoted to identifying the next cryptomarkets to move to and strategies that would enable users and markets to improve security (Barratt et al., 2016; Bradley & Stringhini, 2019; Horton-Eddison & Di Cristofaro, 2017; Ladegaard, 2019a, 2019b; Lorenzo-Dus & Di Cristofaro, 2018; Norbutas et al., 2020). Recognizing this, Lorenzo-Dus and Di Cristofaro (2018) concluded that technological innovation may be an outcome of law enforcement actions, rather than a desire to improve best current practices.

## 4 | THE CURRENT STUDY

While offline/street drug crackdowns are fairly well understood through the lens of deterrence theory, the deterrence effect of police online crackdowns remains insufficiently understood and requires more in-depth study (see, e.g., Maimon, 2020). For now, the range of knowledge is too limited to conclude the (ir)relevance and the (im)possibility of directly transposing the principles of deterrence theory to the online context of drug sales on cryptomarkets and to completely understand the necessary nuances. The cryptomarket drug trade and the police operations that target it are multidimensional, so there could be an array of different impacts on different actors.

This study takes a broad perspective to examine the effect of police online operations on dark web users, recognizing that the expanse of the dark web makes it challenging to capture specific deterrent effects. We therefore aim to uncover evidence of the presence of deterrence in order to understand the role that law enforcement agencies can play in the regulation of cybercrime (Maimon et al., 2019, 2014; Wilson et al., 2015). Specifically, our research focuses on two online

police crackdowns that occurred in 2019—East River and DeepDotWeb. Using a qualitative analysis approach, we frame this research around two research questions:

$RQ_1$: Do online police crackdowns contribute to deterring the drug trafficking participants of cryptomarkets?

$RQ_2$: Do online police crackdowns contribute to the displacement of the drug trafficking participants of cryptomarkets?

## 5 | METHODOLOGY

### 5.1 | Data

Our study is based on posts published on eight discussion forums hosted either on the internet or the dark web[3]. A growing number of studies in criminology are turning to forum posts to study online crime and the dark web (Aldridge & Askew, 2017; Bancroft, 2017; Moeller et al., 2017; Morselli et al., 2017; Munksgaard & Demant, 2016). As explained by Holt et al. (2008), forum data reveal offenders' perceptions of police operations and their impacts, which makes it a useful tool to achieve the objective of our study. We chose these eight specific platforms for two reasons. First, they were discussion forums on cryptomarket drug sales independent from cryptomarket platforms themselves which, as discussed later in this study, reduced the odds that the discussions were manipulated by those who had most to lose from the police crackdowns. Second, according to the platform dark.fail, a key facilitator of drug trafficking on the dark web, they were the most popular discussion forums in terms of visitors on the topic of cryptomarket drug sales at the time of data collection.

We registered on each forum with user accounts to access all threads and posts. We made sure never to post any content to avoid contamination of the data. Then, in the search engine of each forum, we entered specific keywords referring to the two police operations we focused on. To identify threads and posts referring to Operation East River, we used the keywords "wall street market," "wall street," "wall st," and "WSM." For Operation DeepDotWeb, the keywords were "DeepDotWeb" and "DDW." To extend our search, we used keywords such as "takedown," "shutdown," "bust," "seize," "darknet," "DNM shutdown," "feds" and "police." Only discussions with posts published between April 2019, when the police operations started, and March 2020, when we ended the data collection, were considered, as well as posts in English. We first identified 427 threads composed of 6507 posts (Min = one word; Max = 4319 words; Mean = 48 words; S.D. = 121 words).

An author with extensive experience in online data gathering built a custom web scraper whose task was to download the content of the 427 threads. This was achieved by querying the URL of each thread and then requesting the additional pages of discussion, whenever the posts did not fit onto a single page. Given the small number of threads, this collection process was completed in less than 1 h. Manual inspection of the threads that compared the posts in the collected data set to the posts online confirmed that the web crawler had indeed collected all the posts' content. A final data set composed of the thread title, URL, username of the poster, textual content of the post, date of the post, forum on which it was posted, and order of the post in the thread for each post was the outcome of the data collection process.

## 5.2 | Police crackdowns

To determine the effect of police crackdowns on the online drug dealing market, we have considered two operations: Operation East River and Operation DeepDotWeb. These two operations sought to deter cryptomarket participants by demonstrating law enforcement's ability to collect evidence from cryptomarkets and their facilitators.

*Operation East River*: This operation, which was conducted for almost 2 years by U.S., German, and Dutch law enforcement agencies, led to the seizure of the cryptomarket Wall Street Market and the arrest of its three administrators, who had just executed an exit scam[4] (Department of Justice, 2019a). At the time of the shut down—April 23 and 24, 2019—Wall Street Market was the second largest cryptomarket on the dark web, with approximately 63,000 products for sale, 5400 sellers, and 1,150,000 customers (Europol, 2019a). The result of this operation was the seizure of all the data from the cryptomarket servers with much incriminating information about the cryptomarket participants.

*Operation DeepDotWeb*: DeepDotWeb, a popular Dark Web news website hosted on both the internet and the dark web, was seized, and its administrators were arrested on May 6, 2019, through a partnership of 11 law enforcement organizations (Europol, 2019b). DeepDotWeb facilitated drug transactions on cryptomarkets and was an important middleman in the dark web infrastructure (Department of Justice, 2019b). On DeepDotWeb, individuals could find links to cryptomarkets, tutorials on how to use cryptomarkets anonymously, and even interviews with cryptomarket administrators. DeepDotWeb did not host a cryptomarket for drug transactions, but administrators were arrested for laundering money they received from referral links to such cryptomarkets (Department of Justice, 2019b; Europol, 2019b). In this case, the cryptomarket community lost its main communication channel to publish news, train new users on how to connect to cryptomarkets, and share information on the cryptomarket ecosystem in general.

## 5.3 | Analytical strategy

We used an inductive qualitative content analysis method because of the scarcity of research results on this topic and the exploratory nature of this study (Drisko & Maschi, 2016). This method, "grounded in the original data," allowed us to focus on the views and voices of dark web users who expressed their attitudes and beliefs (Drisko & Maschi, 2016: 103). All the posts were read and coded by two research assistants who, first, inductively and independently extracted themes from a random sample of 100 messages, obtaining an inter-rater reliability score of 93%. Disagreements were discussed and resolved between the coders and the researchers. Once the coding themes and subthemes had been determined, all posts were coded by the same two research assistants. In total 1796 posts of the 6507 (28%) from 380 different threads portrayed attitudes and beliefs regarding deterrence and the operations on DeepDotWeb and East River.

In order to analyze the different threads representing a high volume of unstructured data, we used the qualitative data analysis software tool QDA Miner which has proven to be relevant in this field (G. R. Gibbs, 2014; Peters & Wester, 2007; Talanquer, 2014). The data were imported into QDA Miner 5.0.32 to identify, group, and examine the themes addressed. Each post was read, and the sections relevant to each theme and subthemes were coded separately. A post could include references to multiple themes and subthemes. The QDA Miner software was then used to generate lists of sections of posts connected to each theme and subtheme to facilitate the analysis. In summary, QDA Miner was used to facilitate the management and coding of the different themes and subthemes in the text.

**TABLE 1** Distribution of the sample of posts according to the forum on which they were collected.

| Forum | Percentage of posts in the data set (number of posts) |
|---|---|
| Dread | 38.7 (695) |
| Reddit | 34.3 (617) |
| The Hub | 12.4 (223) |
| Avengers | 5.2 (93) |
| Torum | 4.2 (76) |
| Envoy | 3.5 (62) |
| New Zealand | 0.9 (16) |
| Hidden Answers | 0.8 (14) |
| Total | 100 (1796) |

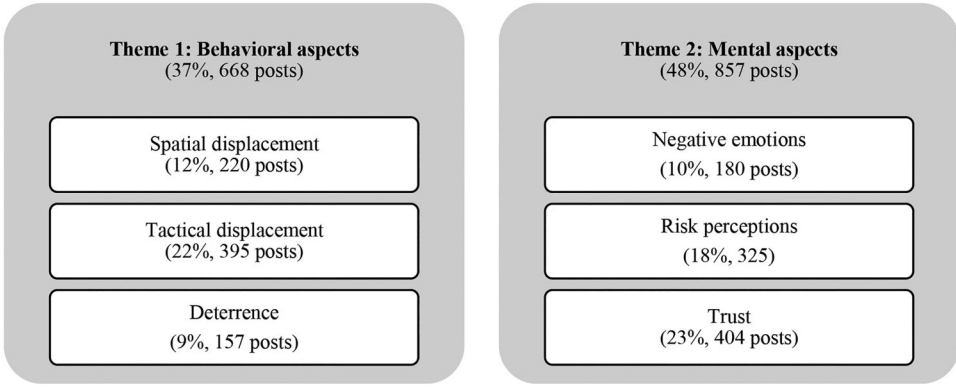


**FIGURE 1** Themes identified in forum posts.

## 6 | RESULTS

Table 1 presents the proportion of posts we gathered from each forum. Almost 75% of the posts were from Dread and Reddit. The posts were published by 1099 different usernames which equates to an average of 1.6 posts per username. A large variability underlies this average since each username was associated with between 1 and 63 posts. Overall, 46% (829) of posts were related to the operation targeting DDW, 37% (670) addressed Operation East River, and 17% (297) referred to both.

The inductive data-driven approach identified two main themes, each again subdivided into three subthemes (see Figure 1). The first, behavioral aspects, represents the attitudes and beliefs of forum participants regarding the displacement and deterrent impact of East River Operation and the operation that targeted DeepDotWeb. The second, mental aspects, relates to the intra-subject changes following the police crackdowns. It must be noted that posts could be coded in several subthemes if different aspects were addressed in the same post; 1167 posts referred to one subtheme, while 629 posts referred to two or more subthemes. We support our results with quotes from the forums and, despite our inductive approach, we supplement our qualitative results with descriptive statistics because of the large sample size.

When considering our data set, 37% (668) discussed attitudes and beliefs regarding behavioral aspects and 48% (857) of posts discussed mental aspects. A description of each theme and the related subthemes follows.

## 6.1 | Behavioral aspects

The data analysis identified several subthemes within the behavioral aspects theme. Specifically, we observed that police crackdowns appeared to deter some individuals while appearing to push others toward spatial or tactical displacement.

### 6.1.1 | Deterrence

Following police online crackdowns and the consequences they triggered, a few subjects mentioned they intended to terminate their involvement in the trade of illicit drugs on the dark web.

> I lost at AB [Alphabay], big loss at Dream, loss at Wall Street, now these fucks [Empire exit scam]. Overall, Ive worked my ass off and lost double what I made. … Either time for a career change or go back to the corner, the rents cheaper.

One subject explained being particularly deterred once he got a visit from local police at his house.

> Final Chapter ended for me last month as i was visited by LE and questioned for more than a week before i was set free again … I will not return here, i will hopefully forget what happened here and also hopefully will never need any drug in my life.

Despite these few isolated cases, subjects generally expected that those who are most likely to be deterred by police operations are market administrators, perhaps because of the sentences they could face.

> A bust that results in a *very long* sentence does have a deterrent effect. If market operators only spent a couple of years in prison, thered be hundreds/thousands of markets. Thats bad for LE.

It is presumably because of these sanctions that, following the seizures of DDW and WSM, other platforms took additional measures to restrict access: some closed voluntarily, while others refused new customers.

> I thought it interesting that dark webnews.com [an equivalent to DDW] is also just flat out missing. Probably self-imposed exile over the fact they carried market links." followed by "From what I heard, they got spooked over the DDW bust, and voluntarily pulled the plug.

> The owner/owners [of the cryptomarket CGMC] got spooked when the Feds took down DeepDotWeb and they decided the time was right to retire. They let vendors

> withdraw all funds from transactions and sailed off into history. One of the few graceful market exits.

### 6.1.2 | Spatial and technical displacements

While some deterrence appears to have taken place (9%, $n = 157$), many users shared their intention to turn to displacement. As a matter of fact, a third of posts indicated that users intended to maintain their activities on the dark web, one way or another: 12% (220) of posts favored spatial displacement, and 22% (395) favored tactical displacement. Many were convinced that the dark web would get over these crackdowns quickly and activity would be back to normal, with the voids left by the closure of DDW and WSM filled quickly.

> The Dark Web is the internet version of a hydra. When you cut off one head, two grow back in its place. The police will never beat it.

> LE are really just pissing in the ocean at this point. I eagerly await the next industrious computer-savvy person to fill in the gap left by DeepDotWeb and we can all go back to buying our precious Fentanyl, Semi-Automatic Rifles and sex slaves in peace.

Many posts were from users who immediately (and sometimes desperately) looked for alternative platforms that would allow them to continue their daily business, suggesting that police crackdowns had not convinced them to stop using such markets.

> Exactly, there is hundreds of thousands of vendors and customers displaced, they have to go some where.

This displacement to new cryptomarkets often led to a temporary slowdown of business as some subjects decided to avoid purchasing for a time and/or to buy smaller quantities.

> The safest course of action is to refrain from buying for a period of months, until the dust settles. Six months ought to do the trick.

A reasonable break seemed to be anywhere from a few weeks to 8 months. Participants were advised to use this time off to improve their online security also known as OPSEC. Some posts also suggest that those who have completely lost trust in the dark web after the police crackdowns or those who will have to put considerable effort into accessing new cryptomarkets may decide to go back to making purchases on the street rather than giving up their illicit drug activities.

> This is the daft part. Its not stopped a lot of people, its just drove them back to the street suppliers, which for some substances, is much more dangerous. Oh well, would rather people die than leave these sites alone!

Last, the loss of trust in and accessibility to "mainstream" cryptomarket infrastructure, as well as an increased perception of risk and, to a lesser extent, financial and reputational losses, seems to have stimulated the development of innovative ways to engage in the illicit drug trade online. These innovations include moving to decentralized markets that cannot be seized due to their

distributed nature and direct deals. Direct deals (or DDs see Childs et al., 2020) are a private online sale between a vendor and a buyer that does not occur through a cryptomarket infrastructure but instead uses an encrypted messaging app. While a few users advised against this approach for a variety of reasons[5], a larger proportion of users vouched for this approach.

> I think that in order to get the DM [dark web market] community to the next step, if you like, market places should become obsolete other than for maybe new vendors who need to prove themselves first.OB [Open Bazaar, a decentralized marketplace] is the most obvious improvement to the status quo, because any potential LE [law enforcement] takeover and honeypot will necessarily only involve one vendor at a time and therefore have much less scope than what they could achieve with the likes of Hansa or WSM. … So I want to put this out there to you brothers & sisters; for both buyers and sellers: Let us support the move to a much more decentralized community. Only that will allow us to survive and thrive in the long term.

## 7 | MENTAL ASPECTS

Following Operations DeepDotWeb and East River, dark web users displayed a wide array of mental reactions associated with increased pressure from police. Those included the triggering of negative emotions (10%, 180 posts), alterations in risk perception (18%, 325 posts), and changes in trust (23%, 404 posts).

### 7.1 | Negative emotions

The majority of posts mentioning negative emotions were published shortly after the events and were largely immediate reactions to announcements of the seizures. Precisely, 66% of posts revealing negative emotions in relation to operation DDW were posted within 2 days of the crackdown. For East River, 51% of posts portraying negative emotions were posted in the first 10 days following the event. Most of those who expressed negative emotions were struggling with worry, anxiety, and paranoia. Following the closing of WSM, users generally worried about the personal information police might have collected, which could lead to detection or arrests:

> i can not sleep at night since weeks, better to say i wasnt in bed at all since about 30 days now. i sleep in my chair, afraid of going on the phone por even open the door for the mailman, expecting LE [law enforcement] or worse every day. i start to have paranoia and this all without any drug at all.

Perhaps because participants had no reason to fear personal sanctions, the shutdown of DDW triggered worry mostly centered on the future of the dark web and the next strategies and targets of law enforcement,

> Wow … this is fucked. We are losing more and more internet freedom on the daily.

> Yo the Americans need to be put in check … this is getting ridiculous. The DN [dark web] is going to be hurting in the coming months. Im betting this is the beginning of a long process and they are going to round a lot of people up during all this.

Since DDW provided links to cryptomarkets, some also expressed worry about how they would access them from now on.

> This is crazy… Where is everyone? Where is our darknet home? I cant get on to any market at all since WallSt [Wall Street Market] went down. This is the only forum that is working for me at the moment Fucking S.O.S please, if yall have already recovered then help me out. What other forums are there and how do I find a trustworthy link? I also want to know the same for markets. Deep dot web is gone, im at a loss.

Other negative emotions[6] were expressed, although to a lesser extent: frustration/anger, sadness/disappointment, shock/surprise, and even disgust.

### 7.1.1 | Risk perception

Crackdowns are aimed at increasing the perceived or objective certainty of detection or arrest and have the potential to change the user's perception of risk (Cohen et al., 2003; Sherman, 1990). For some subjects, the crackdowns on DDW and WSM were a wake-up call that neither they nor the dark web were immune to law enforcement operations.

> Concerning the dark markets, we are in the midst of desperate and dangerous times.

> desperate times mean the risk factor has to go up, no more sitting round eating tea and strumpets while men shove large bulky packages in our mailboxes choc full of illegal substances.

The discussions on risk dealt with two groups of cryptomarket actors: administrators and vendors/buyers. Several users mentioned that not only the administrators of the seized platforms were at risk but also administrators of cryptomarkets not yet targeted.

> You can never avoid the heat. If you are running a dark web market, little or big its a primary target for numerous law enforcement agencies. Taking down even a small market can still result in life in prison depending on the jurisdiction and some nice media attention for LE [law enforcement].

While there was a consensus that market administrators face higher risks of detection and sanctions, subjects also suggest that it is important to remember the risk for vendors and even buyers, especially those who do not use proper operation security, who bought and sold large quantities[7], and who operated from or went to the countries in which arrests took place. The interaction between these three characteristics seemed to be the way many assessed the risks of arrest and detection.

> Guys if you ordered a couple grams of blow in plain text, NO ONE is kicking in your door. Its not even worth the man hours to come and get you, process you, put you through court, fight a public defender or lawyer, deal with appeals, pleas, trials,etc. Now if you were ordering kgs of shit and NOT using pgp [extraction], I got nothing for you. Id move.

> If you are in the country that it was seized in, be slightly concerned and tidy up the house. But if you are doing small things, i wouldnt be to concerned. I am on my 3rd or 4th seized market and still standing. edit. But i encrypted all my messages. Be smart kids.

In addition to the higher perceived risk of being identified or arrested, dark web users elaborated on the heightened risks of further crackdowns, on being monitored by authorities, and on being scammed after platforms have been shut down by law enforcement.

In contrast to some who indicated perceptions of higher risk, others, according to their posts, did not flinch when they encountered pressure from law enforcement and attempted to rationally explain this position, arguing that proving that a transaction was made by a specific person is very tedious for law enforcement, and there are no risks if no personal information was submitted online.

> (IF) they got the shipping addresses, who cares? You have to catch the person in the act WITH the product. I really think these subs are full of fifteen year old worried about mommy and daddy finding out. They can even flag your next shipment, but they still have to produce solid evidence that YOU purchased it and verify how you purchased it, etc.. If you have at least a bit of OPSEC [operational security] it would be difficult to trace the pack to you. Not saying it cant be done, but why would they spend so much time and effort on getting the end user when they are looking for the big dogs?

The quantity involved in the transaction is also an argument brought up by those who see only a low risk:

> I havent really heard of any controlled deliveries for small amounts. Its just not worth the effort, and thats in USA, where LE is harshest. Dont forget plausible deniability. If you have your OPSEC in order its gonna be hell for them to get you in serious trouble for a couple grams of whatever.

This low risk was not seen as the result of infallible technologies and operational security, but because they perceived that police lack the motivation, proactivity, and resources to track all cryptomarket users.

> so you think bc [because] they make some effort theyre going after every single person who ordered without encrypting? wow im shaking. im moving in a week out of the address i ordeted to im sure LE will track me down in another state over some weed. yeah im not worried.

### 7.1.2 | Trust

In addition, after the DDW and WSM crackdowns, many dark web users demonstrated a lack of trust in dark web platforms, administrators, security technologies, fellow dark web users, and even the dark web in general. Manifested in 23% of posts, trust issues are the most widespread mental consequence of the crackdowns.

> why trust anyone here. Anyone here could be anything, we are an anonymous community. For OPSEC, you should be thinking why you trust it. Think, should I trust someone I don't know?

On the one hand, trust was reduced because police crackdowns provided opportunities for scammers. Dark Web users often relied on DDW for reliable links to cryptomarkets; once it was shut down, they protested that scammers seized this opportunity to create phishing links to defraud them.

> LE [law enforcement] might not have crushed the DN [dark web] but scammers are going to take advantage of this situation. with the ability to stand up random shops and shit the DNM [dark web markets] is going to be a shit show.

On the other hand, dark web users also lost trust because they suspected law enforcement was now running dark web platforms and markets (i.e., honeypots).

> I honestly believe that LE [law enforcement] is in control of at least a couple other markets right now. too many strange things happening… but idk [I don't know] man maybe Im also just super paranoid haha.

While negative emotions were seen largely in the immediate aftermath of the crackdowns, trust issues seem to have lingered for up to 10 months after the crackdowns. This distrust and suspicion are detrimental to the dark web community, which may, ultimately, be the goal of the police.

> Its not even trust no one is even bad advice in this environment. Deep down though it is, It's toxic and ultimately destructive … The history of darknet markets is a narrative that at its core is optimistic, idealistic, and more then a little naive. The reality of the current culture I find myself in is 180 degree opposite. There is no sense of community, there is no accountability … we need to be able to trust each other, and the community. Not blindly though, the best way to build trust is holding each other, and ourselves accountable. … So, the idealist are gone, and we are left with the cynics. They do not speak to our inner virtues, they speak to our inherent fears and mistrust. Trust no one, everyone is shit, everone has an angle. Ironically, I feel that it is that very mindset among people that makes it a reality. A self fulfilling prophecy. I can confidently say that when i read through the forums, it is a mindset that has taken root and thrived. The current culture is diseased. So, Community, accountability, trust. How do we get there? Honor. I'm dead fucking serious.

> An article I read recently said that for LE, moving forward, one of their main strategies is to spread mistrust in the community, amongs vendors and buyers, in forums. If you look around do you see that as reality? If so, is it because they are doing a good job, or that we are doing their job for them?

## 8 | DISCUSSION

This study examined the impact that police crackdowns may have on dark web drug dealing. Framed by restrictive deterrence and rational choice perspectives, it qualitatively analyzed 1796

forum posts. The aim of this study was to identify the attitudes and beliefs of cryptomarket users regarding the impacts of the 2019 crackdowns on DeepDotWeb and Wall Street Market. This study answers two research questions that examine the ability of online police crackdowns to lead to (1) absolute deterrence and (2) displacement of the cryptomarket drug trafficking participants.

## 8.1 | Serial police crackdown, inexperience, and risk perception as factors influencing crime desisting

The analysis we have conducted led us to focus on the behavioral and mental aspects that have resulted from these crackdowns. Overall, our results are in line with the findings of past researchers who used a similar qualitative methodology to study the dark web after crackdowns (Barratt et al., 2016; Bradley & Stringhini, 2019; Porter, 2018). Dark Web users appeared shaken by police online crackdowns, and many indicated that they had experienced fear and considered desisting from their dark web activities. This is in line with past research (Pickett, 2018; Pickett et al., 2017; Roche et al., 2020) about the presence of fear, and how fear may be a driver of behavior. This behavior cannot, however, be captured simply by collecting messages, and further studies should engage with behavior, rather than attitudes and beliefs. It was clear, from our qualitative approach, that the different impacts of the police operations did not occur in silos but were intertwined. For instance, for some, the negative emotions and trust issues were mentioned before claims about a desire to desist from cryptomarkets altogether. These results advocate for residual deterrence that could extend over time, beyond the end of policing operations (Sherman, 1990).

Our results contribute to the literature focusing on deterrence by bringing up key nuances in the rationality, emotions, attitudes, and beliefs that underlie the decision-making process of those who engage and participate in the dark web drug trade. In line with the propositions of the restrictive deterrence perspective (J. P. Gibbs, 1975; Jacobs, 1996a, 1996b, 2010), the attitudes and beliefs related to deterrence were not presented as the same among all classes of dark web actors. Forum posts indicate that participants perceived that crackdowns are particularly effective at inducing fear in market administrators, in large part because of the severity of the sentences they faced if convicted, which would make them more prone to be deterred. This suggests that for those in management positions in infrastructure dealing with the sale of illicit goods online, the severity of sanctions could be as important as the certainty of being sanctioned. The interaction between severity and certainty of sanctions might be the most important deterrent for market administrators (Paternoster, 1987; Roche et al., 2020).

To a lesser extent, our results indicate that attitudes and beliefs about the deterrence of vendors and buyers may increase after an individual is visited by law enforcement following an online crackdown. However, as only one dark web user in our sample indicated having experienced such an event, further studies are needed to determine if this effect is widespread. Inexperienced dark web users as well as those with low operational security or who trade large quantities of drugs also seemed to struggle more with negative emotions and accessibility issues, therefore making them more prone to be deterred. As this study was unable to distinguish reliably among vendors, buyers, and administrators when analyzing the posts, future studies should investigate whether deterrence is experienced the same way for these three groups as it could indeed have differential outcomes.

We noticed that most of those who indicated they had desisted from dark web activities after Operations DeepDotWeb and East River had been influenced not by a single event but by the accumulation of police seizures, scams, and denial of service attacks that block users from logging on to a website. Van Buskirk et al. (2017) suggest that successive cryptomarket disruptions reduce the

recovery capacity of markets. This is also in line with Sherman's (1990) recommendations that law enforcement conducts multiple short crackdowns on different targets. This would hopefully create some residual deterrence that would continue after the crackdown is done. The reactions of dark web users are similar to those of the offline/street drug dealers interviewed by Fader (2016), who explained that they gave up dealing after a run of bad luck. Green (1995) explains that the success of police operations may not be due to deterrence but due to discouragement, where offenders change their cost–benefit analysis and determine that costs now outweigh the risks. This process seems a more accurate description of what led some dark web offenders to claim to have stopped rather than deterrence resulting from the perceived risk of arrest or detection and highlights the role of emotions in the deterrence process.

This finding suggests two recommendations for law enforcement agencies planning online operations. First, as it appears that one crackdown is not sufficient to neutralize the dark web, serial crackdowns, which also provide opportunities for scammers, might add discouragement to deterrence. However, this assumes that police agencies have the resources to sustain this process over time, which is generally not the case (Lawton et al., 2005; Sherman, 1990). Second, law enforcement agencies might be more effective if, rather than mobilizing their resources to conduct arrests, they focused on operations that discourage dark web users. Conducting operations that alter the level of trust in the community might also lead to discouragement. However, as mentioned by Munksgaard et al. (2022), the level of institutional trust of individuals is not homogeneously distributed and is dependent on several factors including age, gender, and country of origin. In this context, even if some platforms are seized and individuals are arrested, some of them will maintain a certain level of trust from users, while others will not (Munksgaard et al., 2022).

Our data did not enable us to determine whether future dark web users—those who have not yet initiated a presence on platforms and therefore depend largely on the media for information about the dark web (Ladegaard, 2018)—might have been deterred after the mainstream coverage. Media reports of these events could deter some potential users but might increase the interest of others (Bhaskar et al., 2019). It remains to be determined whether the visibility of police crackdowns on cryptomarkets through mainstream media has a general deterrent effect on those who are not yet dark web users.

## 8.2 | When benefits overcome risks: A rational choice approach to online police crackdowns

Even though police online crackdowns have mental and practical consequences, these effects are, more often than not, insufficient to make the risks outweigh the benefits. The rational choice perspective offers a suitable angle of analysis. According to this economic analysis of the offender's decision-making process, if the risks incurred are perceived as lower than the expected benefits, deterrence cannot be achieved (Cornish & Clarke, 1986, 1987). In other words, law enforcement crackdowns do not convince dark web vendors and buyers to stop their activities, let alone, as mentioned in one post, destroy their belongings, and move halfway across the world. Perhaps, crackdowns, "like aspirin for arthritis" (Sherman et al., 1995: 777), fail to act effectively and permanently on the phenomenon they are supposed to combat (Sorg et al., 2013).

This result agrees with what previous authors have found using both quantitative assessments of market activity indicators (Bhaskar et al., 2016; Décary-Hétu and Giommoni, 2017; Ladegaard, 2019b; Van Buskirk et al., 2014) and qualitative methods (Barratt et al., 2016; Bradley and Stringhini, 2019; Porter, 2018). Our results, however, bring nuances to the concept of deterrence in cyberspace related to cryptomarket drug sales by showing that, in spite of everything, there is

evidence that some attitudes and beliefs are consistent with conditional deterrence. It remains to be determined whether this conditional deterrence effect in cyberspace is a satisfactory outcome in light of the high costs and efforts invested by law enforcement in this field.

### 8.3 | Criminal displacement on the dark web: A particularistic restrictive deterrence approach

Our study shows that dark web users claimed to have used spatial and tactical displacement as a result of law enforcement actions. In the virtual environment, spatial displacement refers to the migration from one platform or market to another. After the crackdowns, most users of DeepDotWeb claimed to have moved to dark.fail, while vendors and buyers on Wall Street Market claimed to have moved to Empire; activities thus moved to "nearby" locations (Eck, 1993; Green, 1995; Ratcliffe & Breen, 2011; Reppetto, 1976). Such a result is in line with the particularistic restrictive deterrence developed by Jacobs (1996a). It suggests that in order to limit risk, individuals make their criminal activities less visible by reducing their severity, using detection-avoidance strategies, or displacing them. Drug transactions returning to the streets are also an example of spatial displacement. Maher and Dixon (1999) found that the displacement after crackdowns in street drug markets led to riskier heroin consumption habits; we saw concerns in the dark web community that the movement from cryptomarkets back to the streets might have similar adverse effects as vendors and buyers would be confronted with more violence and would more likely have to deal with impure drugs.

It is difficult to determine whether this claimed displacement increased friction and led to a smaller number of transactions, even for a short period of time. It is possible that shifting from one location to another may have taken time and effort, and thus slowed down the rate of transactions. Future research should investigate more quantitatively whether this displacement indeed entails a reduction in the number of transactions, tactical displacement of transaction sizes and drug types to reduce risks, and ever-increasing demands for OPSEC. The increased interest in decentralized markets and direct dealing can be seen as a tactical displacement. Our results highlight that, even in a fast-paced environment such as the dark web, old habits die hard as recent law enforcement operations seem to have convinced a majority of users to consider returning to a more closed and decentralized market model based on direct deals.

This alternative to cryptomarkets might contribute to increasing drug sales after a police operation because decentralized markets and direct deals provide users with a greater feeling of trust (Childs et al., 2020). The literature review of the effects of police disruption on offline/street crime revealed that both vendors and buyers engaged in displacement; the effects on the dark web community reveal a similar trend. It should be noted that several buyers believe that selling small amounts of drugs is not going to attract law enforcement. According to the particularistic restrictive deterrence perspective, this could be interpreted as a strategy to reduce the visibility of criminal activity and thus the risk of being caught (Jacobs, 1996a).

## 9 | DETERRENCE IN ONLINE ENVIRONMENTS: AN ATTEMPT OF THEORETICAL CONTRIBUTION

The results of this research present several theoretical implications. It supports the idea that crackdowns have a limited impact on deterrence and that, if they do have an impact on individuals'

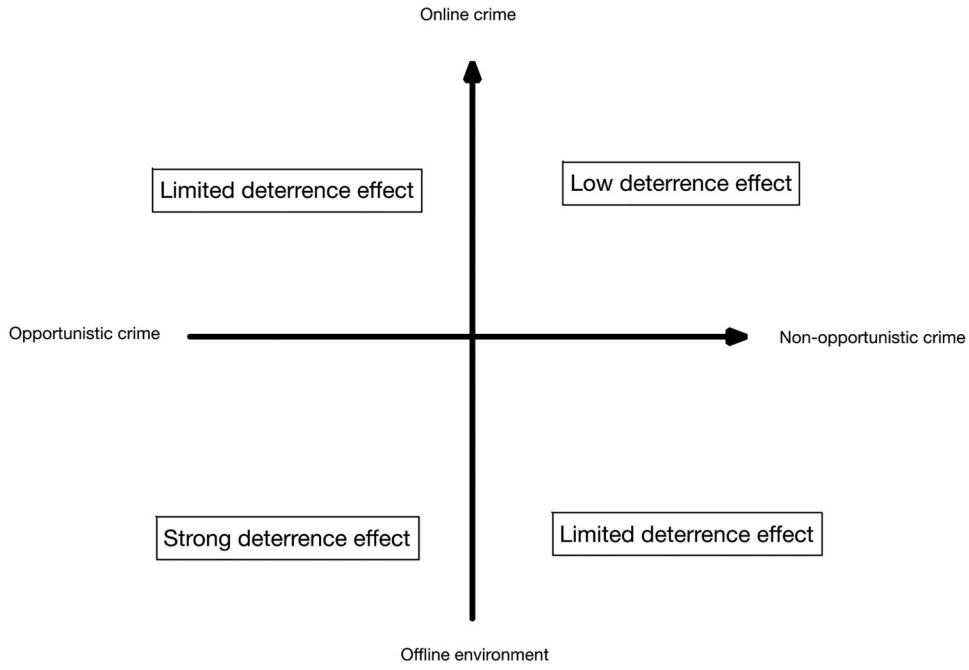


**FIGURE 2** Theoretical representation of the deterrence effects according to the level of opportunism and the criminal environment.

feelings and emotions, they are more likely to shift their activities (i.e., displacement) than to stop them according to the restrictive deterrence perspective (J. P. Gibbs, 1975). Moreover, according to the particularistic restrictive deterrence perspective (Jacobs, 1996a), our results suggest that the effects of deterrence may be balanced by the degree of expertise of individuals. Thus, the higher the criminal expertise, the more limited the deterrent effects would be.

As expressed by the rational choice perspective with the concept of bounded rationality (Cornish & Clarke, 1986), the decision-making process of individuals is particularly impacted by the available information. In this context, the concept of deterrence and desistance from criminal activity could be applied to those individuals whose criminal skills (i.e., ability to avoid police detection) are most limited. In other words, individuals with a high degree of confidence in their ability to avoid police detection and a low degree of trust in the ability of law enforcement agencies to identify and convict them may be minimally affected by deterrence operations. This theoretical assumption may be reinforced by the "online" nature of crime. As has been discussed in the past, the least opportunistic crimes are those for which deterrence is less likely to have an effect (i.e., displacement rather than desistance is more likely to occur, see Repetto, 1976).

Although the dark web drug dealing requires minimal physical involvement of individuals (e.g., substance shipping), the fact remains that online criminal activity reinforces the perception of impunity that criminals may feel, thus reducing the deterrent effects based on the ability of the justice system to identify and convict perpetrators. We have summarized this proposal in Figure 2, which represents the theoretical continuum of two dimensions of crime that might impact the deterrence effects: opportunism and environment. The proposal is the following: the more virtual the environment and the less opportunistic the crime is, the more limited the desisting effect is likely to be.

The crime pattern (i.e., online, non-opportunistic) limits the perception that individuals have of the perceived risks and consequences (e.g., jail, arrest, and fines) that might apply to them. In other words, and in the words of Becarria (1963[1764]), in order for a police crackdown to be effective and deter the targets, it would have to provide the certainty and celerity of a conviction with a sufficiently severe perceived penalty. Under these conditions, police crackdowns could have a more likely residual deterrent effect (Sherman, 1990). The online nature (e.g., difficulty in identifying individuals) combined with the absence of opportunism (e.g., better preparation for the crime) more likely leads to no or restrictive deterrence than to crime desistance. Variation in the degree of deterrence on individuals is likely mediated by individual factors as well as their skill level.

## 10 | LIMITATIONS

Our study sheds light on important aspects of online policing and contributes to the literature on deterrence in cyberspace and conditional deterrence by providing a qualitative assessment of the effect of crackdowns on dark web users. A few limitations should, however, be mentioned. As has been noted in previous studies, qualitative data from online forums are not perfect reflections of reality as dark web users may lie in their online communications (Bradley and Stringhini, 2019; Childs et al., 2020). Similarly, dark web users often express intentions rather than descriptions of actual behavior, so there may be a difference between what they say they intend to do and what they actually do. Those who said they intended to abandon their activities may not have done so, while those who suggested they intended to change their activities through displacement may either have not done so or been deterred.

In addition, all the posts we collected were published after the police crackdowns, which means we were unable to include the pre-crackdowns context in our assessment. We attempted to minimize the effects of this limitation by choosing posts that explicitly mentioned the consequences of the two specific operations under consideration. However, including pre-crackdown comments might have made it possible to locate implicit impacts.

Last, since we based our study on post-crackdown comments by dark web users, we may have underestimated the number of users who were deterred, since those who had abandoned their activities on the dark web for fear of detection or sanction may have already stopped posting on forums. We aimed to minimize the impact of this limit on our data by using posts from forums that were completely independent of transactional platforms. We could expect that cryptomarket users who were deterred from engaging in transactions by the crackdown would choose to stay away from the transactional platforms, while continuing to visit forums. We, however, could not grasp the points of view of those who were deterred completely from accessing the dark web, if any. Despite these limitations, our study sheds light on some of the consequences and drawbacks of police online crackdowns that could help orient dark web policing in the future.

## 11 | POLICY IMPLICATIONS

As for the practical implications, the results of this study suggest a number of avenues. If a large majority of dark web users are able to continue their activities after a police crackdown and these crackdowns may even help increase the lifespans of such markets, does this mean that the dark web should be allowed to exist without policing? We do not think so, and we suggest

that law enforcement should look at innovative offline/street policing in planning online operations if they hope to achieve more sustainable results. Whether it takes place online or on the streets, drug dealing can be seen as one of the most resilient types of crime that police crackdowns are facing (Sherman, 1990). Online police drug crackdowns have been similar to the traditional offline/street crackdowns that have occurred since the 1980s (Bossler and Holt, 2013) in the sense that deterrence is, at best, short termed and conditional.

However, law enforcement agencies are increasingly recognizing that offline/street crackdowns are not the most effective way to manage and prevent drug crime and have begun to use more effective innovative approaches, such as problem-oriented policing and, more specifically, pulling levers/focused-deterrence strategies (Braga & Weisburd, 2012; Corsaro et al., 2010, 2009; Mazerolle et al., 2007). The pulling levers/focused deterrence strategy is a problem-oriented policing approach (Telep & Weisburd, 2012) that identifies key actors in a specific crime problem and then uses diverse sanctions and community resources to limit or stop their activities (Braga, 2008). An important part of this strategy is communicating with these individuals to make them understand that they are being specifically targeted in a program that involves police and social services. A pulling-levers intervention set up in Nashville, TN, resulted in a 56% decrease in drug crimes in the treatment area and a 38% decrease in the adjacent area, suggesting that spatial displacement was not an adverse factor in this initiative. The authors also suggest that pulling-levers strategies seem to generate more long-term results than crackdowns (Corsaro et al., 2010).

Transposing this strategy to the dark web, police could build partnerships with private companies and social regulators to contact online offenders and replicate the pulling-levers strategy. The internet makes it difficult to identify targets but makes it much easier to contact them. Communication technologies also offer all the tools necessary to create anonymous online focus groups that would allow police to interact with users. It would be interesting to launch experiments to evaluate the effect of translating problem-oriented policing online, an avenue that could be promising (Dodge and Burruss, 2019) but has yet to be studied.

## 12 | FUTURE RESEARCH

In the future, to better understand the deterrent effect of dark web police operations, studies should take into account the level of experience and involvement of users with the dark web. In addition, our study assumes that most of the users who post on forums use the Dark Web to purchase illicit drugs, since these are the goods most widely dealt with on cryptomarkets (Bhaskar et al., 2019). Future studies should focus on police operations directed at the online trade in other harmful goods and services (hacking services, firearms sales, child pornography, counterfeit credit cards and currencies, and fake passports), which may have had different results. Finally, future studies should explore the theoretical assumptions we develop by testing them with an empirical approach.

### ACKNOWLEDGMENTS

This paper is part of the research project "Disrupting the Darknet: Law Enforcement and their Impact of Darknet Offenders" and funded by PMI IMPACT. The grant does not have a grant number.

### CONFLICT OF INTEREST

The authors confirm that they have no conflict of itnerest to declare.

## ORCID

*David Décary-Hétu* https://orcid.org/0000-0002-4360-140X

## ENDNOTES

[1] Not all cryptomarket closures are the result of law enforcement operations. Some are closed by administrators, either legitimately or through exit scamming. Others are shut down by denial-of-service attacks (Faubert et al., 2021).

[2] The dark web refers to an anonymous communication channel that makes it extremely difficult to identify the location of web servers, as well as the location of the visitors of those websites (Bian et al., 2021).

[3] These forums are Avengers, Dread, Envoy, Hidden Answers, The Hub, New Zealand, Reddit, and Torum.

[4] In an exit scam, administrators voluntarily close their own cryptomarket and steal all the virtual currency (generally Bitcoins) that users have left in escrow or in their accounts (Department of Justice, 2019a)

[5] Mostly because risks of scams for buyers are greater, but one user mentions that law enforcement track vendors on the apps.

[6] It is important to note that since the administrators of Wall Street Market had carried out an exit scam in the weeks preceding their arrests, some dark web users posted positive comments about the police crackdown, considering it payback for the exit scam. For example: "*HA FUCKING HA! Serves them right. I hope WSM admin is thrown in the lowest hole in the worst of prison*."

[7] With regard to the opioid crisis going on in the United States, some dark web users mention that those who buy or sell fentanyl or other opioids are at greater risk of being targeted by law enforcement.

## REFERENCES

Akers, R. L. (1990). Rational choice, deterrence, and social learning theory in criminology: The path not taken. *Journal of Criminal Law and Criminology*, *81*(3), 653–676. https://doi.org/10.2307/1143850

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://doi.org/10.1016/j.drugpo.2016.10.010

Aldridge, J., & Décary-Hétu, D. (2016). *Cryptomarkets and the future of illicit drug markets. The Internet and Drug Markets*. European Monitoring Centre for Drugs and Drug Addiction: Insights 21. https://www.emcdda.europa.eu/publications/insights/internet-drug-markets_en

Bancroft, A. (2017). Responsible use to responsible harm: Illicit drug use and peer harm reduction in a Darknet cryptomarket. *Health, Risk & Society*, *19*(7–8), 336–350. https://doi.org/10.1080/13698575.2017.1415304

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

Bhaskar, V., Linacre, R., & Machin, S. (2019). The economic functioning of online drug markets. *Journal of Economic Behavior & Organization*, *159*, 426–441. https://doi.org/10.1016/j.jebo.2017.07.022

Beccaria, C. (1963[1764]). *On crimes and punishments*. Bobbs-Merrill.

Bian, J., Cao, C., Wang, L., Ye, J., Zhao, Y., & Tang, C. (2021). Tor hidden services discovery and analysis: A literature survey. *Journal of Physics: Conference Series*, *1757*(1), 012162. https://doi.org/10.1088/1742-6596/1757/1/012162

Bossler, A. M., & Holt, T. J. (2013). Assessing officer perceptions and support for online community policing. *Security Journal*, *26*, 349–366. https://doi.org/10.1057/sj.2013.2

Bradley, C., & Stringhini, G. (2019). A qualitative evaluation of two different law enforcement approaches on Dark Net Markets. *IEEE European Symposium on Security and Privacy Workshops*, Delft, Netherlands.

Braga, A. A. (2008). Pulling levers/focused deterrence strategies and the prevention of gun homicide. *Journal of Criminal Justice*, *36*(4), 332–343. https://doi.org/10.1016/j.jcrimjus.2008.06.009

Braga, A. A., & Weisburd, D. (2012). The effects of focused deterrence strategies on crime: A systematic review and meta-analysis of the empirical evidence. *Journal of Research in Crime and Delinquency*, *49*(3), 323–358. https://doi.org/10.1177/0022427811419368

Caulkins, J. P. (1992). Thinking about displacement in drug markets: Why observing change of venue isn't enough. *The Journal of Drug Issues*, *22*(1), 17–30. https://doi.org/10.1177/002204269202200102

Childs, A., Coomber, R., Bull, M., & Barratt, M. J. (2020). Evolving and diversifying selling practices on drug cryptomarkets: An exploration of off-platform Direct Dealing. *Journal of Drug Issues*, *50*(2), 173–190. https://doi.org/10.1177/0022042619897425

Cohen, J., Gorr, W., & Singh, P. (2003). Estimating intervention effects in varying risk settings: Do police raids reduce illegal drug dealing at nuisance bars. *Criminology*, *41*(2), 257–292. https://doi.org/10.1111/j.1745-9125.2003.tb00988.x

Cooper, H., Moore, L., Gruskin, S., & Krieger, N. (2005). The impact of a police drug crackdown on drug injectors' ability to practice harm reduction: A qualitative study. *Social Science & Medicine*, *61*(3), 673–684. https://doi.org/10.1016/j.socscimed.2004.12.030

Cornish, D. B., & Clarke, R. V. (1986). Introduction. In D. B. Cornish & R. V. Clarke (Eds.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 1–16). Springer-Verlag.

Corsaro, N., Brunson, R. K., & McGarrell, E. F. (2010). Evaluating a policing strategy intended to disrupt an illicit street-level drug market. *Evaluation Review*, *34*, 513–548. https://doi.org/10.1177/0193841x10389136

Corsaro, N., Brunson, R. K., & McGarrell, E. F. (2009). Problem-oriented policing and open-air drug markets: Examining the Rockford pulling-levers deterrence strategy. *Crime & Delinquency*, *59*(7), 1085–1107. https://doi.org/10.1177/0011128709345955

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

Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Force Quarterly*, *77*(2), 8–15. https://faculty.nps.edu/dedennin/publications/Rethinking%20the%20Cyber%20Domain%20and%20Deterrence%20-%20jfq-77_8-15.pdf

Department of Justice. (2019a). *3 Germans who allegedly operated Dark Web marketplace with over 1 million users face U.S. narcotics and money laundering charges [Press release]*. https://www.justice.gov/usao-cdca/pr/3-germans-who-allegedly-operated-dark-web-marketplace-over-1-million-users-face-us

Department of Justice. (2019b). *Administrators of DeepDotWeb Indicted for money laundering conspiracy, relating to kickbacks for sales of fentanyl, heroin and other illegal goods on the Darknet [Press release]*. https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales

Department of Justice. (2014). *Dozens of online "dark markets" seized pursuant to the forfeiture complaint filed on Manhattan Federal Court in conjunction with the arrest of the operator of Silk Road 2.0*. https://www.justice.gov/usao-sdny/pr/dozens-online-dark-markets-seized-pursuant-forfeiture-complaint-filed-manhattan-federal

Dodge, C., & Burruss, G. W. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. In R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 339–358). Routledge.

Drisko, J. W., & Maschi, T. (2016). *Content analysis*. Oxford University Press.

Eck, J. (1993). The threat of crime displacement. *Problem Solving Quarterly*, *6*(3), 1–2. https://live-cpop.ws.asu.edu/sites/default/files/library/psq/1993/Summer_1993_Vol_6_No_3.pdf

Ekland-Olson, S., Lieb, J., & Zurcher, L. (1984). The paradoxical impact of criminal sanctions: Some microstructural findings. *Law and Society Review*, *18*(2), 159–178. https://doi.org/10.2307/3053401

Europol. (2020). *Europol's 20 most noteworthy operations*. https://www.europol.europa.eu/about-europol/europol-20-years/europols-20-most-noteworthy-operations

Europol. (2019a). *Double blow to Dark Web marketplaces [Press release]*. https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces

Europol. (2019b). *DeepDotWeb shut down: Administrators suspected of receiving millions of kickbacks from illegal dark web proceeds [Press release]*. https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspectedof-receiving-millions-of-kickbacks-illegal-dark-web-proceeds

Fader, J. J. (2016). Selling smarter, not harder: Life course effects on drug sellers' risk perceptions and management. *International Journal of Drug Policy*, *36*, 120–129. https://doi.org/10.1016/j.drugpo.2016.04.011

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J., & Dupont, B. (2021). Law enforcement and disruption of offline and online activities: A review of contemporary challenges. In M. W. Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in context* (pp. 351–370). Springer.

Gibbs, G. R. (2014). Using software in qualitative analysis. In U. Flick (Ed.), *The SAGE handbook of qualitative data analysis* (pp. 277–294). Sage.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. Elsevier.

Green, L. (1995). Cleaning up drug hot spots in Oakland, California: The displacement and diffusion effects. *Justice Quarterly*, *12*(4), 737–754. https://doi.org/10.1080/07418829500096271

Hiramoto, N., & Tsuchiya, Y. (2023). Are illicit drugs a driving force for cryptomarket leadership? *Journal of Drug Issues*, *53*(3), 451–474. https://doi.org/10.1177/00220426221133030

Hodgkinson, T., Saville, G., & Andresen, M. A. (2020). The diffusion of detriment: Tracking displacement using a city-wide mixed methods approach. *The British Journal of Criminology*, *60*(1), 198–218. https://doi.org/10.1093/bjc/azz025

Horton-Eddison, M., & Di Cristofaro, M. (2017). Hard intervention and innovation in crypto-drug markets: The ESCROW example. *Policy Brief*, *11*, 1–11. https://www.swansea.ac.uk/media/Hard-Interventions-and-Innovation-in-CryptoDrug-Markets-The-escrow-example.pdf

Jacques, S., & Reynald, D. M. (2012). The offenders' perspective on prevention: Guarding against victimization and law enforcement. *Journal of Research in Crime and Delinquency*, *49*(2), 269–294. https://doi.org/10.1177/0022427811408433

Jacobs, B. A. (1996a). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology*, *34*(3), 409–431. https://doi.org/10.1111/j.1745-9125.1996.tb01213.x

Jacobs, B. A. (1996b). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly*, *13*(3), 359–381. https://doi.org/10.1080/07418829600093011

Jacobs, B. A., & Cherbonneau, M. (2014). Auto theft and restrictive deterrence. *Justice Quarterly*, *31*(2), 344–367. https://doi.org/10.1080/07418825.2012.660977

Johnson, B. D., & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police*, *14*, 49–69.

Ladegaard, I. (2019a). 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

Ladegaard, I. (2019b). 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. (2018). 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

Lawton, B. A., Taylor, R. B., & Luongo, A. J. (2005). Police officers on drug corners in Philadelphia, drug crime, and violent crime: Intended, diffusion, and displacement impacts. *Justice Quarterly*, *22*(4), 427–451.

Ledberg, A. (2015). The interest in eight new psychoactive substances before and after scheduling. *Drug and Alcohol Dependence*, *152*, 73–78. https://doi.org/10.1016/j.drugalcdep.2015.04.020

Leong, C. (2014). A review of research on crime displacement theory. *International Journal of Business and Economics Research*, *3*(6–1), 22–30. https://doi.org/10.11648/j.ijber.s.2014030601.14

Lorenzo-Dus, N., & Di Cristofaro, M. (2018). I know this whole market is based on the trust you put in me and I don't take that lightly: Trust, community and discourse in crypto-drug markets. *Discourse & Communication*, *12*(6), 608–626. https://doi.org/10.1177/1750481318771429

Maher, L., & Dixon, D. (1999). Policing and public health: Law enforcement and harm minimization in a street-level drug market. *The British Journal of Criminology*, *39*(4), 488–512. https://doi.org/10.1093/bjc/39.4.488

Maimon, D. (2020). Deterrence in cyberspace: An interdisciplinary review of the empirical literature. In T. J. Holt & M. Bossler (Eds.), *The Palgrave handbook of international cybercrime* (pp. 449–467). Palgrave Macmillan.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33–59. https://doi.org/10.1111/1745-9125.12028

Maimon, D., Testa, A., Sobesto, B., Cukier, M., & Ren, W. (2019). Predictable deterrable? The case of system trespassers. In G. Wang, J. Feng, M. Z. A. Bhuiyan, & R. Lu. (Eds.), *Security, privacy, and anonymity in computation, communication, and storage* (pp. 317–330). Springer Nature.

Mazerolle, L., Soole, D., & Rombouts, S. (2007). Drug law enforcement: A review of the evaluation literature. *Police Quarterly*, *10*(2), 115–153. https://doi.org/10.1177/1098611106287776

Moeller, K., Munskgaard, 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. https://doi.org/10.1177/0002764217734269

Moeller, K., Svensson, B., & Munksgaard, R. (2021). Fentanyl analogs on the Swedish webforum flashback: Interest and impact of scheduling. *International Journal of Drug Policy*, *87*, 103013. https://doi.org/10.1016/j.drugpo.2020.103013

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict management in illicit drug cryptomarkets. *International Criminal Justice Review*, *27*(4), 237–254. https://doi.org/10.1177/1057567717709498

Munksgaard, R., Ferris, J. A., Winstock, A., Maier, L. J., & Barratt, M. J. (2022). Better bang for the buck? Generalizing trust in online drug markets. *The British Journal of Criminology*, *63*(4), 906–928. https://doi.org/10.1093/bjc/azac070

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*, 102635. https://doi.org/10.1016/j.drugpo.2019.102635

Paternoster, R. (1987). The deterrent effect of the perceived certainty and severity of punishment: A review of the evidence and issues. *Justice Quarterly*, *4*(2), 173–217. https://doi.org/10.1080/07418828700089271

Peters, V., & Wester, F. (2007). How qualitative data analysis software may support the qualitative analysis process. *Quality & Quantity*, *41*(5), 635–659. https://doi.org/10.1007/s11135-006-9016-8

Pickett, J. T., Roche, S. P., & Pogarsky, G. (2017). Toward a bifurcated theory of emotional deterrence. *Criminology*, *56*(1), 27–58. https://doi.org/10.1111/1745-9125.12153

Pickett, J. T. (2018). Using behavioral economics to advance deterrence research and improve crime policy: Some illustrative experiments. *Crime & Delinquency*, *64*(12), 1636–1659. https://doi.org/10.1177/0011128718763136

Pineau, T., Schopfer, A., Grossrieder, L., Broséus, J., Esseiva, P., & Rossy, Q. (2016). The study of doping market: How to produce intelligence from Internet forums. *Forensic Science International*, *268*, 103–115. https://doi.org/10.1016/j.forsciint.2016.09.017

Porter, K. (2018). Analyzing the DarkNet Markets subreddit for evolutions of tools and trends using LDA topic modeling. *Digital Investigation*, *26*, S87–S97. https://doi.org/10.1016/j.diin.2018.04.023

Pratt, T. C., Cullen, F. T., Blevins, K. R., Daigle, L. E., & Madensen, T. D. (2017). The empirical status of deterrence theory: A meta-analysis. In F. T. Cullen, J. P. Wright, & K. R. Blevins (Eds.), *Taking stock: The status of criminological theory* (pp. 367–395). Transaction Publishers.

Ratcliffe, J. H., & Breen, C. (2011). Crime diffusion and displacement: Measuring the side effects of police operations. *The Professional Geographer*, *63*(2), 230–243.

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

Reuter, P., Pardo, B., & Taylor, J. (2021). Imagining a fentanyl future: Some consequences of synthetic opioids replacing heroin. *International Journal of Drug Policy*, *94*, 103086. https://doi.org/10.1016/j.drugpo.2020.103086

Roche, S. P., Wilson, T., & Pickett, J. T. (2020). Perceived control, severity, certainty, and emotional fear: Testing an expanded model of deterrence. *Journal of Research in Crime and Delinquency*, *57*(4), 493–531. https://doi.org/10.1177/0022427819888249

Sherman, L. (1990). Police crackdowns: Initial and residual deterrence. *Crime & Justice: Review of Research*, *12*, 1–48. https://doi.org/10.1086/449163

Sherman, L., Rogan, D. P., Edwards, T., Whipple, R., Shreve, D., Witcher, D., Trimble, W., The Street Narcotics Unit, Velke, R., Blumberg, M., Beatty, A., & Bridgeforth, C. A. (1995). Deterrent effects of police raids on crack houses: A randomized, controlled experiment. *Justice Quarterly*, *12*(4), 755–781. https://doi.org/10.1080/07418829500096281

Sorg, E. T., Haberman, C. P., Ratcliffe, J. H., & Groff, E. R. (2013). Foot patrol in violent crime hot spots: The longitudinal impact of deterrence and posttreatment effects of displacement. *Criminology*, *51*(1), 65–102. https://doi.org/10.1111/j.1745-9125.2012.00290.x

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Proceedings of the 24th USENIX Security Symposium*, Washington, D.C.

Talanquer, V., Bunce, D. M., & Cole, R. S. (2014). Using qualitative analysis software to facilitate qualitative data analysis. In D. Bunce, et al. (Eds.), *Tools of chemistry education research* (pp. 83–95). ACS Publications.

Telep, C. W., & Weisburd, D. (2012). What is known about the effectiveness of police practices in reducing crime and disorder? *Police Quarterly*, *15*(4), 331–357. https://doi.org/10.1177/1098611112447611

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

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

Van Nostrand, L. M., & Tewksbury, R. (1999). The motives and mechanics of operating an illegal drug enterprise. *Deviant Behavior*, *20*(1), 57–83. https://doi.org/10.1080/016396299266597

Ward, D. A., Stafford, M. C., & Gray, L. N. (2006). Rational choice, deterrence, and theoretical integration. *Journal of Applied Social Psychology*, *36*(3), 571–585.

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency*, *52*(6), 829–855. https://doi.org/10.1177/0022427815587761

Windle, J., & Farrell, G. (2012). Popping the Balloon effect: Assessing drug law enforcement in terms of displacement, diffusion, and the containment hypothesis. *Substance Use & Misuse*, *47*(8–9), 868–876. https://doi.org/10.3109/10826084.2012.663274

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427. https://doi.org/10.1177/147737080556056

Yim, H. (2021). *Getting inside the "black box" of deterrence: Does communication of focused deterrence deter crime?* [Doctoral Dissertation. Doctorate of Philosophy in Criminology]. The University of Texas at Dallas. https://utd-ir.tdl.org/bitstream/handle/10735.1/9321/YIM-DISSERTATION-2021.pdf?sequence=1%26isAllowed=y

**How to cite this article:** Décary-Hétu, D., Faubert, C., Chopin, J., Malm, A., Ratcliffe, J., & Dupont, B. (2023). "Like aspirin for arthritis": A qualitative study of conditional cyber-deterrence associated with police crackdowns on the dark web. *Criminology & Public Policy*, *22,* 639–664. https://doi.org/10.1111/1745-9133.12642

## AUTHOR BIOGRAPHIES

**David Décary-Hétu**, Ph.D., is an associate professor at the School of Criminology of the Université de Montréal, as well as the Chair of the Darknet and Anonymity Research Centre. His research focuses on the impact of technology on crime.

**Camille Faubert** has a Ph.D. in criminology from the Université de Montréal. She is currently a researcher at the École nationale de police du Québec. Her Ph.D. thesis focused on the training of law enforcement officers.

**Julien Chopin**, Ph.D., is a researcher at the School of Criminology of the Université de Montréal. His research focuses on victims and sex offenders. He recently published with Éric Beauregard a new book *Elderly sexual abuse: theory, research, and practice*.

**Aili Malm**, Ph.D., is a professor at the School of Criminology of the Criminal Justice and Emergency Management College at the California State University—Long Beach. Her research focuses on police and the analysis of crime through social network analysis. Aili has been involved in numerous studies on law enforcement practices.

**Jerry Ratcliffe**, Ph.D., is a professor at the Department of Criminal Justice of Temple University. He has written numerous books on intelligence-led policing and has experience both as a law enforcement officer and as a researcher.

**Benoît Dupont**, Ph.D., is a professor at the School of Criminology of the Université de Montréal. Benoit has two Canadian Chairs of Research on cybersecurity and the prevention of cybercrimes. He is also the Scientific Director of the Human-Centric Cybersecurity Partnership that was founded in 2021.