Criminologie

# Les interventions policières sur les facilitateurs du crime
# Police interventions directed toward crime facilitators
# Intervenciones policiales sobre facilitadores del delito

Isabelle Fraser, Geneviève Sophie Chauvin, Camille Faubert and David Décary-Hétu

Volume 54, Number 2, Fall 2021

URI: https://id.erudit.org/iderudit/1084298ar
DOI: https://doi.org/10.7202/1084298ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (print)
1492-1367 (digital)

Explore this journal

Cite this article

Fraser, I., Chauvin, G. S., Faubert, C. & Décary-Hétu, D. (2021). Les interventions policières sur les facilitateurs du crime. *Criminologie*, *54*(2), 295–320. https://doi.org/10.7202/1084298ar

Article abstract

Cryptomarkets are e-commerce platforms that specialize in the sale of illicit drugs. The success of these markets has brought them to the attention of law enforcement agencies around the world, but coordinated efforts to shut them down and arrest their participants have so far been ineffective. This study analyses the impact of a recent police intervention that led to the closure of one of the main facilitators of cryptomarket activities, the DeepDotWeb platform. Analysis of 2,841 messages posted on discussion forums dedicated to cryptomarkets made it possible to understand how participants saw the prevention mechanisms used against DeepDotWeb and how they adapted to its closure. The results suggest that interventions that increase the effort and risk associated with browsing the darknet while also decreasing the expected benefits of crime may be more effective in disrupting illicit activities over the long term than the closure of any single market.

# Les interventions policières sur les facilitateurs du crime

Isabelle Fraser[1,2]
*Étudiante à la maîtrise*
*École de criminologie, Université de Montréal*
*isabelle.fraser.1@umontreal.ca*

Geneviève Sophie Chauvin
*Étudiante à la maîtrise*
*École de criminologie, Université de Montréal*
*genevieve.sophie.chauvin@umontreal.ca*

Camille Faubert
*Postdoctorante*
*Département de justice criminelle, Temple University, États-Unis*
*camille.faubert@umontreal.ca*

David Décary-Hétu
*Professeur agrégé*
*École de criminologie, Université de Montréal*
*Chercheur régulier*
*Centre international de criminologie comparée*
*david.decary-hetu@umontreal.ca*

**RÉSUMÉ** • *Les cryptomarchés sont des plateformes de commerce en ligne spécialisées dans la vente de drogues illicites. Le succès de ces marchés a attiré l'attention de nombreux organismes d'application de la loi à travers le monde, mais leurs efforts coordonnés pour fermer ces marchés et arrêter leurs participants se sont jusqu'à maintenant avérés inefficaces. L'objectif de cette étude est de décrire et de comprendre les impacts d'une récente intervention policière visant à supprimer l'un des principaux facilitateurs des activités des cryptomarchés, la plateforme DeepDotWeb. L'analyse de 2841 messages publiés sur des forums de discussion a permis d'étudier les perceptions des participants relatives aux mécanismes de prévention situationnelle à l'œuvre dans la fermeture de DeepDotWeb et de comprendre comment ils s'y sont adaptés. Les résultats indiquent que les interventions ayant le potentiel d'augmenter les efforts et*

---

1. Université de Montréal, 2900, boulevard Édouard-Montpetit, Montréal (Québec), Canada, H3J 1J4.

2. Cette recherche a bénéficié de la subvention PMI Impact Project.

*les risques associés à la navigation sur le* darknet*, et qui peuvent en même temps diminuer les bénéfices du crime, sont possiblement plus efficaces que n'importe quelle fermeture de marché unique pour perturber les activités illicites à long terme.*

**MOTS CLÉS** • *Interventions policières, cryptomarchés, prévention situationnelle, facilitateurs du crime.*

## Introduction

Les cryptomarchés sont des plateformes de commerce en ligne dédiées principalement à la vente de drogues illicites (Martin, 2014). Leurs ventes annuelles en forte augmentation sont aujourd'hui estimées à 700 millions de dollars américains (Chainalysis, 2020). De façon générale, les études montrent que les participants aux cryptomarchés s'adaptent aux interventions policières en développant des technologies toujours plus sophistiquées (Afilipoaie et Shortis, 2018 ; Gupta, 2018 ; Hutchings et Holt, 2014) et en se déplaçant collectivement vers de nouveaux cryptomarchés (Ladegaard, 2019 ; Soska et Christin, 2015 ; van Wegberg et Verburgh, 2018).

Ces résultats ont incité les organisations policières à élargir leur répertoire d'actions pour adopter des tactiques visant la perturbation de l'écosystème selon les principes de la prévention situationnelle. La prémisse serait de cibler les infrastructures qui facilitent les opérations des cryptomarchés sans nécessairement toucher aux cryptomarchés eux-mêmes (Hutchings et Holt, 2014 ; Martin, Cunliffe et Munksgaard, 2019). La fermeture de DeepDotWeb, un site web de nouvelles qui affichait des liens vers les plus importants cryptomarchés (Europol, 2019), est un exemple récent de cette nouvelle orientation stratégique. La présente étude vise à constater les impacts des stratégies policières de perturbation du *darknet* en étudiant les conséquences de la fermeture de DeepDotWeb.

La première section de cet article présente les cryptomarchés et les résultats des premières tentatives de contrôle par les forces de l'ordre. Les infrastructures qui facilitent les activités des cryptomarchés sont ensuite présentées, en mettant l'accent sur le rôle de DeepDotWeb. Un survol des stratégies de prévention situationnelle appliquées dans des contextes traditionnels hors ligne est réalisé, puis nous explicitons leur transition vers le domaine cyber. Après avoir présenté nos données et notre méthode, nous ferons connaître nos résultats pour discuter des impacts de la fermeture de DeepDotWeb sur les cryptomarchés.

## Les cryptomarchés et les tentatives de contrôle par les forces de l'ordre

Les cryptomarchés sont des sites web transactionnels hébergés sur le *darknet* destinés principalement à la vente de drogues illicites (Martin, 2014). Ils servent d'intermédiaires entre des vendeurs et des acheteurs, tous indépendants, qui, en échange d'une commission, bénéficient d'une forme de gouvernance et d'administration (Martin *et al.*, 2019). Ces dernières années, toutefois, les cryptomarchés ont été la cible de nombreuses opérations policières coordonnées à l'international (Leontiadis et Hutchings, 2015 ; Martin, 2014). La majeure partie des interventions policières s'est concentrée sur la fermeture des cryptomarchés et l'arrestation de leurs administrateurs (Gupta, 2018 ; Hutchings, Clayton et Anderson, 2016). De nombreux chercheurs ont mis en doute l'efficacité de cette stratégie, coûteuse en temps et en ressources (Broséus *et al.*, 2016 ; Martin, 2014 ; van Hardeveld, Webber et O'Hara., 2017). Ces opérations de longue haleine, d'une part, peinent à ralentir la croissance du nombre d'utilisateurs, du volume des transactions et des revenus générés sur les cryptomarchés (Décary-Hétu et Giommoni, 2017 ; Ladegaard, 2019 ; Martin, 2014 ; Soska et Christin, 2015 ; Van Buskirk *et al.*, 2017). D'autre part, la pression exercée par les forces de l'ordre aurait incité les participants à renforcer la sécurité de leurs activités illicites en ligne (Afilipoaie et Shortis, 2018 ; Gupta, 2018 ; Hutchings et Holt, 2014 ; Lorenzo-Dus et Di Cristofaro, 2018 ; Martin, 2014).

Les méthodes de perturbation actuelles sont alors considérées comme obsolètes par nombre de chercheurs, qui appellent à des solutions alternatives concentrées sur la prévention et l'intervention active (DiPiero, 2017 ; Hutchings et Holt, 2014 ; Lane, Salmon, Cherney, Lacey et Stanton, 2019 ; van Hardeveld *et al.*, 2017). L'une des propositions est de cibler les infrastructures qui facilitent les activités des cryptomarchés dans le but de déstabiliser leur écosystème.

### *Les infrastructures qui facilitent les activités des cryptomarchés*

L'économie globale des cryptomarchés repose en partie sur des sites web indépendants des cryptomarchés qui facilitent leurs opérations (Ladegaard, 2020). La plateforme DeepDotWeb, créée en 2013 par un groupe d'experts en relations publiques, est un exemple particulièrement éloquent de facilitateur de transactions illicites ayant lieu sur les cryp-

tomarchés. D'abord annoncé comme une « organisation de marketing pour le *darknet* » (Martin, 2014, p. 45, notre traduction), DeepDotWeb s'est rapidement positionné en tant que principale source d'informations liées aux activités des cryptomarchés. Bien qu'aucune transaction illicite ne fût directement réalisée sur son site web, DeepDotWeb tenait à jour des listes d'accès aux cryptomarchés et participait au lancement des nouveaux cryptomarchés en diffusant des entretiens avec leurs administrateurs (Martin *et al.*, 2019). Ce faisant, il offrait beaucoup de visibilité aux marchés répertoriés et simplifiait le processus de recherche et d'accès pour les utilisateurs.

Au fil du temps, DeepDotWeb s'est taillé une place de choix dans l'écosystème du *darknet* et a grandement contribué à faciliter ses activités. On y retrouvait des guides pour débutants sur la façon d'acheter des drogues en ligne par le biais des cryptomarchés, sur l'installation et la configuration de Tor, sur l'utilisation du cryptage PGP, ou encore, sur l'achat et l'utilisation sécuritaire des cryptomonnaies (Caleb, 2019). DeepDotWeb fournissait également des conseils sur la façon de maintenir une sécurité de base sur les cryptomarchés (Lane, Lacey, Stanton, Matthews et Salmon, 2018) et aidait les participants à évaluer la réputation d'un vendeur ou d'un marché, ce qui limitait les risques de fraude et d'escroquerie (Martin *et al.*, 2019). Pendant des années, DeepDotWeb a contribué de manière significative à réduire l'incertitude qui règne dans ces marchés illicites anonymes. Les ressources et les informations disponibles aidaient les participants à prendre des décisions éclairées à la suite d'un choc externe, comme la fermeture de leurs marchés préférés par les forces de l'ordre ou une escroquerie de sortie (*exit scam*), menée par les administrateurs d'un cryptomarché.

Le 6 mai 2019, les visiteurs de DeepDotWeb se sont butés à une bannière de « saisie par ordonnance du tribunal » à la place de la page d'accueil habituelle du site web (Caleb, 2019). DeepDotWeb venait d'être la cible d'une intervention policière d'envergure, au cours de laquelle les deux administrateurs de la plateforme ont été arrêtés (Europol, 2019). Selon l'acte d'accusation dans l'affaire USA v. Tal Prihar et al. (18 U.S.C. § 1956(h)), chaque achat de produits illégaux effectué sur un cryptomarché grâce aux liens d'accès que fournissait DeepDotWeb aux participants rapportait aux administrateurs une commission variant de 2 % à 4 % du montant de la transaction, totalisant une somme estimée à près de 15 millions de dollars américains.

La fermeture de DeepDotWeb témoigne d'un véritable changement stratégique de la part des autorités policières, qui jusqu'à tout récemment, concentraient leurs efforts de contrôle sur les plateformes transactionnelles, plutôt que sur les structures qui facilitent leur fonctionnement (Leontiadis et Hutchings, 2015 ; Martin *et al.*, 2019). Considérant le rôle particulier de DeepDotWeb dans l'économie globale des cryptomarchés, il importe de bien comprendre les conséquences de sa fermeture qui a le potentiel de perturber les activités de plusieurs cryptomarchés simultanément (Greenberg, 2019 ; Martin *et al.*, 2019).

### *La prévention situationnelle sur Internet*

La fermeture de DeepDotWeb par les forces de l'ordre s'apparente à de la prévention situationnelle. Cette théorie, que certains auteurs ont déjà appliquée au domaine cyber (Brewer *et al.*, 2019 ; Miró-Llinares et Moneva, 2020), propose de comprendre la prévention de la criminalité à travers la réduction des opportunités criminelles. Cette approche part du principe que les délinquants sont des acteurs rationnels et que leurs choix et leurs décisions sont influencés par les caractéristiques présentes dans leur environnement immédiat (Clarke et Cornish, 1985). Les mesures de prévention situationnelle visent à rendre les opportunités criminelles moins attrayantes, en manipulant les caractéristiques situationnelles de manière à créer un déséquilibre dans le calcul coûts-bénéfices des délinquants (Brewer *et al.*, 2019 ; Jacques et Reynald, 2012). Pour ce faire, trois stratégies de réduction de la criminalité peuvent être mises de l'avant : 1) l'augmentation des efforts nécessaires pour commettre une infraction ; 2) l'augmentation des risques d'appréhension (réels ou perçus) ; et 3) la réduction des bénéfices prévus (Clarke et Cornish, 1985 ; Cornish et Clarke, 2003).

De nombreuses études témoignent du succès de stratégies de prévention situationnelle (Clarke, 2009) comme les contrôles d'accès par la fermeture de rues (Harocopos et Hough, 2005), l'installation de caméras de surveillance en circuit fermé, et l'amélioration de l'éclairage public (Baker et Wolfer, 2003). L'efficacité des techniques de prévention situationnelle est cependant contestée au motif qu'elles ne permettraient pas de réduire le crime, mais seulement de le déplacer (Gabor, 1990). Le déplacement s'observe donc si la réduction de la criminalité induite par une mesure préventive entraîne une augmentation parallèle de la criminalité dans un autre lieu, à un autre moment, envers une autre

cible, à l'aide de différentes méthodes, par de nouveaux délinquants ou pour d'autres types de crime (Clarke, 2009 ; Guerette et Bowers, 2009). Toutefois, certaines études empiriques ont déterminé que ce déplacement ne constitue pas un inconvénient systématique des mesures de prévention situationnelle (Guerette et Bowers, 2009 ; Johnson, Guerette et Bowers, 2014). De plus, les études ayant observé un déplacement tendent à révéler un effet de déplacement partiel, c'est-à-dire que le volume de la criminalité déplacée n'est pas aussi imposant que celui découragé ou empêché (Weisburd *et al.*, 2006).

Dans le domaine cyber, les utilisateurs d'Internet ont déjà largement recours aux stratégies de prévention situationnelle. Brewer *et al.* (2019) en présentent une liste qui inclut les systèmes pare-feu et les programmes de détection d'intrusion et de détection de fraudes. Bien que la littérature évaluative de l'efficacité de celles-ci demeure au stade embryonnaire (Leontiadis et Hutchings, 2015 ; Miró-Llinares et Moneva, 2020), les études existantes tendent à montrer que les délinquants s'adaptent aux mesures de prévention (Hutchings et Holt, 2014). On ignore cependant si la suppression des infrastructures qui facilitent les opérations des cryptomarchés par les forces de l'ordre est une technique de prévention efficace pour contrer les activités illicites sur ces marchés. Dans ce contexte, la présente étude vise à décrire et comprendre les impacts de la suppression d'un facilitateur du crime – DeepDotWeb – comme stratégie de prévention pour lutter contre la vente de drogues illicites sur le *darknet*. Un regard éclairé sur les progrès des interventions policières contre la cyberdélinquance est susceptible d'avoir des implications pratiques pour les différents acteurs œuvrant dans ce domaine et d'orienter les stratégies mises en place. Plus particulièrement, cette étude permet d'identifier les mécanismes de perturbation les plus efficaces grâce à l'utilisation d'une approche qualitative novatrice et rigoureuse.

## Méthodologie

Jusqu'ici, les données en ligne générées par les participants aux cryptomarchés ont été utilisées pour fournir des aperçus quantitatifs des activités sur ces marchés et pour étudier les impacts de leur fermeture par les forces de l'ordre (Décary-Hétu et Giommoni, 2017 ; Ladegaard, 2019 ; Soska et Christin, 2015 ; Van Buskirk *et al.*, 2017 ; van Wegberg et Verburgh, 2018). En comparaison, relativement peu d'études utilisent

les données des forums pour réaliser des analyses qualitatives (Bradley et Stringhini, 2019 ; Lacson et Jones, 2016). La présente étude s'ajoute à ce dernier groupe de recherches en se servant des publications sur des forums de discussion dédiés aux cryptomarchés comme principale source de données. Jacques et Bonomo (2017) soutiennent que les délinquants sont généralement les mieux placés pour expliquer pourquoi et comment ils sont touchés par les mesures de prévention du crime. La recherche qualitative permettrait donc d'affiner la compréhension des mécanismes par lesquels une intervention donnée influence la criminalité ou comment les délinquants s'y adaptent.

D'abord créés par les administrateurs de marché pour faciliter les communications entre leurs participants, les forums de discussion sont rapidement devenus des lieux de rassemblement des utilisateurs du *darknet* (Paquet-Clouston, Autixier et Décary-Hétu, 2018). À des fins de recherche, ces forums permettent de récolter les points de vue des membres de cette communauté anonyme qui pourraient se montrer réticents à partager leurs identités pour se soumettre à de traditionnelles entrevues de recherche. Bien qu'il soit difficile de vérifier si des actions ont été entreprises après la publication des messages, l'intérêt de l'analyse de forums réside dans sa capacité à identifier les mécanismes de prévention susceptibles d'avoir le plus d'effets sur les processus de pensée et les opinions des contributeurs (Bradley et Stringhini, 2019 ; Childs, Coomber, Bull et Barratt, 2020) et à évaluer le potentiel de déplacement. Le caractère asynchrone des données publiées sur les forums offre également une plus grande flexibilité de récupération pour le chercheur et permet d'intégrer une dimension temporelle aux analyses (Im et Chee, 2006).

Bradley et Stringhini (2019) figurent parmi les premiers chercheurs à avoir utilisé les données des forums en ligne pour mesurer l'impact de deux opérations policières majeures – Hyperion et Bayonet – sur les utilisateurs des cryptomarchés. En se basant sur les messages publiés sur le forum *Reddit,* les chercheurs ont conclu que l'opération Bayonet avait généré un plus grand impact sur l'écosystème que l'opération Hyperion, principalement parce que les effets étaient plus immédiats et avaient créé plus d'incertitude dans la communauté. En nous inspirant de la démarche méthodologique de Bradley et Stringhini (2019), nous avons d'abord identifié des forums de discussion de langue anglaise où les participants des cryptomarchés sont actifs en utilisant des moteurs de recherche et des répertoires de sites web ; 14 forums ont été repérés,

dont une majorité (8) se trouve sur le *darknet*. Pour chacun des forums consultés, nous avons créé un compte d'utilisateur afin d'accéder aux fils de discussions et aux commentaires publiés par les membres. Dans les 14 forums, le mot clé « DeepDotWeb » ainsi que son abréviation « DDW » ont été recherchés de même que des mots clés ayant une portée plus large, tels que « takedown », « shutdown », « bust », « seize », « *darknet* », « DNM shutdown », « feds » et « police ».

La pertinence des publications et des commentaires a été déterminée par deux facteurs : leur contenu et leur date de publication. Les publications ont été inspectées manuellement et les messages portant sur la fermeture de DeepDotWeb ont été copiés dans un document texte. Nous avons restreint la collecte de messages aux six mois suivant la fermeture de DeepDotWeb le 6 mai 2019. Le nombre de messages pertinents était très limité au-delà de cette fenêtre, ce qui suggère une saturation dans les communications. Au total, nos analyses se basent sur 74 fils de discussion qui comprennent 2 841 messages.

L'analyse thématique a été choisie pour analyser les messages en raison de sa capacité à identifier les thèmes récurrents dans les données (Gavin, 2008). Conformément à l'approche inductive, nous nous sommes familiarisés avec les données collectées en lisant l'ensemble des messages pour développer les thèmes (Ritchie, Spencer et Connor, 2003). Le logiciel QDA Miner a été utilisé pour la codification des données. Une évaluation de l'accord interjuge a été réalisée sur un échantillon de 200 messages, sélectionnés aléatoirement et codés séparément par les deux codeurs. Sur la base de trois indices d'interfiabilité (présence, fréquence et importance relative), le coefficient alpha de Krippendorff était supérieur à 0,67, soit le seuil minimal pour témoigner d'un accord satisfaisant entre les codeurs (Krippendorff, 2004 ; Oleinik, Popova, Kirdina et Shatalova, 2014). Un examen des accords et des désaccords a été réalisé pour garantir une compréhension commune de la signification de chaque thème. Par la suite, l'ensemble des messages a été codé selon les thèmes identifiés.

## Résultats

Deux thèmes et six sous-thèmes ont émergé des données. Ceux-ci sont répertoriés dans le Tableau 1.

**TABLEAU 1**

**Thèmes et sous-thèmes identifiés**

| Thèmes | Sous-thèmes |
|---|---|
| Mécanismes de prévention situationnelle | Augmentation des efforts |
| | Augmentation des risques réels ou perçus |
| | Réduction des bénéfices |
| Réponses des participants aux mécanismes de prévention situationnelle | Rétractation temporaire ou définitive des activités du *darknet* |
| | Fermeture volontaire d'autres plateformes |
| | Adaptation |

Le premier thème fait référence aux mécanismes de prévention situationnelle sous-jacents à l'intervention policière ayant mené à la fermeture de DeepDotWeb. Ses trois sous-thèmes se rapportent aux stratégies proposées par Clarke et Cornish (1985 ; voir aussi Cornish et Clarke, 2003) : 1) l'augmentation des efforts qui passent par le contrôle d'accès et le contrôle des ressources et d'informations ; 2) l'augmentation des risques externes et internes ; et 3) la réduction des bénéfices. Le second thème se rapporte aux impacts de ces stratégies sur les participants du *darknet* et les réponses de ces derniers. Certains se sont : 1) rétractés temporairement ou définitivement du *darknet* ; 2) certaines plateformes ont fermé volontairement au vu de l'augmentation des risques générée par la fermeture de DeepDotWeb ; alors que d'autres ont 3) mis de l'avant des stratégies d'adaptation pour limiter l'impact d'interventions similaires dans le futur par la décentralisation des infrastructures, l'archivage des ressources, l'autonomisation des participants et les restrictions d'accès aux cryptomarchés. Ces différents aspects sont présentés en détail ci-dessous et appuyés par des citations[3].

### *Les mécanismes de perturbation*

La fermeture de DeepDotWeb a eu un effet de surprise sur la communauté du *darknet* puisque personne ne s'attendait à ce que les forces de l'ordre puissent s'en prendre à un site de nouvelles fournissant des liens

3. Les citations, dans leur version originale anglaise, ont été traduites en français par nous pour publication.

d'accès. Beaucoup témoignent du changement de stratégie policière que cet évènement représente.

> S****b : Je pense que c'est l'un des premiers cas où non seulement les marchés sont touchés, mais aussi les sites d'informations. Ça rend les choses un peu différentes.

Les propos des participants indiquent que la fermeture de DeepDotWeb est conforme aux trois mécanismes de perturbation des activités illicites de la prévention situationnelle.

### Augmentation des efforts

L'une des techniques de prévention situationnelle consiste à limiter les voies d'accès des délinquants potentiels vers les lieux propices à la criminalité (Clarke et Eck, 2016). Dans le contexte cyber, les voies d'accès s'apparentent davantage à des « itinéraires virtuels » entre deux cyberespaces, ou sites web (Miró-Llinares et Moneva, 2020). En procédant à la fermeture de DeepDotWeb, les forces de l'ordre ont éliminé l'une des voies d'accès principales vers les cryptomarchés. À de nombreuses occasions, les participants ont souligné l'influence qu'avait la plateforme DeepDotWeb sur le flux de trafic vers les cryptomarchés et ont même laissé entendre que les effets de la suppression de la plateforme seraient possiblement plus importants que n'importe quelle suppression de marché unique.

> B****r : Ils ont fermé deepdotweb parce que c'était LA porte d'entrée du Joe moyen pour accéder aux marchés […]. Cela a définitivement causé le chaos et rendu plus difficile pour les débutants de trouver leur chemin dans les DNM [marchés du *darknet*]. Honnêtement, c'était une plus grosse fermeture pour eux que n'importe quel marché unique.

Dans une approche de prévention situationnelle, les contrôles des moyens et de l'information sont des techniques destinées à réduire l'accessibilité aux ressources, outils et informations qui facilitent l'exécution d'un délit (Clarke et Eck, 2016 ; Cusson, 2005 ; Ekblom et Tilley, 2000). Les messages des participants indiquent que DeepDotWeb favorisait la convergence de nombreuses ressources clés sur une même plateforme et que sa fermeture a considérablement augmenté le temps et les efforts investis pour se familiariser avec les façons d'utiliser le *darknet* pour participer efficacement au trafic de drogues.

L'une des visées de DeepDotWeb était de fournir suffisamment d'informations sur les cryptomarchés actifs pour permettre aux participants de trouver une autre plateforme spécialisée où continuer leurs activités après la fermeture de leurs plateformes préférées. La disparition de DeepDotWeb semble avoir supprimé l'accès aux informations leur donnant la possibilité de prendre des décisions éclairées et d'évaluer la fiabilité des marchés alternatifs.

> m****d : Les forces de l'ordre essaient de rendre plus difficile de se regrouper… en coupant l'accès à de l'information légale qui aident les gens à trouver le prochain marché, après que leur ancien marché favori ait disparu/ait été fermé/ait fait une escroquerie de sortie.

### Augmentation des risques

La fermeture de DeepDotWeb a causé une augmentation des risques (réels ou perçus) associés à l'implication dans des activités illicites sur le *darknet*. Les risques dits externes à l'écosystème du *darknet* se rapportent aux risques de détection, d'appréhension ou d'arrestation dans le monde physique par les forces de l'ordre pour des activités commises en ligne. Les risques internes à l'écosystème constituent des risques d'être victime de fraude ou d'escroquerie en s'impliquant dans des activités illicites sur le *darknet*.

Les risques externes à l'écosystème sont principalement associés à la compromission de l'anonymat en ligne, ce qui révélerait l'identité des délinquants aux forces de l'ordre et pourrait mener à leur arrestation (Martin, 2014). La fermeture de DeepDotWeb a engendré des préoccupations en ce sens. Certains utilisateurs s'étant servis de la plateforme ont manifesté leurs inquiétudes à l'idée que les forces de l'ordre disposent d'informations sensibles et potentiellement incriminantes à la suite de la saisie du site.

> M****n : Qui sait combien d'informations ils seront capables de recueillir grâce à cette saisie ? Il est possible que s'il y avait des informations ou des communications compromettantes, ils soient en attente du bon moment. […]

En contrepartie, plusieurs participants ne semblent pas préoccupés, considérant qu'aucune information identitaire n'était requise pour naviguer sur la plateforme et qu'il n'était pas nécessaire de créer un compte pour pouvoir utiliser les services offerts par DeepDotWeb.

> A****0 : […]quelles infos les personnes ont-elles mises sur DDW qui pourraient mener les [forces de l'ordre] vers elles ? Je n'ai même jamais créé un compte sur DDW. Je ne connais personne qui l'a fait. Et généralement, tu ne donnes aucune information personnelle juste en faisant un compte sur un site du deep web. Donc, je ne vois pas comment les [forces de l'ordre] qui ferment DDW pourraient affecter le moindrement les utilisateurs.

En plus de ces perceptions des risques externes, les messages des participants nous ont permis d'observer que ces derniers semblent plus sensibles à l'augmentation des risques internes de fraude et d'escroquerie. La fermeture de DeepDotWeb a engendré une augmentation considérable de ces risques en privant les participants d'une grande quantité d'informations et de ressources fiables. Par exemple, DeepDotWeb distinguait les liens frauduleux des liens valides pour accéder aux cryptomarchés, ce qui permettait d'interrompre de nombreuses tentatives d'hameçonnage. Les solutions disponibles depuis la fermeture de la plateforme sont moins efficaces dans ce domaine, et les escrocs le savent et en profitent. Il semblerait même que le fait que les coûts de l'utilisation du *darknet* surpassent dorénavant les bénéfices soit associé plus fortement aux risques internes qu'aux risques externes.

> [deleted] : Après la chute de Deepdotweb.com, plusieurs sites web contrefaits tels que Deepdotweb.com ont émergé sur Google pour diriger les personnes vers un marché frauduleux.
>
> 8****8 : Comme tous les anciens le savent, au fil du temps, plusieurs marchés sont venus et sont partis – ont été renversés par les [forces de l'ordre], ou les administrateurs ont fait une escroquerie de sortie. Cela n'a jamais été ce qu'on appellerait une navigation tranquille. Récemment seulement, avec toutes les attaques DDoS [Distributed Denial-of-Service], les fraudes, l'argent des gens qui disparaît des portefeuilles du marché et autres, j'ai eu l'impression que le risque a atteint un point où il l'emporte sur les bénéfices.

### Réduction des bénéfices

De façon plus indirecte, la fermeture de DeepDotWeb a eu l'effet de réduire les bénéfices des vendeurs et des administrateurs de marchés, en limitant le bassin d'acheteurs intéressés à transiger sur les cryptomarchés. En effet, des vendeurs ont noté que l'augmentation des risques internes amène une perte de confiance des acheteurs dans les cryptomarchés. Moins d'acheteurs implique moins de revenus pour les vendeurs et les administrateurs des cryptomarchés.

F****t : Ils perdent une confiance massive maintenant, trop de personnes se faisant hameçonner fera en sorte que tous les clients éviteront [le cryptomarché] Empire.

### *Réponses des participants aux mécanismes de perturbation*

Trois réactions possibles des participants à la fermeture de DeepDotWeb ont été identifiées : la rétractation temporaire ou définitive des cryptomarchés ; la fermeture volontaire des sites similaires et de cryptomarchés ; et l'adaptation des participants.

#### Rétractation temporaire ou définitive

La fermeture de DeepDotWeb a déstabilisé l'écosystème des cryptomarchés de sorte que les risques internes ont pris une place considérable. Pour éviter d'être victimes de fraude ou d'escroquerie, certains proposent de cesser les activités sur le *darknet* pendant quelques mois.

g****g : Le paradis des fraudeurs comme vous l'avez dit, tout le monde devrait se tenir tranquille pendant quelques mois, je crois. Et ne pas suivre les liens des *feds* ou les liens d'hameçonnage qui seront mis ici. […]

Certains vendeurs et acheteurs sont plus draconiens et témoignent de leur intention de se rétracter du commerce en ligne pour poursuivre leurs activités dans la « rue ». Cette décision demeure tout de même mal accueillie puisque, en s'appuyant sur les principes de la réduction des méfaits, ces vendeurs et acheteurs suggèrent que les cryptomarchés sont des environnements plus « sûrs » pour effectuer des transactions de drogues et se procurer des produits de meilleure qualité.

s****8 : Ce qui est ennuyeux, c'est qu'au moins nous avions une certaine sécurité, une certaine responsabilité… maintenant nous allons revenir à l'achat des drogues de rue coupées avec du fentanyl… bien joué FBI. Vous êtes *fucking* intelligents…! (…) Mettre la vie des gens en danger, encore… Dites-moi pourquoi!!

#### Fermeture volontaire des sites similaires et de cryptomarchés

Le modèle d'affaire de DeepDotWeb était basé sur des ententes avec les administrateurs de nombreux cryptomarchés qui leur versaient 2 % à 4 % de chaque vente effectuée grâce à un lien d'accès. Face à l'augmentation des risques externes, certains administrateurs impliqués dans cette

entente avec DeepDotWeb ont choisi de mettre un terme à leurs activités.

> g****n : [Le cryptomarché] CGMC a fermé, ils n'ont arnaqué personne. Ils ont simplement décidé qu'ils couraient un trop grand risque en gérant le plus ancien et le plus gros marché du *darknet* après la saisie de deepdotweb.

Également, les administrateurs de sites similaires à DeepDotWeb, qui diffusait gratuitement des liens vers les cryptomarchés, auraient été découragés de poursuivre leurs activités en raison de l'arrestation des administrateurs de DeepDotWeb.

> F****r : J'ai trouvé intéressant que darkwebnews.com soit également disparu. Probablement un exil auto-imposé dû au fait qu'ils présentaient des liens de marchés.

### Adaptation des participants

Si l'augmentation des efforts et des risques semble avoir convaincu certains participants et administrateurs de mettre fin à leurs activités illicites sur le *darknet*, du moins temporairement, d'autres participants ont manifesté leur volonté de s'adapter pour contourner les stratégies de prévention situationnelle. Nous avons identifié quatre formes d'adaptation aux différents mécanismes de perturbation : la décentralisation des infrastructures ; l'archivage ; l'autonomisation des participants ; et les restrictions d'accès aux cryptomarchés. Ces formes d'adaptation imposent toutefois des contraintes importantes aux participants, que nous explicitons plus en détail.

La recommandation la plus souvent mentionnée par les participants pour s'adapter à des évènements comme la saisie de DeepDotWeb consiste à décentraliser les infrastructures, qu'il s'agisse des plateformes transactionnelles, de moyens de communication ou de sites informationnels, de manière à disposer de solutions de rechange fiables en cas de saisie policière. Dès lors, plusieurs plateformes ont vu le jour après la fermeture de DeepDotWeb et se sont présentées aux utilisateurs comme des remplaçants potentiels. L'idée est que les utilisateurs devraient consulter plusieurs sources d'informations et de liens vers les cryptomarchés pour éviter de mettre tous leurs œufs dans le même panier.

> s****3 : Mon point était que je ne voudrais pas une répétition de ce qui est arrivé avec DDW. Si nous avions 1 ou 2 ressources supplémentaires pour

> les liens de DNM comme dark fail en guise de sécurité, cela assurerait que le DNM continue de fonctionner correctement si l'un d'entre eux ferme.

Cela dit, la décentralisation des infrastructures permet à tous ceux qui en ont la volonté de proposer des liens vers les cryptomarchés, ce qui ouvre la voie aux plus mal intentionnés. En raison de l'augmentation des risques internes causée par la déstabilisation de l'écosystème du *darknet*, les participants ont plus de difficultés à faire confiance aux sites nouvellement opérationnels qui ne citent pas clairement leurs origines. Ultimement, dans les six mois suivants la saisie de DeepDotWeb, les participants estiment qu'il n'existe pas de site comparable en termes de qualité et de fiabilité, ce qui complique la décentralisation des sources.

> m****e : C'est le chaos parce qu'on ne peut croire personne qui fournit des liens en ce moment, et il n'y a plus d'agrégateur principal comme deepdotweb. Tout le monde dit dark fail mais qui sont-ils ? Ils fonctionnent par donations. Ils pourraient facilement insérer au hasard des sites frauduleux dans leur liste de liens.

Après la fermeture de DeepDotWeb, plusieurs participants se sont reproché de ne pas avoir sauvegardé le contenu du site web pour pouvoir le consulter ultérieurement. Pour éviter que cela ne se reproduise, les participants ont proposé d'archiver le contenu de plateformes toujours actives ou de forums de discussion.

> W****5 : Je lisais les archives de nouvelles de DDW, et j'ai réalisé, Hey, cela pourrait arriver à n'importe quoi et à tout moment, donc, logiquement, pourquoi ne pas archiver cette merde ? Ce message sera mis à jour de temps en temps avec une archive plus récente de Dark.Fail à des fins de préservation, dans l'éventualité où il serait soudainement saisi, fermé ou perdu.

Devant la montée des risques internes à la suite de la disparition de DeepDotWeb, plusieurs recommandent fortement aux participants d'apprendre à s'assurer eux-mêmes de la fiabilité des liens vers les cryptomarchés à l'aide de technologies innovatrices, plutôt que de se fier au répertoire de liens fournis par une seule et même plateforme nouvelle en laquelle ils n'ont pas confiance. Cette méthode permettrait d'interrompre de nombreuses tentatives de fraude et, par le fait même, de contourner les perturbations causées par la fermeture de DeepDotWeb.

> r****6 : Tu ne sais pas, regarde ce qui est arrivé à deepdotweb… c'est pourquoi tu apprends comment fonctionne le PGP, comment activer 2FA et comment vérifier les liens toi-même. Tu vas finir par te faire arnaquer éventuellement, mais c'est juste le prix à payer pour faire des affaires.

Néanmoins, ces innovations technologiques requièrent une certaine expertise de la part des utilisateurs. Dans un contexte où les ressources pour débutant que fournissait DeepDotWeb ne sont plus accessibles, il peut s'avérer compliqué pour ceux n'ayant pas ces connaissances de devenir autonomes pour vérifier les liens des cryptomarchés, éviter les escroqueries et poursuivre leurs activités illicites sur le *darknet*. En effet, plusieurs ont simplement du mal à configurer et à utiliser les technologies « de base » pour éviter d'être identifiées ou victimes de fraudes.

> 8****8 : regarde combien de gens ont du mal à simplement utiliser le PGP & 2FA de base pour éviter d'être arnaqué. Quelles sont les chances qu'ils apprennent à exporter leur clé privée de BTC [bitcoin], à la garder en sécurité et autres.

Outre les capacités limitées des utilisateurs, la volonté de faire des profits ou d'obtenir des produits de consommation rapidement peut mener à une certaine forme de négligence et à la prise de risques inutiles. En effet, la connaissance des mesures de protection efficaces ne garantit pas que les participants feront tout en leur pouvoir pour les mettre en œuvre.

> C****r : […] S'il y a une chose que j'ai apprise au cours des dernières années dans le DN, c'est que les gens ne veulent pas : *Lire, *Apprendre ou *Penser. Les gens sont justes obsédés par obtenir leur drogue de choix, et ils la veulent MAINTENANT ! Ils ne peuvent littéralement pas penser à autre chose -- même leur propre sécurité est secondaire, voyez le nombre de personnes qui n'utilisent toujours pas le cryptage, même pour leurs adresses de livraison.

Le caractère public des cryptomarchés rendait leurs utilisateurs plus vulnérables aux fraudes et escroqueries lorsque l'écosystème du *darknet* a été perturbé par la fermeture de DeepDotWeb. Pour réduire les risques internes de leurs utilisateurs, les administrateurs de certains marchés ont choisi de restreindre ou de privatiser l'accès à leur plateforme de sorte que seulement les utilisateurs invités ou répondant à certains critères pouvaient y accéder. L'accès à ces plateformes est généralement réservé à ceux qui ont assez bonne réputation ou qui ont du crédit auprès de la communauté, ce qui exige plus de temps et d'efforts de leur part.

> s****k : Si tu fais partie de n'importe quelle communauté du dn et possède certaines compétences ou valeur, les gens vont t'inviter à des marchés sur invitation seulement. Aussi, c'est grâce à ces communautés et tes associés

> (personne n'est ton ami dans le dn) que tu vas obtenir des liens légitimes pour les sites dont tu as besoin. Il est temps de travailler cette crédibilité pour que tu puisses t'asseoir à la table cool au lieu d'obtenir ton 411 du Clearnet :)

Par exemple, le marché Versus exige que les vendeurs aient au moins 700 transactions vérifiées sur d'autres marchés et un taux de rétroactions positives de 98 %. De nombreux participants ont souligné l'aspect restrictif de ces conditions, qui favorisent nettement les vendeurs déjà actifs, au détriment de tous les nouveaux qui désirent s'y joindre.

## Discussion

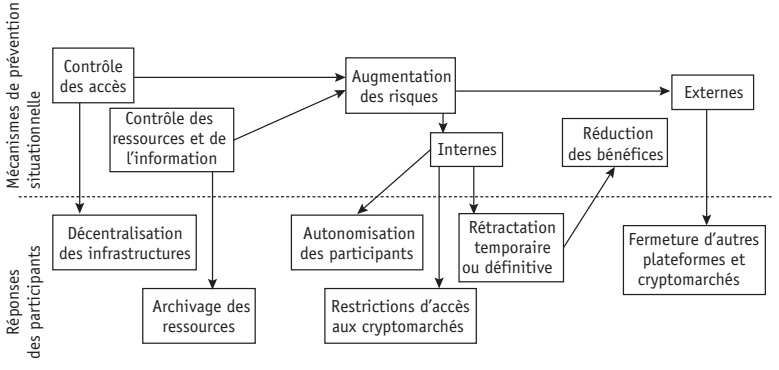
La prévention situationnelle est basée sur la réduction de l'attrait des opportunités criminelles, en manipulant les caractéristiques situationnelles de manière à créer un déséquilibre dans le calcul coûts-bénéfices des délinquants et ainsi réduire la criminalité (Brewer *et al.*, 2019 ; Jacques et Reynald, 2012). La fermeture de DeepDotWeb, un facilitateur des activités des cryptomarchés, cadre avec cette approche. L'objectif de la présente étude était donc de décrire et comprendre les impacts de cet évènement sur les utilisateurs du *darknet*. Nos résultats montrent, dans un premier temps, que la fermeture de DeepDotWeb a mené à une augmentation des efforts nécessaires pour pratiquer des activités illicites sur le *darknet* en limitant les accès vers les cryptomarchés et en restreignant la disponibilité des ressources et de l'information pour y naviguer. Cet évènement a également engendré une augmentation des risques externes, mais principalement internes à l'écosystème, et, indirectement, une réduction des bénéfices potentiels pour les vendeurs et les administrateurs des marchés. Comme certains utilisateurs découragés choisissent d'abandonner temporairement ou définitivement leurs activités sur le *darknet*, nos résultats s'alignent sur ceux des recherches théoriques et empiriques sur l'efficacité de la prévention situationnelle (Clarke et Eck, 2016), disant que le déplacement est généralement incomplet ; le volume de la criminalité déplacée ne semble pas égal à celui découragé ou empêché (Guerette et Bowers, 2009 ; Weisburd *et al.*, 2006).

Dans un deuxième temps, nos résultats mettent en lumière différentes réponses des utilisateurs du *darknet* à cette perturbation. Alors que certains ont cessé temporairement ou définitivement leurs activités sur le *darknet* et que des administrateurs ont fermé leurs plateformes, une

importante proportion d'utilisateurs a témoigné de mesures d'adaptation visant à se protéger et protéger l'écosystème de futures interventions policières, ce qui suggère une forme de déplacement (Gabor, 1990). Par exemple, pour rendre le *darknet* moins vulnérable aux stratégies de prévention situationnelle, les utilisateurs proposent de décentraliser les infrastructures, archiver les contenus pertinents et devenir plus autonomes dans l'utilisation des ressources technologiques. Les administrateurs, quant à eux, peuvent devenir plus sélectifs en restreignant l'accès à leurs plateformes ou en les privatisant.

**FIGURE 1**

**Modèle de l'impact d'une intervention policière visant un facilitateur du crime sur le *darknet***




Bien que ces stratégies et réactions aient été abordées jusqu'ici séparément, elles ne surviennent pas en vase clos. La Figure 1 présente donc une intégration des thèmes et sous-thèmes ayant émergé des données exploitées dans cette étude.

Le contrôle d'accès aux cryptomarchés qu'a provoqué la fermeture de DeepDotWeb est une stratégie d'augmentation des efforts qui a aussi causé une augmentation des risques, puisque les participants visitent d'autres plateformes pour obtenir des liens vers les cryptomarchés et risquent donc d'employer des liens frauduleux. Le contrôle d'accès aux cryptomarchés stimule également le mécanisme d'adaptation de décentralisation des infrastructures puisque, si les utilisateurs avaient recours à plusieurs sources fiables, ils seraient moins ébranlés par la disparition de l'une d'elles. Le contrôle des ressources et de l'information mène à une augmentation des risques, car les participants peu expérimentés et

mal informés sont vulnérables aux fraudes et escroqueries sur le *darknet*. L'archivage des ressources permettrait aux participants de s'adapter, considérant que l'information demeurerait disponible même si les plateformes disparaissaient.

L'augmentation des risques semble occuper une place importante dans le schéma de prévention situationnelle appliqué au *darknet*, car cet aspect est directement ou indirectement lié à presque tous les autres. L'augmentation des risques internes est associée à deux stratégies d'adaptation : l'autonomisation des participants et les restrictions d'accès aux cryptomarchés. Or, l'augmentation des risques internes peut aussi mener au découragement de certains qui vont choisir de se rétracter temporairement ou définitivement des activités illicites sur le *darknet*, ce qui engendrera une réduction des bénéfices des vendeurs et des administrateurs de cryptomarchés. Finalement, l'augmentation des risques externes peut mener à la fermeture d'autres plateformes et cryptomarchés dont les administrateurs craignent d'être identifiés et arrêtés.

Les propos des participants ont permis de constater que le processus principal par lequel la fermeture de DeepDotWeb, comme stratégie de prévention situationnelle, a perturbé le *darknet* est une augmentation des efforts par le contrôle des accès et des ressources, ce qui a causé une augmentation des risques internes. Pour y remédier, les participants ont suggéré de diversifier les infrastructures, archiver les ressources, rendre les participants plus autonomes et restreindre les accès aux cryptomarchés. Dans une moindre mesure, la fermeture de DeepDotWeb a amené une augmentation des risques externes et une réduction des bénéfices. De façon générale, les participants n'étaient pas inquiets de se faire arrêter ou de perdre leurs bénéfices associés aux activités illicites qu'ils menaient sur le *darknet*, mais plutôt de se faire frauder, ce qui les a amenés à développer plusieurs stratégies d'adaptation.

Les études quantitatives traitant des effets de la fermeture de cryptomarchés avaient déjà soulevé la préoccupation que ces interventions pouvaient mener les participants à prendre des mesures supplémentaires pour contourner les stratégies policières et fortifier l'écosystème (Afilipoaie et Shortis, 2018 ; Gupta, 2018 ; Hutchings et Holt, 2014 ; Lorenzo-Dus et Di Cristofaro, 2018 ; Martin, 2014). Nous avons observé que les stratégies de prévention situationnelle peuvent avoir ces conséquences également. À long terme, ces différentes formes d'adaptation sont susceptibles de compliquer le travail des forces de l'ordre. Il

appert cependant qu'à court terme, la faible confiance qu'ont les utilisateurs du *darknet* à l'égard des nouvelles plateformes et les capacités technologiques limitées que possède la majorité des utilisateurs pourraient ralentir l'adaptation. Nos résultats suggèrent donc que les formes d'adaptation à la fermeture de DeepDotWeb ne sont pas toujours optimales et imposent des contraintes non négligeables aux participants. Ce constat permet de nuancer les résultats des études quantitatives qui rapportent différentes formes de déplacement à la suite de la fermeture des cryptomarchés (Décary-Hétu et Giommoni, 2017 ; Ladegaard, 2019 ; Soska et Christin, 2015 ; Van Buskirk *et al.*, 2017 ; van Wegberg et Verburgh, 2018). La prise en compte du point de vue des délinquants a permis de constater que le déplacement n'est pas perçu d'un bon œil, qu'il n'est pas toujours facile à réaliser, et qu'à long terme, cela peut générer une perte d'engouement pour les cryptomarchés. Selon Windle et Farrell (2012), la notion même d'être « contraint » de se déplacer signifie que la nouvelle façon de procéder n'était pas la méthode préférée des délinquants, et ce, généralement pour plusieurs raisons. Nos résultats montrent, par exemple, que la fermeture de DeepDotWeb a forcé les participants à se réorganiser d'une manière susceptible de menacer la facilité d'utilisation des cryptomarchés. Or, nous savons que la facilité du processus transactionnel figure parmi les principales motivations des participants pour transiger sur ces marchés anonymes (Van Hout et Bingham, 2013).

Pour cette raison, l'utilisation de stratégies de prévention situationnelle qui augmenteraient les efforts et les risques pour les délinquants tout en réduisant leurs bénéfices potentiels semble être une avenue intéressante pour les forces de l'ordre impliquées dans la régulation du *darknet*. L'intervention à l'étude représente un véritable *game changer*, dans la mesure où elle cible les facilitateurs des activités des cryptomarchés plutôt que les plateformes transactionnelles. Cette approche pourrait perturber suffisamment le *darknet* de façon que les activités ralentissent, d'autant plus qu'elle a le potentiel de bousculer les activités de plusieurs cryptomarchés simultanément (Greenberg, 2019 ; Martin *et al.*, 2019). Plutôt que de se concentrer sur la fermeture des cryptomarchés, la police pourrait envisager de déstabiliser l'écosystème de sorte que l'incertitude associée aux fraudes et escroqueries en décourage suffisamment pour réduire les activités illicites sur le *darknet*. Pour déterminer la plus-value des stratégies de prévention situationnelle appliquées au *darknet*, des recherches futures pourraient comparer les

coûts engendrés par celles-ci aux ressources nécessaires à la fermeture de cryptomarchés pour déterminer l'approche la plus rentable et la plus réaliste à long terme.

### *Les limites*

L'utilisation de messages de forums comporte certaines limites méthodologiques déjà soulevées par d'autres (Childs *et al.*, 2020 ; Enghoff et Aldridge, 2019). La plus évidente étant que les messages de forums sont extraits de leur contexte d'origine ; cela peut entraîner l'inclusion de messages non pertinents et limiter la capacité du chercheur à en valider l'authenticité. En outre, il est difficile de garantir la participation égale de tous les utilisateurs ciblés par l'intervention, ce qui signifie que les publications sur les forums de discussion peuvent ne pas être représentatives de l'expérience vécue par l'ensemble des acteurs impliqués dans les activités des cryptomarchés (Enghoff et Aldridge, 2019).

## Conclusion

Cette étude démontre que la fermeture des cryptomarchés par les forces de l'ordre ne représente qu'une avenue parmi plusieurs autres susceptibles d'avoir un effet sur les participants. Nos analyses montrent que cibler les facilitateurs des opérations des cryptomarchés peut être une solution intéressante, et ce, même si l'intervention policière à l'étude n'a pas réussi à décourager l'ensemble des participants de transiger sur les cryptomarchés. Il appert, en effet, que les formes d'adaptation mobilisées par les participants ne sont pas optimales et peuvent, à plus long terme, occasionner une perte d'engouement pour les cryptomarchés. Si la recherche quantitative peut être utile pour déterminer l'efficacité d'une mesure de prévention situationnelle pour réduire la criminalité (Jacques et Bonomo, 2017), notre étude démontre la pertinence d'intégrer un volet qualitatif à cette recherche pour mieux cerner les mécanismes de perturbation en cause. Dans le cadre de cette intervention, les participants ont démontré une plus grande sensibilité aux risques internes à l'écosystème. Ce type d'information peut être utile pour orienter les futures interventions policières. L'approche qualitative a également permis de comprendre les raisons pour lesquelles les délinquants ne s'adapteront pas en toutes circonstances, en mettant en évidence les défis que cette adaptation représente. Les chercheurs devraient

se concentrer davantage sur la manière dont la négligence des participants ou encore la facilité d'utilisation des cryptomarchés peut être exploitée pour provoquer des perturbations à long terme.

## Références


Afilipoaie, A. et Shortis, P. (2018). Crypto-market enforcement – New strategy and tactics. *Policy*, *54*, 87-98.

Baker, T. et Wolfer, L. (2003). The crime triangle : Alcohol, drug use, and vandalism. *Police Practice and Research*, *4*(1), 47-61.

Bradley, C. et Stringhini, G. (2019). A qualitative evaluation of two different law enforcement approaches on dark net markets. Dans *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (p. 453-463). IEEE.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A. et Maimon, D. (2019). Situational crime prevention. Dans M. Gill (dir.), *Crime Prevention and Security Management* (p. 17-33). Palgrave MacMillan.

Broséus, J., Rhumorbarbe, D., Mireault, C., Ouellette, V., Crispino, F et Décary-Hétu, D. (2016). Studying illicit drug trafficking on Darknet markets : Structure and organisation from a Canadian perspective. *Forensic Science International*, *264*, 7-14.

Caleb. (2019, 7 mai). *Updated Information About the Investigation into DeepDotWeb.* Repéréàhttps://medium.com/@c5/what-do-we-know-about-the-deepdotweb-seizure-98ca45de9987

Chainalysis. (2020, 28 janvier). *Darknet Market Activity Higher Than Ever in 2019 Despite Closures. How Does Law Enforcement Respond ?* Repéré à https://blog.chainalysis.com/reports/darknet-markets-cryptocurrency-2019

Childs, A., Coomber, R., Bull, M. et 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.

Clarke, R. V. (2009). Situational crime prevention : Theoretical background and current practice. Dans M. D. Krohn, A. J. Lizotte et G. P. Hall (dir.), *Handbook on crime and deviance* (p. 259-276). New York, NY : Springer.

Clarke, R. V. et Cornish, D. B. (1985). Modeling offenders' decisions : A framework for research and policy. *Crime and justice*, *6*, 147-185.

Clarke, R. V. et Eck, J. (2016). Crime analysis from problem solvers in 60 small steps. Repéré à https://www.ojp.gov/ncjrs/virtual-library/abstracts/crime-analysis-problem-solvers-60-small-steps

Cornish, D. B. et Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions : A reply to Wortley's Critique of situational crime prevention. *Crime Prevention Studies*, *16*, 41-96.

Cusson, M. (2005). Comment prévenir ? Les techniques et la méthode de la prévention situationnelle. Dans M. Cusson, B. Dupont et F. Lemieux (dir.), *Traité de sécurité intérieure* (p. 413-428). Montréal, Québec : Hurtubise HMH.

Décary-Hétu, D. et Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets ? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75.

DiPiero, C. (2017). Deciphering cryptocurrency : Shining a light on the deep dark web. *University of Illinois Law Review*, *2017*(3), 1267-1299.

Ekblom, P. et Tilley, N. (2000). Going equipped : Criminology, situational crime prevention and the resourceful offender. *British Journal of Criminology*, *40*, 376-398.

Enghoff, O. et Aldridge, J. (2019). The value of unsolicited online data in drug policy research. *International Journal of Drug Policy*, *73*, 210-218.

Europol. (2019, 8 mai). *DeepDotWeb shut down : Administrators suspected of receiving millions of kickbacks from illegal dark web proceeds*. Europol. Repéré à https://www.europol.europa.eu/newsroom/news/deepdotweb-shut-down-administrators-suspected-of-receiving-millions-of-kickbacks-illegal-dark-web-proceeds

Gabor, T. (1990). Crime displacement and situational prevention : Toward the development of some principles. *Canadian Journal of Criminology*, *32*(1), 41-73.

Gavin, H. (2008). Thematic analysis. Dans H. Gavin (dir.), *Understanding research methods and statistics in psychology* (p. 273-282). SAGE Publications Ltd.

Greenberg, A. (2019, 5 septembre). *Feds Dismantled the Dark-Web Drug Trade—but It's Already Rebuilding*. Wired. Repéré à https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/

Guerette, R. T. et Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits : A review of situational crime prevention evaluations. *Criminology*, *47*(4), 1331-1368.

Gupta, A. (2018). The dark web as a phenomenon : A review and research agenda. Dans *Australasian Conference on Information Systems 2019*, 1-11.

Harocopos, A. et Hough, M. (2005). *Drug dealing in open-air markets. Problem-Oriented Guides for Police, Problem-Specific Guides Series : No. 31*. Washington, DC : US Department of Justice, Office of Community Oriented Policing Services.

Hutchings, A. et Holt, T. J. (2014). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

Hutchings, A., Clayton, R. et Anderson, R. (2016). Taking down websites to prevent crime. Dans *2016 APWG Symposium on Electronic Crime Research (eCrime)* (p. 1-10). IEEE.

Im, E. O. et Chee, W. (2006). An online forum as a qualitative research method : practical issues. *Nursing research*, *55*(4), 267.

Jacques, S. et Bonomo, E. (2017). Learning from the offenders' perspective on crime prevention. Dans B. Leclerc et E. Savona (dir.), *Crime prevention in the 21st century* (p. 9-18). New York, NY : Springer.

Jacques, S. et 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.

Johnson, S., Guerette, R. et 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.

Krippendorff, K. (2004). *Content Analysis : An Introduction to its Methodology* (2e éd.). Thousand Oaks, CA : Sage.

Lacson, W. et Jones, B. (2016). The 21st century darknet market : Lessons from the fall of silk road. *International Journal of Cyber Criminology*, *10*(1), 40-61.

Ladegaard, I. (2019). Crime displacement in digital drug markets. *International Journal of Drug Policy*, *63*, 113-121.

Ladegaard, I. (2020). Open secrecy : How police crackdowns and creative problem-solving brought illegal markets out of the shadows. *Social Forces*, *1*, 1-28.

Lane, B. R., Lacey, D., Stanton, N. A., Matthews, A. et Salmon, P. M. (2018). The dark side of the net : Event analysis of systemic teamwork (EAST) applied to illicit trading on a darknet market. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *62*(1), 282-286.

Lane, B. R., Salmon, P. M., Cherney, A., Lacey, D. et Stanton, N. A. (2019). Using the Event Analysis of Systemic Teamwork (EAST) broken-links approach to understand vulnerabilities to disruption in a darknet market. *Ergonomics*, *62*(9), 1134-1149.

Leontiadis, N. et Hutchings, A. (2015). Scripting the crime commission process in the illicit online prescription drug trade. *Journal of Cybersecurity*, *1*(1), 81-92.

Lorenzo-Dus, N. et 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 and Communication*, *12*(6), 608-626.

Martin, J. (2014). *Drugs on the Dark Net : How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. Palgrave Macmillan. https://doi.org/10.1057/9781137399052

Martin, J., Cunliffe, J. et Munksgaard, R. (2019). *Cryptomarkets : A Research Companion*. Emerald Group Publishing.

Miró-Llinares, F. et Moneva, A. (2020). Environmental criminology and cybercrime : Shifting focus from the wine to the bottles. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, *24*, 491-511.

Oleinik, A., Popova, I., Kirdina, S. et Shatalova, T. (2014). On the choice of measures of reliability and validity in the content-analysis of texts. *Quality & Quantity*, *48*(5), 2703-2718.

Paquet-Clouston, M., Autixier, C. et Décary-Hétu, D. (2018). Comprendre les interactions des vendeurs de drogues illicites sur les forums de discussion des cryptomarchés. *Canadian Journal of Criminology and Criminal Justice*, *60*(4), 455-477.

Ritchie, J., Spencer, L. et O'Connor, W. (2003). Carrying out qualitative analysis. Dans J. Ritchie et J. Lewis (dir.), *Qualitative Research Practice : A Guide for Social Science Students and Researchers* (p. 219-262). Londres, Royaume-Uni : Sage.

Soska, K. et Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. Dans *24th {USENIX} security symposium ({USENIX} security 15)*, 33-48.

United States of America v. Tal Prihar et al. Criminal case No.19-115. Western District of Pennsylvania, Acte d'accusation déposé le 24 avril 2019 aux termes de l'article 18 U.S.C. § 1956(h).

Van Buskirk, J., Bruno, R., Dobbins, T., Breen, C., Burns, L., Naicker, S. et Roxburgh, A. (2017). The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, *173*, 159-162.

van Hardeveld, G. J., Webber, C. et O'Hara, K. (2017). Deviating from the cybercriminal script : Exploring tools of anonymity (mis) used by carders on cryptomarkets. *American Behavioral Scientist*, *61*(11), 1244-1266.

Van Hout, M. C. et Bingham, T. (2013). 'Silk Road', the virtual drug marketplace : A single case study of user experiences. *International Journal of Drug Policy*, *24*(5), 385-391.

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

Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C. et Gajewski, F. (2006). Does crime just move around the corner ? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology*, *44*, 549-592.

Windle, J. et 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.

## Police interventions directed toward crime facilitators

**ABSTRACT** • *Cryptomarkets are e-commerce platforms that specialize in the sale of illicit drugs. The success of these markets has brought them to the attention of law enforcement agencies around the world, but coordinated efforts to shut them down and arrest their participants have so far been ineffective. This study analyses the impact of a recent police intervention that led to the closure of one of the main facilitators of cryptomarket activities, the DeepDotWeb platform. Analysis of 2,841 messages posted on discussion forums dedicated to cryptomarkets made it possible to understand how participants saw the prevention mechanisms used against DeepDotWeb and how they adapted to its closure. The results suggest that interventions that increase the effort and risk associated with browsing the darknet while also decreasing the expected benefits of crime may be more effective in disrupting illicit activities over the long term than the closure of any single market.*

**KEYWORDS** • *Police interventions, cryptomarkets, situational prevention, crime facilitators.*

## Intervenciones policiales sobre facilitadores del delito

**RESUMEN** • *Los cryptomarkets son plataformas de comercio en línea especializadas en la venta de drogas ilícitas. El éxito de estos mercados ha llamado la atención de muchas agencias de aplicación de la ley en todo el mundo, pero sus esfuerzos coordinados para cerrar estos mercados y arrestar a sus participantes hasta ahora han resultado ineficaces. El objetivo de este estudio es describir y comprender los impactos de una reciente intervención policial destinada a suprimir uno de los principales facilitadores de las actividades de criptomercados, la plataforma DeepDotWeb. El análisis de 2.841 mensajes publicados en foros de discusión nos permitió estudiar las percepciones de los participantes sobre los mecanismos de prevención situacional en funcionamiento en el cierre de DeepDotWeb y comprender cómo se han adaptado a él. Los resultados sugieren que las intervenciones con el potencial de aumentar la tensión y el riesgo asociados con la navegación en la red oscura, y que al mismo tiempo pueden disminuir las ganancias del crimen, son posiblemente más efectivas que cualquier cierre de mercado único para interrumpir las actividades ilícitas a largo plazo.*

**PALABRAS CLAVE** • *Intervenciones policiales, criptomercado, prevención situacional, facilitadores de delitos.*