Université de Montréal

Les impacts des opérations policières non traditionnelles sur les participants des cryptomarchés : une étude qualitative

Par

Geneviève S. Chauvin

École de criminologie

Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade de Maîtrise ès sciences (M.sc.) en criminologie

Septembre 2021

Université de Montréal
École de criminologie, Faculté des arts et des sciences

Ce mémoire intitulé

Les impacts des opérations policières non traditionnelles sur les participants des cryptomarchés : une étude qualitative

Présenté par
Geneviève S. Chauvin

A été évalué par un jury composé des personnes suivantes

Rémi Boivin
Président-rapporteur

David Décary-Hétu
Directeur de recherche

Karine Côté-Boucher
Membre du jury

Résumé

Le premier site de cryptomarché, hébergé dans le darkweb, a été lancé en 2011. Ces plateformes rendent possible la vente de divers produits et services illicites. Depuis, de nombreuses interventions policières ont été effectuées dans le but mettre un frein à leurs activités. Malgré de nombreuses tentatives, les effets de ces opérations se sont avérés limités et temporaires. En effet, les revenus générés par cet écosystème sont en constante augmentation. Récemment, les forces policières ont changé leur approche et ont tenté de nouvelles stratégies pour mettre un terme à ce trafic. L'efficacité de ces interventions reste inconnue, car très peu d'études s'y sont attardées. L'objectif de ce mémoire est donc de comprendre quels sont les impacts des opérations policières non traditionnelles sur les participants des cryptomarchés. À l'aide de données récupérées sur différents forums de discussion orientés sur cet écosystème distinct et sa communauté, nous étudierons les effets de deux opérations policières récentes, soit la fermeture de la plateforme DeepDotWeb, et l'opération DisrupTor. Les principaux résultats démontrent que ces interventions ont ébranlé les activités commerciales de ces sites et ont affecté la confiance des membres de la communauté. Malgré l'augmentation de la perception des risques chez plusieurs, les membres ne sont toutefois pas découragés et tentent de trouver une façon de contourner les obstacles imposés par les interventions des forces de l'ordre, en améliorant la structure en place ou en innovant vers de nouveaux outils technologiques. Cependant, les capacités d'adaptation des participants semblent atteindre une certaine limite, et leur essoufflement est perceptible.

Mots clés : intervention policière, cryptomarché, adaptation, trafic de stupéfiants, réduction de l'offre et de la demande, déplacement

Abstract

The first cryptomarket, hosted in the darkweb, was launched in 2011. These platforms make it possible to sell various illicit products and services. Since then, numerous police interventions have been carried out with the aim of shutting down their activities. Despite many attempts, the effects of the opreations turned out to be limited and temporary. Indeed, the income generated by these websites is constantly increasing. Recently, the police forces have changed their approach and tried new strategies in order to stop this narcotics network. The effectiveness of these interventions remains unknown, as very few studies have focused on them. The objective of the research is therefore to understand the impacts of non-traditionnal police operations on cryptomarket participants. Using data collected from various discussion forums focused on this distinct ecosystem and its community, we will study the effects of two recent police operations : the closure of the DeepDotWeb website, and Operation DisrupTor. The main results show that these interventions have shaken the commercial activities of the ecosystem and have affected the confidence of its community. Despite the increase in risk perception among many, members are not, however, discouraged, and try to find a way to circumvent the obstacles imposed by the police interventions, either by improving the infrastructure in place or by innovating toward new technological tools. However, the coping skills of the participants seem to have reached a certain limit, and their shortness of breath is noticeable.

Keywords : police intervention, cryptomarket, adaptation, drug trafficking, reduction in supply and demand, displacement

Table des matières

Liste des tableaux

Liste des abréviations

BTC – Bitcoin

CIA – Central Intelligence Agency

DARPA – Defense Advanced Research Projects Agency

DDOS – Distributed denial-of-service/Attaque de déni de service

DDW – DeepDotWeb

DNM – DarknetMarket

DOJ – Department of Justice/Département de la Justice des États-Unis

EMCDDA – European Monitoring Centre for Drugs and Drug Addiction

FBI - Federal Bureau of Investigation

IRC – Internet Relay Chat

JCODE – Joint Criminal Opioid Darknet Enforcement

NCIDETF – Northern California Illicit Digital Economy Task Force

OpSec – Operationnal Security/Sécurité Opérationnelle

PGP - Pretty Good Privacy

TOR – The Onion Router

2FA – Two-Factor Authentification – Authentification à deux facteurs

Remerciements

Les deux dernières années furent remplies de challenge, de nuits blanches, d'apprentissages et d'émotions, mais nous sommes tout de même finalement parvenus de l'autre côté! Tout cela n'aurait pas été possible sans la présence et l'appui de certaines personnes que je tiens à mentionner.

Je tiens tout d'abord à remercier mon directeur de recherche, David Décary-Hétu. Tu m'as introduite non seulement à l'univers fascinant du darkweb, mais également au monde de la recherche et de la création du savoir scientifique. Merci pour ta grande disponibilité, pour ta confiance, tes conseils et ta générosité. Et surtout, merci de m'avoir guidé à travers cet immense projet.

Je tiens également à remercier ma famille, et plus particulièrement mes parents. Merci d'avoir toujours été présents, et merci de votre soutien et de vos encouragements incessants depuis le tout début. Vous vous êtes toujours assurés que je ne manque de rien et que j'aie tout en ma possession pour foncer tête première dans mes projets. Je ne serais pas ici sans vous.

Finalement, merci à mes amis pour votre patience, lors de mes disparitions durant les fins de session, et pour votre compassion lorsque j'en avais par-dessus la tête. Grâce à vous, j'ai pu garder un pied sur terre. Votre soutien et votre présence dans ma vie quotidienne ont fait en sorte que les dernières années soient passées beaucoup plus facilement et rapidement.

Introduction

Au tournant du siècle dernier, nous avons été témoins de la remarquable évolution qu'ont connue les technologies de communication, et nous avons vu l'Internet et les technologies de l'information prendre une place d'avant-plan dans nos vies (Brisset et Naegelen, 2008; Flanagin, Metzger, Pure et Markov, 2011). Ces innovations ont permis de développer un nouveau moyen d'effectuer nos transactions, grâce aux sites de commerce en ligne. D'abord popularisés avec la création d'eBay en 1995 (Brisset et Naegelen, 2008), suivi d'Amazon, les achats en ligne occupent actuellement l'une des premières places dans le commerce d'aujourd'hui. Ces développements technologiques n'ont cependant pas seulement profité aux commerçants légitimes; ils ont également ouvert la porte à de prospères criminels, qui ont saisi cette opportunité pour créer des plateformes permettant des transactions de produits et de services illicites (Mikhaylov et Frank, 2016).

Le premier site de cryptomarché, hébergé dans le darkweb, a été lancé en 2011 (Martin, 2014a). Ces plateformes rendent possible la vente de divers produits et services illicites. Depuis, de nombreuses interventions policières ont été effectuées dans le but mettre un frein à leurs activités. Malgré de nombreuses tentatives, les effets de ces opérations se sont avérés limités et temporaires (Bhaskar, Linacre et Machin, 2019; Ladegaard, 2019; Norbutas, Ruiter et Corten, 2020 ; Soska et Christin, 2015; van Buskirk, Bruno, Dobbins, Breen, Burns, Naicker et Roxburgh, 2017). En effet, les revenus générés par cet écosystème sont en constante augmentation (Europol, 2017; Winstock et al., 2019). Récemment, les forces policières ont changé leur approche et ont tenté de nouvelles stratégies pour mettre un terme à ce trafic. L'efficacité de ces interventions reste inconnue, car très peu d'études s'y sont attardées. L'objectif de ce mémoire est donc de comprendre quels sont les impacts des opérations policières non traditionnelles sur les participants des cryptomarchés.

Suite à l'introduction, ce mémoire proposera cinq chapitres. Nous débuterons d'abord par une revue de la littérature, où nous présenterons les principales notions théoriques et empiriques concernant les interventions policières qui ont lieu contre les réseaux de trafic de substances

illicites, dans l'espace physique et dans le cyberespace. Nous discuterons également des cryptomarchés, de leur fonctionnement et des mécanismes et des outils technologiques sur lesquels repose leur infrastructure. Nous observerons également les nouvelles pratiques empruntées par les forces de l'ordre, dans le but de perturber les activités réalisées dans cet écosystème et parvenir à y mettre fin.

Le second chapitre énoncera la problématique et les objectifs de notre recherche. Nous y présenterons également les deux opérations policières qui serviront de contexte dans le cadre de notre étude, soit l'intervention qui a mené à la fermeture de la plateforme informationnelle DeepDotWeb, et l'opération DisrupTor.

Le chapitre suivant expliquera la méthodologie et les sources de données utilisées. Après avoir détaillé des étapes entreprises lors de notre collecte de données, nous mettrons en évidence les raisons pour lesquelles nous avons choisi d'avoir recours à la méthodologie qualitative et à l'approche inductive pour atteindre les objectifs de cette recherche.

Le quatrième chapitre présentera les résultats obtenus lors de nos analyses. Nous discuterons des divers impacts ressentis par les membres de la communauté active dans les cryptomarchés au niveau de l'accès aux plateformes, de la facilité d'utilisation et des risques perçus. Nous observerons également les réactions de ces derniers, en portant attention à d'éventuels signes de dissuasion ou de déplacement de la part des membres.

Le cinquième chapitre prendra la forme d'une discussion, où nous interpréterons les principaux résultats de notre étude, et il offrira une comparaison entre nos conclusions et celles provenant de la littérature. Ce chapitre mènera à une conclusion, où seront également présentées les limites de notre étude ainsi que de possibles perspectives de recherches à explorer dans le futur.

Chapitre 1 : Recension des écrits

1. 1 Les actions policières pour contrer le trafic de stupéfiants

Dans les années 1980, le président américain Reagan a déclaré la guerre contre la drogue (Bagley, 1988). Cette déclaration fut accompagnée de l'implantation d'un grand nombre de politiques internes et externes, ainsi que de l'augmentation des efforts policiers au niveau de la rue, dont les objectifs étaient la répression et le contrôle du trafic de stupéfiants dans les rues du pays (Bagley, 1988; Caulkins, 1993). Malgré les multiples efforts et ressources investis dans cette guerre, ces interventions sont aujourd'hui qualifiées comme ayant été simplement « réactives et contre-productives » (Buchanan et Young, 2000), et les résultats de cette guerre ne permettent toujours pas de la considérer comme étant une réussite (Bagley, 1988; McWilliams, 1994).

Dans la réalisation de leur mandat, les agents des forces de l'ordre oeuvrant dans cette guerre contre la drogue ont recours à différentes stratégies d'intervention. Deux types distincts d'opérations policières existent (Mazerolle, Soole et Rombouts, 2007; Zimmer, 1990). D'abord, il y a les opérations policières réactives. Tel que le nom l'indique, ces interventions sont effectuées suite au déroulement d'un événement criminel. Il peut s'agir de raids (opérations de recherche localisée), de policing intensif (saturation de la présence policière dans un milieu donné), ou encore d'interventions « search and seize », et il s'agit de mettre en place une tactique visant la résolution d'un phénomène ciblé dans le temps et l'espace (Mazerolle et al., 2007).

Viennent ensuite les interventions policières proactives. Les interventions de ce type sont mises sur pied dans un effort anticipatoire, afin de contrer un phénomène criminel plus complexe, qui demande une connaissance du contexte approfondie, ainsi que la mise en place de stratégies organisationnelles développées (Mazerolle et al., 2007). Ces interventions prennent souvent la forme d'un partenariat entre différents groupes de forces de l'ordre, au côté de diverses agences d'application de la loi, ou encore l'emploi tactique d'individus hors de ce domaine. L'implantation d'une police communautaire, qui consiste en la création d'un partenariat entre les forces policières et les habitants d'un quartier, en est un exemple (Mazerolle

et al., 2007; Scott, 2003). Cette stratégie a un but préventif et permet de créer et d'exploiter des liens existant entre les deux groupes, afin d'éduquer et de sensibiliser les individus se trouvant dans un contexte social potentiellement plus à risque de développer des problèmes de criminalité (Scott, 2003).

1. 1. 1 La diminution de l'offre et de la demande

Les différents efforts policiers sont ainsi déployés avec deux objectifs distincts : réduire l'offre de substances dans les rues ou en réduire la demande (May et Hough, 2001). D'abord, les stratégies visant la réduction de l'offre ont comme objectif de diminuer la disponibilité des substances dans les marchés (Murji, 1993). Le fait de rendre certains produits plus rares aura un impact sur le prix des substances, ainsi que sur la facilité des consommateurs à s'en procurer (Hough et Natarajan, 2000; Kerr, Small et Wood, 2005; Murji, 1993). Ceci peut être réalisé par des interventions à la source même de la production. Les efforts d'éradication des plantations, de même que l'identification, l'interception et la destruction de larges quantités de marchandise au moment de la livraison aux revendeurs ont pour objectif principal de contrecarrer les efforts des trafiquants, en retirant du marché d'importantes quantités de substances destinées à la revente (Mazerolle et al. 2007).

Il existe également plusieurs stratégies pouvant mener à la réduction de l'offre de substances au niveau des marchés dans la rue. Parmi ces stratégies se trouvent les opérations « crackdown », soit des interventions policières hautes en intensité et en visibilité, limitées dans le temps, qui se concentrent sur une cible précise (Best, Strang, Beswick et Gossop, 2001; Mazerolle et al., 2007). Les opérations « crackdown » sont généralement composées de l'augmentation de la présence policière ressentie, notamment grâce à des patrouilles plus fréquentes, à la mise en place d'opérations de surveillance et à une série d'arrestations et de saisies successives et remarquées (Scott, 2003). Le fait d'avoir recours à ce type d'intervention hautement visible vise le découragement de certains revendeurs actifs ou potentiels à poursuivre de telles activités, occasionnant par le fait même une réduction dans le nombre de fournisseurs actifs, et donc, de substances disponibles (Fader, 2016; Moeller, Copes et Hochstetler, 2016).

Les stratégies opérant pour la réduction de la demande cherchent à diminuer le nombre de consommateurs actifs, ainsi que la quantité de substances consommées (Hough et Natarajan, 2000), en augmentant la perception des risques et du coût reliés à l'achat de substances illicites. Les forces de l'ordre y parviennent, par exemple, en réalisant des opérations de policing sélectif, soit l'arrestation d'individus identifiés comme étant dépendants. Le retrait des plus importants consommateurs aura comme effet d'abaisser la demande de consommation, et ébranlera le fonctionnement du marché (May et Hough, 2001). Une autre stratégie utilisée est celle d'augmenter les inconvénients dans le processus d'achat (appelé « inconvenience policing » (Moore, 1990)). En imposant des obstacles supplémentaires dans le parcours suivi par le consommateur pour atteindre la marchandise, tels que des patrouilles plus fréquentes, la présence d'agents doubles, l'installation de surveillance informelle ou le remaniement des installations dans les lieux de consommation, la réalisation de la transaction devient plus ardue et risquée pour le client. L'augmentation du temps et des efforts requis pour parvenir à se procurer certaines substances aura comme effet d'augmenter le prix effectif (non monétaire) auprès des consommateurs, ce qui pourrait décourager les utilisateurs moins motivés ou occasionnels (Caulkins, 1993; Kleiman et Smith, 1990; Murji, 1993; Moore, 1990; Pearson, 1992), et pourrait donc décourager ces derniers dans la poursuite de leurs activités (Murji, 1993). Les forces de l'ordre parviennent donc à réduire les activités économiques du marché en diminuant le nombre d'individus y prenant part, et en limitant son développement et ses revenus potentiels (May et Hough, 2001).

1. 1. 2 L'efficacité des mesures utilisées contre les réseaux de vente de drogue

Après plusieurs décennies d'acharnement de la part des gouvernements et des agences d'application de la loi pour venir à bout de la guerre contre la drogue, il semblerait que leurs efforts ne soient pas synonymes de succès (Bagley, 1988; McWilliams, 1994). En effet, plusieurs études ont tenté de mesurer l'efficacité des opérations menées contre les réseaux de trafiquants de drogue. Malgré les observations de certains dérangements obtenus suite à une opération policière réussie (Aitken, Moore, Higgs, Kelsall et Kerger, 2002; Cohen, Gorr et Singh, 2003;

Kleiman, 1988), la majorité des opérations n'ont produit aucun impact majeur sur les marchés de vente de drogue. D'abord, les résultats des opérations policières contre les réseaux de trafic de drogues seraient temporaires et d'une efficacité limitée. Les impacts modestes se feraient ressentir le temps que dure l'intervention policière; une fois la présence policière retirée, les effets s'estomperaient et la normalité reviendrait (Cohen et al., 2003; Sherman et Rogan, 1995). Deux semaines après une opération majeure comprenant plusieurs « crackdown » ayant eu lieu dans dix quartiers différents de Londres, en 2000, Best et al., (2001) ont interviewé plusieurs habitués des marchés visés (N=174), afin d'évaluer les impacts de cette intervention. Les résultats sont mitigés ; il ne semble pas y avoir de changement au niveau du prix, de la pureté ou de la disponibilité des substances dans la rue. Cependant, ils notent une baisse de la demande et du nombre total d'achats impliquant de l'héroïne ou du crack, dans les endroits situés à proximité des interventions. D'autres études aboutissent également à des constats similaires (Caulkins et Reuter, 1998; Mazerolle et al., 2007; Wood et al., 2004). En 2002, Aitken et al., se sont attardés aux impacts causés par l'opération Clean Heart, au cours de laquelle il y a eu une saturation de la présence policière dans un quartier aux prises avec des problèmes de trafic de stupéfiants. Malgré une visibilité haute et soutenue des forces de l'ordre dans le quartier, les impacts de l'opération se sont avérés superficiels, temporaires, et ont rapidement été remplacés par des effets négatifs : une hausse des actes violents et des habitudes de consommation dangereuses en public sont apparues dans le quartier visé par l'intervention (Aitken et al., 2002). Différentes études abondent d'ailleurs dans le même sens; lors des interventions policières, les impacts sont parfois importants au début (Smith, 2001), mais se résorbent rapidement (Sherman et Rogan, 1995; Smith, 2001).

Plusieurs études font également état de mouvements de déplacement des activités criminelles suite à la présence des forces de l'ordre dans un milieu (Curran, Dale, Edmunds, Hough, Millie et Wagstaff, 2005; Sherman, 1990; Sherman et Rogan, 1995). Ce phénomène n'implique pas uniquement la relocalisation des activités dans un milieu voisin, mais peut également engendrer des comportements problématiques supplémentaires. Maher et Dixon (1999), par exemple, ont dénoté une augmentation d'habitudes de consommation à risque chez les individus fréquentant les lieux visés par une frappe policière, alors que Wood et al., (2004), ont remarqué que la consommation, généralement réalisée en lieu privé, s'était déplacée dans les

parcs et lieux publics en réponse à la perte de leurs lieux de consommation habituels. De plus, ces interventions policières affectent davantage les membres les moins dominants des réseaux ciblés. Il est donc fréquent de voir les individus interceptés être remplacés rapidement par d'autres membres qui conservent ainsi intactes les activités du réseau (Edmunds, Hough et Urqufa, 1996; May et Hough, 2001).

Les membres des marchés ciblés démontrent de bonnes capacités d'adaptation qui leur permettent de mettre sur pied des stratégies afin de contrecarrer les obstacles imposés par les forces de l'ordre. Certains organisent un système de coopération avec d'autres membres dans le but d'avertir lors de la présence de membres des forces de l'ordre dans un périmètre délimité (Johnson et Natarajan, 1995), alors que d'autres établissent des mots de passe afin de s'identifier et de valider leur appartenance au réseau de vente de drogue (Johnson et Natarajan, 1995). D'autres utilisent des outils technologiques, tels que des téléphones portables, afin d'améliorer l'efficacité de leurs opérations et de passer d'un marché ouvert à un marché fermé, et par le fait même moins risqué (Edmunds et al., 1996; May et Hough, 2001).

Finalement, plusieurs chercheurs ont identifié des changements dans les comportements et les habitudes des participants influencés par une intervention policière à l'endroit de leur réseau : certains camouflent leur marchandise sur eux, d'autres préfèrent diminuer la quantité qu'ils transportent lors de leur déplacement ou encore la cacher en lieu sûr, pour ainsi réduire les risques d'être appréhendés alors qu'ils sont en possession (Erickson et al., 2013; Fader, 2016; Jacobs, 1996; Smith et al., 1992). La présence de ces adaptations et innovations, orchestrées par les participants aux réseaux de vente de stupéfiants, cause certains soucis aux forces de l'ordre. En développant de telles stratégies dans le but de contourner ou diminuer les impacts des interventions policières, les participants rendent plus difficile la réussite des interventions menées par les forces de l'ordre (VanNostrand et Tewksbury, 1999).

1. 1. 3 Les interventions policières et la dissuasion

En criminologie, la dissuasion s'observe lorsqu'un individu se retient de commettre un acte criminel afin d'éviter les sanctions ou punitions qui pourraient en découler (Cusson, 1993; MacCoun, 1993; Paternoster, 2010). Basée, d'abord, sur les écrits de Beccaria, cette théorie veut que l'individu soit rationnel et fasse des choix libres et éclairés (O'Connell, Visher, Martin, Parker et Brent, 2011). Ainsi, si le délinquant potentiel considère que ses actions risquent de lui apporter plus de conséquences négatives que de bénéfices, ce dernier cherchera à éviter les punitions en refusant ou reportant la commission de son acte (Bossner, 2021; Cusson, 1993; Gibbs, 1975; Paternoster, 2010). Pour que la dissuasion soit efficace, la sanction doit posséder trois caractéristiques : la célérité, la certitude et la sévérité (Alinsato, 2012; MacCoun, 1993; O'Connell et al., 2011). La sanction doit donc se produire de manière contemporaine par rapport à l'acte. Elle doit également être assez sévère pour décourager les individus dans la poursuite de leurs activités, en imposant des conséquences négatives plus imposantes que les bénéfices qui pourraient en être retirés (Nagin, Solow et Lum, 2015). Finalement, l'aspect de la certitude serait le plus important des trois (Maimon, 2020; Nagin et al., 2015) : un individu qui perçoit une certitude de punition suite à la commission d'un acte criminel, même si cette dernière est modérée, sera moins déterminé dans son passage à l'acte que s'il perçoit une peine sévère, mais peu probable et dont il pourrait potentiellement se soustraire (Maimon, 2020).

Il existe différents types de dissuasion abordés dans la littérature. D'abord, la dissuasion est considérée générale lorsque les effets de la menace de la peine imposée découragent l'ensemble des membres d'une population à poser le geste ciblé. La dissuasion spécifique, de son côté, n'implique que les individus déjà concernés par l'expérience de la punition, et vise plutôt la prévention de la récidive chez les individus sanctionnés (Chalfin et McCrary, 2017; Maimon, 2020). Il existe également un concept de dissuasion restrictive, reposant sur les principes que les individus réagiront de manière rationnelle face à l'augmentation des facteurs de certitude et sévérité des sanctions. Ainsi, face à de nouvelles mesures ou stratégies visant à diminuer la commission d'un acte en particulier, les individus visés par ces mesures chercheront à trouver des façons de s'adapter, tout en maintenant leurs activités. Ils effectueront des modifications dans leurs comportements et seront même prêts à réduire certaines de leurs activités afin d'éviter les risques de sanctions, mais ne seront cependant pas découragés au point d'abandonner leurs activités en entier (Fader, 2016). Finalement, la littérature fait également référence à la

dissuasion initiale et à la dissuasion résiduelle. La dissuasion initiale est définie par des effets dissuasifs immédiats, observés durant et immédiatement suite à une intervention policière. La dissuasion résiduelle sera observée par les effets dissuasifs persistant dans un environnement, suite au départ des forces policières (Sherman, 1990).

Peu de résultats, dans la littérature, indiquent la présence d'un effet de dissuasion chez les participants des réseaux de vente de stupéfiants, suite aux opérations policières. Dans une revue de plusieurs opérations « crackdown » ayant eu lieu contre des marchés de vente de drogue, Sherman (1990) indique que ces interventions produisent généralement des effets insatisfaisants. En plus de ne remarquer aucun signe de dissuasion résiduelle, l'auteur indique que les activités reprennent rapidement, une fois la présence policière retirée des marchés (Sherman, 1990). Quelques études dénotent la présence d'une dissuasion restrictive, soit l'obligation ressentie par les membres de modifier certains aspects de leurs habitudes ou comportements, afin de permettre la survie de leurs activités illicites (Erickson, van der Maas et Hathaway, 2013; Jacobs, 1996). La majorité des chercheurs, cependant, indiquent avoir remarqué que la majorité des participants à ces réseaux sont motivés à poursuivre leurs activités au même niveau. Ils vont plutôt tenter de s'adapter et d'innover, dans le but de contrecarrer les effets négatifs des interventions des forces de l'ordre contre eux (Edmunds et al., 1996; Erickson et al., 2013; Fader, 2016; Johnson et Natarajan, 1995; May et Hough, 2001; Smith, Sviridoff, Sadd, Curtis et Grinc, 1992).

1. 2 Le cyberespace et les drogues

Jusqu'à présent, nous avons traité des opérations policières contre les réseaux de vente de substances illicites ayant lieu dans l'espace physique. Cependant, il existe également un effervescent marché pour ces substances, qui se retrouve au niveau du cyberespace. Le développement de l'Internet et des différentes technologies de communication a changé la manière de réaliser des échanges commerciaux et de se procurer les produits de consommation de la vie courante (Brisset et Naegelen, 2008; Flanagin et al., 2011; Goullé, Mura et Guerbet, 2017), entre autres grâce à l'émergence des réseaux sociaux et à l'arrivée des plateformes de commerce électronique dans notre quotidien (Demant, Bakken, Oksanen et Gunnlaugsson, 2019). Les marchés proposant des biens et des substances illicites, en constante recherche

d'expansion, n'échappent pas à cette nouvelle vogue d'échanges. Cependant, au lieu de se produire sur les mêmes plateformes que les sites qui permettent la vente de biens ordinaires, ces activités ont lieu dans une partie cachée de l'Internet. L'Internet se divise en deux sections; le web ouvert, dit de surface, et le web profond. Le web de surface inclut tout ce qui est indexé et accessible via les moteurs de recherche réguliers, tel que Google. Cette section de l'Internet ne représente qu'une portion minime de la totalité du web; entre 4% (Goullé et al., 2017) et 10% de l'Internet en entier (Hurlburt, 2017) se trouverait dans cette partie ouverte. Le web profond contient donc la grande majorité du contenu se trouvant sur le web; tel que, par exemple, les données privées et les réseaux internes appartenant aux individus ou aux corporations ou encore le contenu des boites courriel. Pour atteindre cette portion de l'Internet, les sites WWW et les moteurs de recherche réguliers ne sont pas utiles; l'aspect caractériel de cette section du web est de « prôner la sécurité par l'obscurité » (Hulrburt, 2017). Finalement, c'est dans le web profond que se trouve le darkweb. Cette section du web est, d'ailleurs, uniquement accessible via l'utilisation d'outils et de technologies de cryptage (Van Hout, 2015). Un de ces outils, le réseau TOR (The Onion Router), permet de préserver l'anonymat en protégeant l'identité et en brouillant la localisation des utilisateurs des différents sites qui y sont hébergés (Owen et Savage, 2015). Initialement utilisé pour protéger la liberté d'expression et permettre la dénonciation politique, TOR attire de plus en plus d'individus cherchant à commettre des actes illicites et criminels en toute tranquillité. En 2015, il était estimé que TOR accueillait plus de 2 millions d'usagers par jour, et ces chiffres sont en augmentation constante (Owen et Savage, 2015).

C'est donc dans le darkweb, et par l'entremise du réseau TOR, que nous retrouvons les marchés de drogues illicites en ligne, les cryptomarchés. Ce terme, créé par James Martin (2014a), désigne des sites de type forum ou plateforme commerciale en ligne, où différents biens et services sont offerts. Ces échanges ont lieu entre deux parties utilisant les technologies de cryptage et les outils d'anonymisation. Comme Martin (2014a) le signale, toutes les transactions effectuées sur ces sites ne sont pas nécessairement illégales, et toutes les activités qui ont lieu dans ces plateformes, ainsi que les participants qui y prennent part, ne sont pas obligatoirement toutes en relation avec la cybercriminalité. Toutefois, la majorité l'est : 62% du contenu retrouvé sur ces sites est lié à la vente de drogues et de substances illicites (Europol, 2017). Les participants des cryptomarchés présentent des habitudes de consommation variées et multiples;

les usagers se procurent le plus souvent de la MDMA (66,8%), du LSD (55,6%) ou du cannabis (54,8%). Les drogues dures figurent également dans la liste des produits couramment achetés par l'entremise des cryptomarchés : 28% des usagers s'y sont procuré du crystal meth, et 26% y ont acheté de la cocaïne (Winstock et al., 2019). Ces sites ne servent pas qu'à la consommation individuelle. En étudiant les annonces du défunt cryptomarché Silk Road, Aldridge et Décary-Hétu (2016), il a été démontré que 26% des annonces du site concernaient des articles fichés à 1000$ et plus, et que la moyenne en poids des articles annoncés dans cette catégorie atteignait les 402,17g. Les auteurs sont donc parvenus à la conclusion que les cryptomarchés peuvent également servir à la facilitation de vente de drogue « en gros », se positionnant comme une source de ravitaillement pour les groupes criminalisés qui cherchent à s'enrichir grâce à la revente de stupéfiants. Les profits de ces marchés sont d'ailleurs en constante croissance, ayant atteint les 350 millions US$ en 2015 (Martin, Cunliffe et Munksgaard, 2019). Malgré le fait que ces chiffres soient minimes par rapport au montant total d'argent généré par le trafic de drogues à l'échelle mondiale, Europol (2017) stipule tout de même que ce type de marché, quoique modeste, reste significatif, et représente un potentiel de croissance important. Le Global Drug Survey, dans son plus récent sondage, abonde en ce sens: une hausse du nombre d'individus qui se sont approvisionnés via les cryptomarchés est observable depuis quelques années (Winstock et al., 2019). Au Canada, notamment, ce chiffre est passé de 5,3% en 2015, à 11,4% en 2019, alors qu'au Royaume-Uni, cette proportion a doublé entre 2015 (14,3%) et 2019 (28,6%) (Winstock et al., 2019).

1. 2. 1 L'origine des cryptomarchés

Il faut remonter jusqu'en 1971, dans les laboratoires informatiques des universités américaines, afin de retracer la première transaction de vente de drogue en ligne. C'est en se servant des technologies en place que des étudiants de l'Université de Stanford et du MIT procédaient à des transactions impliquant la vente de marijuana (DiPiero, 2017). Le commerce en ligne s'est ensuite développé grâce à l'expansion et la mondialisation de l'Internet, un phénomène qui a conduit à la possibilité de transférer des biens et d'offrir des services à l'échelle planétaire (DiPiero, 2017). Les cryptomarchés ont d'ailleurs été créés grâce à la conjoncture de plusieurs éléments. D'abord, l'arrivée des technologies de cryptage, au tournant des années 1990,

qui sont attribuables aux forces des US Navy (Goullé et al., 2017), représente le premier de ces éléments. Créées par la US Defense Advanced Research Projects Agency (DARPA), ces technologies avaient pour fonction d'anonymiser les informations concernant l'origine et la destination des trafics internet, protégeant ainsi la provenance et la destination des communications émises (Martin et al., 2019a). Les cryptomarchés sont également les descendants des marchés d'échanges existant auparavant sur les Internet Relay Chat (IRC), des salles de clavardages et de forums en ligne, dans les années 1990 et au début des années 2000. Les usagers de ces plateformes s'en servaient pour se rencontrer, pour discuter et pour effectuer des échanges en ligne. Cette façon de faire a d'ailleurs rapidement attiré l'attention des forces de l'ordre, qui ont procédé à une série d'arrestations et à la fermeture des plateformes impliquées (Aldridge et Décary-Hétu, 2016). Finalement, avec la création de TOR, en 2004, et l'arrivée des cryptomonnaies dans l'usage courant avec le Bitcoin en 2008 (Europol, 2017), tous les éléments propices à la création des cryptomarchés étaient réunis (Goullé et al., 2017). C'est donc à partir de 2011 que fut mis en ligne le premier espace de cybermarché, le cryptomarché Silk Road, où étaient offertes différentes marchandises illicites et où la commission d'actes criminels était facilitée par la vente de matériel informatique destiné à la fraude et au « hacking ». Pour paraphraser les paroles de son créateur, « tout était en place, il n'eut qu'à mettre les morceaux ensemble » (Martin et al., 2019a).

1. 2. 2 Le fonctionnement du darkweb

Les cryptomarchés sont en tout point semblables aux sites de commerce électronique populaires qui se retrouvent dans le web régulier (Barratt, Lenton, Maddox et Allen, 2016; Europol, 2017). Il s'agit de plateformes transactionnelles qui revêtent le rôle d'intermédiaire entre les vendeurs et les clients potentiels. En échange d'un certain pourcentage des ventes effectuées sur la plateforme, les administrateurs s'occupent d'établir et de maintenir une cohésion entre les usagers et les transactions, et mettent en place un système qui permet aux usagers d'effectuer leurs activités commerciales avec une certaine stabilité (Martin et al., 2019a). La structure des cryptomarchés ressemble donc grandement à celle de sites plus connus tels qu'eBay et Amazon. D'abord, il y a l'espace où les vendeurs détaillent publiquement la liste des

produits et des services qu'ils offrent, ainsi que les conditions entourant leurs échanges. Les clients potentiels parcourent librement les annonces et les trient selon leurs intérêts (Broséus, Rhumorbarbe, Mireault, Ouellette, Crispino et Décary-Hétu, 2016). L'acheteur intéressé peut alors entrer en contact avec l'annonceur et procéder à l'achat. Une fois la transaction complétée, la marchandise est envoyée par la poste (Martin, 2014a). Des systèmes de notation sont mis en place et les membres sont encouragés à laisser un commentaire portant sur le déroulement de la transaction achevée et sur la qualité de la marchandise (Broséus et al., 2016).

Là où les plateformes comme eBay et les cryptomarchés diffèrent, est d'abord dans la nature des articles offerts; les cryptomarchés sont majoritairement reconnus pour leur offre diversifiée de biens et de services illicites (Martin, 2014a). De plus, les individus fréquentant ces plateformes font généralement usage des différents outils de cryptage et d'anonymisation qui y sont disponibles, un phénomène qui est d'ailleurs moins courant lors de l'utilisation des sites de commerce électronique réguliers (Martin, 2014b; Spagnoletti, Ceci et Bygstad, 2018). La présence de telles technologies offre l'opportunité aux criminels d'y vendre une variété de produits et de services, tel que des drogues, des armes, des logiciels informatiques permettant la réalisation d'attaques informatiques ou de fraudes bancaires, le tout en réduisant considérablement les probabilités d'être découverts par les forces de l'ordre.

1. 2. 3 Les technologies qui soutiennent les cryptomarchés

En théorie, l'utilisation des cryptomarchés est relativement simple, facile et sécuritaire. C'est d'ailleurs l'une des raisons pour lesquelles l'utilisation de ces plateformes web est de plus en plus répandue. L'utilisation des différentes technologies d'anonymisation, tel que TOR ou encore les clés PGP (Pretty Good Privacy – un logiciel de cryptographie qui protège l'anonymat des usagers grâce à des clés d'identification personnelles), est indissociable des activités se déroulant sur ces sites (Europol, 2017).

Ces technologies camouflent d'une part, la localisation des serveurs hébergeant les cryptomarchés, les rendant très difficiles à localiser par les forces de l'ordre, et font de même pour les adresses IP des usagers ; les participants profitent donc d'une double protection, soit de

leur identité, ainsi que de l'endroit physique où ils se trouvent lorsqu'ils accèdent aux cryptomarchés. Les cryptomarchés opérant dans la partie cachée du web, ils ne sont donc pas accessibles via les navigateurs de recherche communs (Evangelista, Allodi et Cremonini, 2018). TOR (The Onion Router) est le principal navigateur utilisé pour accéder aux différentes plateformes de cryptomarché (Shortis, Aldridge et Barratt, 2020). La marche à suivre pour y accéder est très simple : une courte recherche internet et quelques étapes permettent aux utilisateurs de l'installer et d'y accéder (Gupta, Maynard et Ahmad, 2018). Par la suite, son utilisation est en tout point similaire à celle des navigateurs courants, tels que Firefox ou Explorer (Gupta et al., 2018).

TOR fut initialement créé par les instances gouvernementales américaines, dans le but de camoufler et de sécuriser les communications militaires (DiPiero, 2017). En temps normal, lorsqu'un utilisateur navigue sur le net, ses déplacements et ses données sont liés à son adresse IP, ce qui permet d'identifier et de localiser la provenance physique de l'usager. L'utilisation de TOR rend ainsi très difficile de remonter à la source de la navigation (DiPiero 2017). Ce navigateur permet donc à ses utilisateurs de masquer leur adresse IP, les protégeant contre les usagers malveillants et les forces de l'ordre qui tenteraient de les identifier et les localiser (Shortis et al., 2020). Cela constitue donc la première étape vers l'établissement de leur anonymat (Evangelista et al., 2018).

Les utilisateurs des cryptomarchés peuvent également faire usage d'autres technologies d'anonymisation, tels que les outils permettant le cryptage des conversations (Bancroft et Reid, 2016). La clé PGP (Pretty Good Privacy) est d'ailleurs un protocole de cryptage utilisé par bon nombre de membres et très courant dans l'univers des cryptomarchés.

Afin de conclure les transactions, les participants des cryptomarchés ont recours à la cryptomonnaie. Créée dans le but de compléter des échanges directement entre les participants, et sans avoir recours à l'implication des institutions bancaires comme tierce partie (Europol, 2017 ; van Hardeveld, Webber et O'Hara, 2017), cette monnaie n'est sous le contrôle d'aucun gouvernement ni d'aucune institution bancaire et difficilement retraçable. Cela explique pourquoi son utilisation permet de garder un certain niveau d'anonymat (Europol 2017; Spagnoletti et al., 2018), et est répandue partout sur la planète (Europol, 2017).

1. 2. 4 L'infrastructure entourant les cryptomarchés

De sa création, en 2011, jusqu'à sa saisie par les forces de l'ordre en 2013, le cryptomarché Silk Road a détenu le monopole des activités dans les cryptomarchés. Sa fermeture a laissé un vide important dans l'écosystème et, depuis, de nombreux marchés sont apparus et ont tenté de faire leur place dans le monde de la cybercriminalité, créant par le fait même un environnement décentralisé (Martin, 2014a; van Buskirk, Roxburgh, Farrell et Burns, 2014).

Cette situation particulière crée une compétition entre les différents cryptomarchés, où chacun essaie de se démarquer et d'attirer sa propre clientèle. Chaque plateforme tente donc de présenter des aspects et des fonctionnalités particuliers, afin de susciter l'intérêt chez les participants (Martin, 2014a). Cette réalité a ouvert la porte à une industrie de services, où plusieurs offrent de l'assistance professionnelle en conception de site web, en relations publiques ou en organisation publicitaire, afin de venir en aide aux administrateurs de cryptomarchés (Martin, 2014a), et entraîne la professionnalisation de l'infrastructure qui soutient les cryptomarchés.

1. 2. 4. 1 Les sites de forum

L'économie globale des cryptomarchés ne repose pas seulement sur les marchés en soi; la communauté complète repose sur une infrastructure de plus en plus complexe, professionnelle, formée de sites web indépendants oeuvrant dans le but de faciliter et de sécuriser l'opérationnalisation et l'utilisation des plateformes (Ladegaard, 2020). D'abord, les forums jouent un rôle très important dans l'écosystème. Ils facilitent la communication entre les utilisateurs, et facilitent le partage du capital illicite au sein de la communauté (Paquet Clouston, Autixier et Décary Hétu, 2018). Les membres y partagent et y valident leurs connaissances en matière de sécurité et de techniques criminelles, et discutent des outils permettant la détection et la gestion des risques (Grimani, Gavine et Moncur, 2020). Y sont également discutées les techniques efficaces pour, entre autres, faciliter la dissimulation et contrer la détection, ainsi que des guides pour débutants et des tutoriels pour faciliter l'utilisation des technologies dédiées à la protection des participants (Martin, 2014a).

Ces plateformes de partage communiquent également, en temps réel, les informations concernant les interventions policières, provoquant ainsi une actualisation constante des stratégies et des avancées des forces de l'ordre contre l'écosystème et ses usagers (Martin, 2014a). Ce flux d'informations constant permet l'augmentation de la capacité des usagers à évaluer les menaces émergentes, et à s'en protéger efficacement (Aldridge et Askew, 2017; Bancroft et Reid, 2016; Martin, 2014a). Bref, ces forums servent à la formation d'une communauté outillée pour faire face aux différents risques, et ouvrent ainsi la porte à la création d'un potentiel commercial plus grand et plus solide pour les cryptomarchés (Motoyama, McCoy, Levchenko, Savage et Voelker, 2011).

Finalement, les forums jouent un grand rôle dans la formation et le maintien de la cohésion de la communauté. Il s'agit d'un espace de socialisation, où il est possible de discuter de tous les sujets (Grimani et al., 2020). Ces sites de partage sont importants dans la création et le maintien d'une communauté propre aux cryptomarchés. Il s'agit d'un des rôles importants revêtus par les plateformes de forum, car une communauté forte représente permet une meilleure capacité de résistance aux chocs ; en effet, plus les usagers ont la capacité de se regrouper, se soutenir et se réorganiser, plus l'écosystème est apte à surmonter les attaques dirigées vers lui (Barratt, 2015; Smith et Frank, 2020). C'est d'ailleurs là, selon Smith et Frank (2020), où les cryptomarchés gagnent contre les forces de l'ordre; ils sont nettement en avance dans leur capacité de partage des connaissances et de réactions aux changements.

1. 2. 4. 2 Les sites d'informations et de nouvelles

Certains sites sont voués au partage d'informations et de nouvelles concernant l'écosystème. Ces sites permettent la diffusion d'informations et de conseils, et documentent l'actualité pertinente aux cryptomarchés (Bancroft et Reid, 2016; Martin, 2014a). Certains sites indépendants offrent également des informations sur les vendeurs et les marchés actifs et fiables. DeepDotWeb, créé en 2013, était d'ailleurs l'un des sites informatifs les plus populaires et appréciés par les utilisateurs (Ladegaard, 2020). En plus de fournir les dernières actualités, il y était suggéré de nombreux tutoriels et guides pour débutants, et l'on pouvait y retrouver des répertoires de liens validés et sécuritaires, réduisant ainsi les risques de fraudes et

d'hameçonnage pour les usagers qui les utilisaient. De telles plateformes aident au partage des connaissances, à la réduction des risques, et permettent la croissance des activités économiques des cryptomarchés (Ladegaard, 2020; Martin et al., 2019a).

1. 3 La confiance dans le cyberespace

L'anonymat dans le milieu du commerce en ligne est nécessaire et problématique à la fois. D'une part, il s'agit d'un élément essentiel pour la protection des intérêts des usagers, alors que d'autre, cela augmente grandement les risques pris lorsque les participants font affaire avec d'autres usagers (Martin, 2014a), car ils ne connaissent ni leur identité, ni leurs intentions. La confiance entre les participants est donc un élément primordial, autant pour les communautés prenant part à des sites aux activités illégales que pour les individus fréquentant les sites standard de commerce électronique. Mayer, Davis et Schoorman (1995) définissent la confiance, dans un contexte commercial, comme étant le choix d'un individu de se placer en position de vulnérabilité, par rapport à la volonté d'un autre. Il se rend donc susceptible d'être une victime facile face à un potentiel individu malhonnête. C'est pourquoi les sites de commerce électronique ont mis sur pied des systèmes de notations entre participants, qui permettent d'offrir un pointage de confiance, ou de popularité aux membres, et qui facilitent ainsi la réalisation des transactions (Brisset et Naegelen, 2008; Xiong et Liu, 2003). Le premier système de la sorte fut instauré par eBay, et était un système d'évaluation des membres après chaque transaction (Brisset et Naegelen, 2008; Xiong et Liu, 2003).

1. 3. 1 La confiance dans les cryptomarchés

Les cryptomarchés sont caractérisés par deux éléments : le caractère illicite des activités qui y sont produites, et l'importance de l'anonymat, ou du moins de la dissimulation de l'identité de leurs participants. Dû à l'illégalité de bon nombre des produits disponibles dans ces marchés, les usagers ne peuvent pas s'appuyer sur des normes institutionnalisées formelles pour gérer et garantir le respect des transactions et des accords passés entre eux (Tzanetakis, 2018). Sans ces mécanismes de régularisation, il n'y a aucune protection dont l'acheteur puisse se prémunir pour contrer les tentatives de fraudes et de vols provenant des vendeurs (Holt, Smirnova, Copes et

Chua, 2015). L'aspect illégal des transactions empêche bien évidemment le recours aux forces de l'ordre ou aux instances légales pour aider à la résolution de conflit (Holt et al., 2015).

De plus, l'aspect virtuel et anonyme des cryptomarchés crée une asymétrie de l'information importante. Par asymétrie de l'information, nous entendons le phénomène selon lequel, lors d'une transaction, le vendeur est le seul qui détienne les connaissances complètes concernant l'état réel du produit (qualité, quantité, nature, etc.). Le client est donc à la merci des usagers malhonnêtes (Holt et al., 2015). Comme il n'existe pas de façon de comparer et valider les produits publiés dans les annonces avant de conclure un achat, ils doivent donc s'en remettre totalement à la parole du vendeur (Pace, 2017).

La confiance, autant entre les clients et les vendeurs de la communauté, qu'entre les usagers de l'écosystème et les administrateurs, est cruciale pour le succès et la survie à long terme d'une plateforme commerciale (Pace, 2017). C'est pour cette raison que les administrateurs des cryptomarchés ont mis en place différentes normes informelles et mécanismes qui permettent une certaine régularisation des transactions (Lorenzo-Dus et Di Cristofaro, 2018).

À l'image des sites de commerce électronique populaires dans le web régulier, le concept de la réputation est au premier plan dans les cryptomarchés. Dans un cas comme dans l'autre, la perception du risque qui provient d'une transaction a un impact sur le comportement de l'acheteur. Selon Manchala (2000), dans un contexte de transaction électronique anonyme, le risque est perçu en fonction de trois critères : la réputation du membre avec qui se déroule l'échange, le coût de la transaction et l'objet de la transaction. En effet, les consommateurs sont prêts à investir entre 7% et 10% de plus lorsqu'ils font affaire avec un vendeur de confiance (Huang et Liu, 2010). Le risque est alors perçu comme étant moins important, et ils sont plus à l'aise de dépenser de plus grands montants d'argent.

Atteindre un niveau élevé de réputation est coûteux en temps et en argent pour les vendeurs actifs. Ces derniers doivent maintenir une bonne conduite et faire preuve d'honnêteté sur une longue période avant d'atteindre un statut avantageux. Souvent, les nouveaux vendeurs,

ou ceux qui cherchent à augmenter leur cote devront inciter les clients à venir vers eux, en échange de diminution des prix ou en offrant des promotions lors de la transaction (Przepiorka, Norbutas et Corten, 2017). Plusieurs mécanismes de régulation ont donc été mis en place dans l'écosystème des cryptomarchés, dans le but d'assurer un niveau de risque transactionnel plus bas, et ainsi faciliter l'instauration de la confiance parmi les membres.

De nombreux sites suggèrent un système de notation de leurs membres. Ce système permet aux usagers d'évaluer la qualité des produits, la rapidité du service et le niveau de professionnalisme et de discrétion (emballage furtif) dont font preuve les vendeurs (Barratt, Ferris et Winstock, 2014; Pace, 2017). En plus d'offrir aux acheteurs un aperçu de la qualité du service et du produit, et le niveau de sécurité employé par les vendeurs (DiPiero, 2017), ces systèmes permettent aux participants de se baser sur les expériences des autres avant de prendre le risque d'entrer en relation contractuelle avec un autre usager (Evangelista et al., 2018). Alors que de bonnes notes récompensent de bons comportements (Holt et al., 2015), de mauvaises notes conduisent à une réduction des ventes. Un vendeur malhonnête qui présente un pointage trop bas peut même être forcé de quitter l'écosystème des cryptomarchés; lorsqu'un usager est étiqueté comme fraudeur, ou lorsqu'il présente un rendement trop mauvais, il peut être tout simplement banni de la plateforme dans laquelle il tient ses activités.

Un second système mis en place dans le but de faciliter les transactions dans l'écosystème des cryptomarchés est le système d'entiercement. Cette innovation majeure reproduit, en quelque sorte, les normes de garanties institutionnalisées des plateformes licites de commerce en général (Lorenzo-Dus et Di Cristofaro, 2018; Tzanetakis, 2018). Il s'agit d'un procédé où l'argent impliqué dans une transaction est détenu par une tierce partie, au nom des deux participants à la transaction, et ce jusqu'à ce que le client confirme la réception de la commande (Evangelista et al., 2018; Lorenzo-Dus et Di Cristofaro, 2018).

1. 4 Les avantages, les limites et les risques des cryptomarchés

La raison pour laquelle les cryptomarchés sont de plus en plus populaires au sein de la communauté des consommateurs de drogue, et ce partout dans le monde, est qu'ils représentent une alternative intéressante aux transactions ayant lieu dans la rue. D'abord, plusieurs voient les cryptomarchés comme des facilitateurs au trafic de drogues (Europol, 2017; Goullé et al., 2017; Martin, 2014a). À partir d'un ordinateur et en quelques étapes seulement, les consommateurs peuvent facilement entrer en contact avec plusieurs vendeurs potentiels, localisés partout sur la planète, commander la marchandise désirée et même la faire livrer au pas de leur porte (Evangelista et al., 2018). Cette façon de faire diminue donc grandement les efforts et le temps investis dans la recherche de stupéfiants, en comparaison à ce qu'ils devraient normalement être dans la rue (Aldridge, Stevens et Barratt, 2018; Martin, 2014a).

1. 4. 1 Facilité et accessibilité

La configuration des pages des plateformes commerciales dans le darkweb permet aux consommateurs de consulter de longues listes d'annonces, qui affichent une variété impressionnante de drogues accessibles. Cela permet aux consommateurs d'atteindre un répertoire diversifié de substances (Martin et al., 2019a), ou de mettre la main sur des produits qui ne sont pas nécessairement accessibles via leur marché local (Aldridge et al., 2018). Grâce aux informations détaillées retrouvées dans ces annonces, les participants peuvent même choisir leurs produits en fonction des effets attendus, une réalité que peu peuvent rencontrer dans le trafic de stupéfiants au niveau de la rue (Aldridge et al., 2018).

L'accès à de telles informations se trouvant sur les pages des vendeurs est un avantage distinct des cryptomarchés, comparativement aux marchés dans le monde physique. En effet, les clients potentiels se retrouvent devant la possibilité, tout d'abord, de comparer les offres et les produits disponibles. Il leur est possible de comparer les conditions d'envoi par exemple, ou encore les prix, avant de faire leur choix (Aldridge et al., 2018). Cela encourage également l'instauration de la compétition parmi les vendeurs, qui peuvent être tentés d'offrir certains avantages ou certaines promotions aux consommateurs qui les approchent.

Les vendeurs profitent de l'espace de la plateforme pour décrire leurs produits et promouvoir la qualité de ceux-ci dans le but d'augmenter leurs ventes et d'attirer plus de clients potentiels (Aldridge et Askew 2016). Ces informations servent également aux consommateurs, qui peuvent se faire une idée de la marchandise et des effets escomptés. Le système de feedback des vendeurs et de leurs produits permet aux consommateurs de se créer un jugement sur la qualité du produit et du service offerts (Cox, 2016). Il leur est donc possible de magasiner selon leur goût, tout en se basant sur les expériences des clients précédents. Encore une fois, il s'agit d'un avantage qui se retrouve dans la réalité des cryptomarchés, mais qui est pratiquement inexistant dans les marchés de drogue du monde physique. Ce système de rétroaction portant sur les vendeurs et leur marchandise encourage les fournisseurs à proposer des produits de meilleure qualité (Aldridge et al., 2018). Pour être compétitifs et garder leur part de marché, les vendeurs doivent s'assurer de satisfaire leurs clients (Barratt, 2015). Lorsqu'un client est insatisfait, il peut simplement, et facilement, accéder à plusieurs autres vendeurs potentiels, simplement en regardant dans la liste d'annonces présentées sur le marché (Aldridge et al., 2018). D'ailleurs, les membres des cryptomarchés semblent percevoir la qualité de la marchandise offerte sur ces plateformes comme étant supérieure à ce que l'on retrouve ailleurs (Bancroft et Reid, 2016; Evangelista et al., 2018; Martin et al., 2019a).

En 2019, une étude publiée par les chercheurs Martin, Munksgaard, Coomber, Demant et Barratt, visait à comprendre pourquoi certains vendeurs choisissaient de poursuivre leurs activités criminelles sur les plateformes du darknet. Cette recherche est basée sur des entrevues passées auprès de vendeurs actifs dans les cryptomarchés (N=13), entre les mois de mars 2017 et mars 2018. Selon les résultats de cette étude, les motivations des vendeurs actifs dans les cryptomarchés sont d'abord matérielles. Selon les auteurs, les participants sont conscients des risques et les prennent en considération lorsqu'ils font le choix de débuter leur carrière dans les cryptomarchés. En effet, l'anonymat et les outils technologiques en place procurent une certaine perception de risque limité et de sécurité accrue. Les risques perçus par les vendeurs proviennent du côté de la détection et des arrestations par les forces de l'ordre, ou encore des usagers malveillants et des compétiteurs qui peuvent s'en prendre à leur commerce. D'autre part, le potentiel de profit est attrayant. Les ventes ne se limitent pas qu'à la clientèle délimitée par la

proximité physique; les vendeurs peuvent faire affaire partout, même à l'international. Le potentiel de profit possible l'emporte donc largement sur les potentiels risques perçus. Les chercheurs ont établi une seconde source de motivation, soit la perception d'un sentiment de satisfaction relié à la liberté, au contrôle et à la transgression des règles grâce à la poursuite de ces activités; un phénomène également perçu chez les vendeurs hors ligne. Pour certains, faire partie d'une communauté distincte et en subversion notée contre la loi et le politique procure un sentiment d'excitation particulier. De plus, le fait de retirer profit de ces activités rend le tout plus émotif et intense (Martin et al., 2019b).

1. 4. 2 Aspect sécuritaire

L'un des avantages les plus importants de l'achat de drogues sur les cryptomarchés est la perception de sécurité qu'ont les usagers lorsqu'ils exécutent leurs transactions. Cette perception provient, d'abord, du caractère anonyme typique de l'environnement du darkweb. Plusieurs ont vu, dans les cryptomarchés, une opportunité d'innovation criminelle leur permettant d'échapper à la détection par les forces de l'ordre (Martin, 2014a). En effet, comme il le fut mentionné plus haut, les technologies en place (utilisation de cryptage des communications, technologie d'anonymat et utilisation des cryptomonnaies) sur ces sites permettent aux participants de camoufler leur identité et l'endroit d'où ils effectuent leurs transactions (Goullé et al., 2017; Martin, 2014a). Cela contribue donc fortement à diminuer la probabilité d'identification et de sanction des participants. La présence d'outils servant à la protection de leur anonymat procure une perception de protection aux usagers, contre les menaces posées par les forces de l'ordre ou les escrocs présents dans la communauté (Holt et al., 2015).

De plus, l'aspect de la violence, qui est caractéristique du trafic de drogue dans les rues, ne fait pas partie de la réalité du trafic de drogues dans les cryptomarchés (Aldridge et al., 2018; Aldridge et Décary-Hétu 2016; Evangelista et al., 2018; DiPiero, 2017; Martin, 2014a; Martin et al., 2019a). En effet, les transactions se font au niveau virtuel, et aucune rencontre en physique entre les acteurs n'est nécessaire. Cela anéantit les risques de confrontation violente, de vol ou de piège lors de la réalisation des transactions (DiPiero, 2017).

L'aspect virtuel, jumelé avec l'anonymat, réduit aussi grandement les risques de violence provenant de la compétition territoriale, des tentatives de règlements de compte entre clans rivaux, etc. (Martin, 2014a). Cette perception de sécurité procure également un sentiment de contrôle relatif chez les membres et les vendeurs, qui n'est pas présent dans le monde physique pour la majorité (Bancroft et Reid, 2016; Evangelista et al., 2018; Martin et al., 2019a).

Finalement, la plupart des cryptomarchés proposent des mécanismes pacifiques de résolution de conflits. Les risques de pertes, de vols ou de fraudes sont donc régulés et sont nettement réduits par l'entremise de ces systèmes. L'implication d'une troisième partie lors des conflits rend leur résolution plus pacifique et ordonnée, et diminue les menaces de violence et de vengeance (Morselli, Décary-Hétu, Paquet Clouston et Aldridge, 2017). Ces systèmes, tel que le système d'entiercement, par exemple, permet une protection supplémentaire pour les usagers contre les fraudes, la mauvaise marchandise ou les vols (Aldridge et al., 2018). De tels arrangements sont pratiquement inexistants dans la réalité physique du trafic de drogue.

1. 4. 3 Les limites des cryptomarchés

Il existe cependant certaines limites aux cryptomarchés. D'abord, les cryptomarchés présentent une limite naturelle quant à leur potentiel de croissance. Afin d'exécuter des transactions sur le darkweb, il faut avoir accès au matériel informatique nécessaire et nécessite l'installation de certaines technologies. Or, ce ne sont pas tous les consommateurs de drogues qui sont en mesure d'acquérir de tels appareils et qui possèdent les capacités de s'en servir adéquatement (Bancroft, 2017). Une bonne proportion des consommateurs de drogue maintient donc leurs activités au niveau du commerce dans la rue (Martin et al., 2019a). Par conséquent, il existe un niveau de saturation de la clientèle, favorisant ceux qui sont d'un certain niveau socioéconomique et qui possèdent un minimum de connaissances et de capacités informatiques.

Malgré l'intuitivité des interfaces des marchés, ainsi que de la facilité avec laquelle les participants peuvent trouver les différents sites, une participation active et sécuritaire dans cet univers demande un certain niveau de compétences techniques, ne serait-ce que pour obtenir et gérer de manière sécuritaire la cryptomonnaie (Barratt et al., 2014). Une fois dans l'écosystème,

un des défis est de trouver les informations actuelles et pertinentes, notamment en ce qui concerne les différents sites actifs et jugés sécuritaires, ainsi que les mesures de protection opérationnelle à prendre. Ces renseignements ne sont pas toujours faciles à trouver, et les usagers doivent faire leur part de recherches pour maitriser l'environnement et les différents outils. Face à l'évolution et aux innovations constantes de l'écosystème, une inégalité se crée alors entre les membres qui ont déjà accès à aux connaissances et ressources requises, et ceux qui n'ont pas encore mis la main dessus et qui sont toujours en apprentissage (Bancroft, 2017). Finalement, sans bonnes capacités technologiques, et sans protection adéquate, les participants courent plusieurs risques et peuvent facilement devenir une cible facile pour les individus malhonnêtes présents dans écosystème (Evangelista et al., 2018).

1. 4. 4 Les risques internes

Malgré le fait que les cryptomarchés représentent un environnement dans lequel le trafic de drogue se veut plus facile et sécuritaire, il persiste encore des risques importants reliés à cette activité. Il existe de nombreux risques provenant de l'intérieur même de l'écosystème, et qui peuvent affecter, voire anéantir les activités des usagers qui en seraient victimes. D'abord, les usagers sont en quelque sorte, une proie au maintien des marchés. Lorsqu'un marché ferme, il y a un risque pour les vendeurs de perdre leur réputation, leur clientèle et les relations de confiance qu'ils ont créées. Il n'est pas évident de trouver un vendeur fiable, qui offre des substances jugées de bonne qualité, et les usagers comptent beaucoup sur cette stabilité pour préserver leurs activités. Il y a également les risques d'exit scam, soit lorsqu'un marché ferme sans avertissement, et que les administrateurs disparaissent avec la totalité de l'argent qui était dans les portefeuilles des utilisateurs ou dans le système d'entiercement du marché. Cela cause des pertes monétaires parfois considérables pour les usagers affectés (Zambiasi, 2020).

L'absence de règlementation externe et l'asymétrie de l'information entre les usagers peuvent mener à des risques de vol, de fraude et de tromperie. Comme nous l'avons vu plus haut, il n'existe pas de normes institutionnalisées qui protègent chaque partie d'une transaction. Les possibilités de fausses publicités, d'escroqueries, ou de vol (Holt et al., 2015) sont donc élevées. À partir du moment où ils débutent une transaction, les usagers demeurent dans l'incertitude, une

réalité qui est présente dans tous les niveaux du processus de distribution. Suite au paiement de l'achat, le client n'est pas assuré de recevoir ce qu'il pense recevoir, ni ce qu'on lui a dit qu'il recevrait (asymétrie d'information). Le vendeur a donc un avantage sur le client qui, lui, doit s'en remettre à sa parole, et est à risque de payer un prix plus élevé pour un produit de faible qualité, ou pour un produit qui ne sera jamais envoyé (Evangelista et al., 2018). S'il y a insatisfaction par rapport aux produits ou au service, les usagers ne peuvent pas s'en remettre au patron ou à la loi; ils doivent faire confiance au système en place et à son efficacité (Martin, 2014a). De tels événements peuvent causer des pertes et des risques pour la vie du consommateur; chose qui, somme toute, n'est pas étrangère au monde du trafic de stupéfiants dans la réalité physique (Moore, 1990).

Finalement, l'achat de drogue sur les cryptomarchés comporte également des risques d'entrer en contact avec des liens d'hameçonnage et des logiciels malveillants. Il est difficile, dans le darkweb, d'évaluer la fiabilité des liens (Evangelista et al., 2018). Malgré l'existence de sites répertoriant les liens validés, les sites changent régulièrement d'URL et utilisent des liens miroirs pour échapper à la détection de leur localisation réelle. Certains usagers malveillants se servent donc de cette réalité pour créer des liens trompeurs, et profiter de la naïveté de leurs victimes.

1. 4. 5 Les risques externes

Les risques externes à l'écosystème sont principalement associés à la compromission de l'anonymat en ligne, ce qui révèlerait l'identité des délinquants aux forces de l'ordre et pourrait éventuellement mener à leur arrestation (Martin, 2014a). Les chocs externes les plus fréquents proviennent des opérations policières, qui se concluent souvent par la fermeture d'une plateforme ou d'un marché et par des arrestations. Cela peut occasionner des pertes significatives pour les participants qui possédaient de l'argent en transaction sur le site, ainsi que pour les vendeurs établis qui risquent de perdre leur clientèle et leur réputation, acquises grâce à l'investissement de nombreux efforts, de ressources et de temps (Zambiasi, 2020). Malgré les efforts et les mesures prises pour camoufler leur identité, l'anonymat des usagers n'est pas absolu, et les forces de l'ordre ont les ressources nécessaires pour parvenir à identifier certains

membres (Martin, 2014a). L'identification des membres représente l'un des risques les plus importants pour les usagers des cryptomarchés, car chaque transaction et chaque conversation laissent une trace dans les cryptomarchés. Suite à l'arrestation ou à l'identification d'un usager, les membres ayant fait affaire avec lui courent donc tous des risques d'identification, ainsi que d'autres conséquences légales.

1. 5 Les techniques d'opérations policières dans le cyberespace

La perception des participants selon laquelle les risques entourant leurs activités illicites, au sein des cryptomarchés, sont moins présents est réelle; en effet, les forces de l'ordre ont bien plus de difficulté à détecter et identifier les participants des transactions réalisées dans les cryptomarchés que ceux ayant lieu au niveau de la rue. Le caractère de l'anonymat omniprésent dans l'écosystème, l'utilisation de la cryptomonnaie difficilement retraçable, et la faible nécessité de déplacement lors de la réalisation des transactions sont tous des éléments qui rendent le travail des policiers nettement plus compliqué (Martin, 2014b). De plus, les cryptomarchés forment un environnement hautement instable, constamment en changement et innovant vers de nouvelles technologies qui visent l'augmentation de la sécurité de ses membres (Martin, 2014a). Il est donc ardu pour les agences d'application de la loi de cibler quels sont les joueurs majeurs, et de savoir comment attribuer judicieusement les ressources nécessaires pour maximiser l'efficacité de leurs opérations. Les forces de l'ordre ont recours sensiblement aux mêmes tactiques que celles utilisées lors d'interventions dans le monde physique, qu'ils prennent cependant soin d'adapter au cyberespace (Décary-Hétu et Giommoni, 2017). Ces interventions visent à perturber l'écosystème des cryptomarchés le plus possible; ils optent généralement pour des frappes de forte intensité, hautes en visibilité, et médiatiquement rapportées. Le type d'opérations utilisées pour atteindre l'univers du darkweb fait partie de la catégorie des opérations réactives, décrites plus haut : opérations d'infiltration, opération de type « crackdown », saisies et arrestations de masse, etc. Dans les dernières années, les états ont identifié les cryptomarchés comme cible principale et ont augmenté leurs efforts visant à combattre leur fréquence d'utilisation grandissante chez les consommateurs de drogues (Gupta et al., 2018; Leontiadis et Hutchings, 2015; Martin, 2014a).

Plusieurs techniques peuvent être efficaces pour ébranler et perturber les activités des cryptomarchés. D'abord, les forces de l'ordre ont recours à des techniques d'intervention spécialisées dans le cyberespace. Grâce à l'utilisation de la criminalistique digitale, et à l'utilisation d'agents d'infiltration au sein des structures organisationnelles des plateformes web, ils ont réussi à cumuler des informations qui peuvent servir d'évidences contre les participants et les administrateurs des différents cryptomarchés (Martin, 2014a). Les agences d'application de la loi ont également recours à des manoeuvres qui ciblent la structure technologique sur laquelle repose la communauté des cryptomarchés, tels que le navigateur TOR ou la cryptomonnaie. Ils y parviennent, entre autres, grâce à l'identification et l'exploitation de leurs faiblesses, afin de les rendre inutilisables et instables. Cependant, cette option est de moins en moins intéressante, car il y a une hausse dans la fréquence de l'utilisation de ces technologies par des usagers légitimes et non criminels. L'altération de ces outils causerait donc du tort à des compagnies financières légitimes, ou de simples particuliers qui utilisent les cryptomonnaies légalement, et qui n'ont rien à voir avec quelconque entreprise illégale (Martin, 2014a).

D'autres techniques peuvent être utilisées, comme la désanonymisation des serveurs des cryptomarchés, suivi de l'identification et de la poursuite de leurs administrateurs. Alors que les cryptomarchés sont construits sur une formule décentralisée et distribuée, leur contenu est toujours bâti et servi sur un modèle traditionnel client-serveur. Cela signifie donc que le serveur est le point central à atteindre, et explique pourquoi les interventions ciblent ces derniers afin de se concentrer vers les administrateurs (Gupta et al., 2018).

Le recours aux attaques DDOS (déni de service distribué) est également une stratégie utilisée par les forces de l'ordre. Ce type d'attaque surcharge les serveurs d'un site, le rendant temporairement inopérable. Cette méthode a pour but de compliquer et ébranler l'écosystème, afin d'en décourager l'utilisation. Cette méthode peut également aider à compléter les efforts de désanonymisation en forçant les utilisateurs à se connecter aux liens de relais offerts, qui sont en réalité des liens contrôlés par les attaquants (Gupta et al., 2018).

Finalement, les forces policières ont également recours à des techniques d'opérations plus conventionnelles, qui visent à réduire directement le trafic de drogue. D'abord, cela peut se faire en effectuant le tri de la poste, afin de déceler et d'intercepter les colis pouvant présenter un contenu illicite. L'interception des colis, la perte de la marchandise et l'échec de la transaction, ainsi que les risques d'identification des deux parties sont les buts visés par cette méthode (Martin, 2014a). Les opérations policières d'envergure, telles que les frappes, les arrestations, les saisies et les fermetures des cryptomarchés, sont les interventions perturbatrices les plus utilisées par les forces de l'ordre, si bien qu'elles sont devenues une réalité constante et normale en arrière-plan du quotidien des participants aux cryptomarchés (Martin et al., 2019b). De nombreuses opérations majeures de cet ordre ont d'ailleurs eu lieu dans les dernières années et, malgré leur coût élevé en temps, en ressources et en argent, n'ont offert que des résultats mitigés.

1. 5. 1 La fermeture de Silk Road

Mis en ligne en 2011, Silk Road est reconnu comme étant le premier marché du darkweb dédié à la vente de produits illicites. Son créateur et administrateur, Dread Pirate Robert, a profité de la conjoncture de plusieurs éléments – la présence de technologies d'anonymisation, la création d'une monnaie électronique désinstitutionnalisée et un système de transaction à trois parties – pour mettre sur pied et faire fonctionner un tel site (Martin, 2014b). Malgré l'apparition de nombreuses plateformes semblables, le cryptomarché Silk Road maintint le monopole des activités de ventes illicites dans le darkweb. Cette plateforme est rapidement devenue un incontournable dans le monde de la cybercriminalité, ce qui explique pourquoi les différentes agences d'application de la loi s'y sont intéressées. Le FBI a mené, durant plus de deux ans, une opération visant à infiltrer le cercle d'administration du site. En octobre 2013, des agents du FBI procédaient à l'arrestation de son fondateur, saisissant au passage des dizaines de millions de dollars en cryptomonnaie (Lacson et Jones, 2016). Le but principal du FBI était de donner, aux participants, la perception que l'écosystème des cryptomarchés n'est pas inébranlable et que sa structure peut être atteinte (Martin, 2014a). Cependant, la réaction suivant la fermeture de Silk Road et l'arrestation de son populaire créateur ne fut pas celle attendue. Au lieu de l'effet dissuasif espéré, cette intervention sembla créer, dans la communauté, un désir de rebondir. Dans les semaines et les mois suivants, les observateurs furent témoins d'une décentralisation des

marchés; plusieurs cryptomarchés se sont créé et ont remplacé l'espace béant laissé par le départ de Silk Road (Martin, 2014a; van Buskirk et al., 2014).

1. 5. 2 L'Opération Onymous

Environ une année après la fermeture de Silk Road, le nombre de cryptomarchés actifs est monté en flèche (Barratt et al., 2016). Parmi eux se trouve Silk Road 2, une réplique du cryptomarché original. En novembre 2014, une opération internationale, réunissant plusieurs agences américaines et européennes est réalisée, dans le but, encore une fois, d'ébranler l'écosystème des cryptomarchés. Lors d'un effort conjoint réunissant plusieurs agences d'application de la loi, autant américaines qu'européennes, les forces de l'ordre sont parvenues à s'infiltrer dans plusieurs cryptomarchés actifs, et ont pu procéder à l'identification d'une quantité importante d'administrateurs avant de procéder à une série d'opérations crackdown et à la fermeture de plusieurs sites. Cette intervention s'est conclue avec la fermeture d'une douzaine de cryptomarchés, de multiples arrestations d'administrateurs et la saisie de plusieurs millions de dollars en biens criminels, drogues et cryptomonnaie (European Monitoring Centre for Drugs and Drug Addiction [EMCDDA], 2016). Tout comme lors de l'opération menant à la fermeture de la plateforme Silk Road, en 2011, cette opération visait à ébranler la confiance des usagers envers la structure de l'écosystème, et tentait également de précipiter la suppression d'une portion importante des cryptomarchés. Cependant, les résultats furent différents de ceux attendus. Il fut possible, suite à l'intervention des forces de l'ordre, d'observer qu'une majorité des usagers ont déplacé leurs activités vers d'autres sites intouchés, et ont ainsi pu maintenir le niveau de leurs activités (EMCDDA, 2016).

1. 5. 3 L'Opération Bayonet

En 2017, le site Alphabay dominait la scène des cryptomarchés, et attirait l'attention des forces de l'ordre. Ces dernières sont parvenues à identifier l'administrateur principal de la plateforme et à l'arrêter. Ils ont également fermé le marché et ont saisi les serveurs du site web (Afilipoaie et Shortis, 2018). Ayant remarqué, suite aux opérations précédentes, que les membres des sites fermés déplaçaient leurs activités vers d'autres cryptomarchés, les forces de l'ordre ont

tendu un piège aux usagers d'Alphabay. Ils avaient, précédemment à l'intervention contre la plateforme, pris le contrôle d'un autre cryptomarché populaire, Hansa.

Comme espéré, une importante croissance du nombre de participants au sein de la plateforme Hansa fut enregistrée suite à la fermeture d'Alphabay (Europol, 2017). Près de 27 jours après avoir pris possession de la plateforme Hansa, les forces de l'ordre ont procédé à sa fermeture définitive. Ils ont profité de ce délai pour cumuler suffisamment d'informations leur permettant d'identifier et d'appréhender un grand nombre de participants, tout en récoltant des renseignements importants sur le comportement des usagers suite aux chocs externes causés par les interventions policières (Afilipoaie et Shortis, 2018).

Après la fermeture de ces deux cryptomarchés, les forces de l'ordre n'ont pas observé les effets dissuasifs attendus. Comme il est coutume, suite à la fermeture des plateformes, ils se sont assuré de rendre publique leur réussite, notamment en médiatisant les stratégies utilisées. Les participants ont pris conscience des lacunes présentes dans leur écosystème, et ont décidé d'améliorer leurs technologies de sécurité opérationnelle. Les participants des cryptomarchés ont cette capacité de s'adapter, dans le but de rendre le travail plus difficile pour les forces de l'ordre, devant l'éventualité d'une prochaine intervention semblable (Martin, 2014a).

1. 6 Les impacts réels des interventions policières

Les études qui se sont concentrées sur les impacts qu'ont eus les opérations policières sur les cryptomarchés présentent des résultats semblables à ceux relevés dans les études traitant des opérations qui ont eu lieu dans l'espace physique. Outre la haute visibilité des opérations et l'intensité des frappes produites, nous pu avons constater, à la lumière des sections précédentes, que les buts visés lors de ces interventions résident dans l'augmentation de la perception des risques des participants aux marchés illicites, ainsi que dans l'ébranlement de leur confiance envers les réseaux auxquels ils appartiennent. Bref, les opérations orchestrées dans l'univers du darkweb ne sont, au final, que des opérations traditionnelles, adaptées à l'univers du cyberespace

(Buxton et Bingham, 2015). Il n'est donc pas étonnant de voir que les conclusions des interventions dans le darkweb sont semblables à celles prenant lieu dans les marchés physiques.

1. 6. 1 Des effets limités et temporaires

Plusieurs études se sont intéressées aux impacts des interventions policières sur les activités des cryptomarchés. Les résultats de ces études pointent vers les mêmes conclusions, soit que les effets de ces interventions sont limités et temporaires. En 2019, Ladegaard a étudié les contrecoups suivant la fermeture, par les forces de l'ordre, de la plateforme Silk Road. Grâce à 3300 commentaires tirés de trois forums différents, il a tenté de comprendre, à travers les réponses des participants, comment ces derniers ont été touchés par les actions policières contre leur écosystème. Selon les résultats de son étude, la tentative de perturbation des forces de l'ordre n'a pas réussi à causer de dommages permanents. Immédiatement suite à l'intervention policière, le nombre de marchés actifs a chuté considérablement, passant de 19 à 12 plateformes en fonction. Cependant, six mois plus tard, ce nombre est revenu au même niveau, pour être par la suite dépassé quelques mois après. Les impacts peuvent donc se faire ressentir rapidement suite à une intervention, mais un retour à la normale est généralement observé dans un court délai (Bhaskar, et al., 2019; Ladegaard, 2019; Soska et Christin, 2015). Cette tendance est également remarquée au niveau du nombre de participants actifs dans les cryptomarchés suite aux interventions policières; d'abord, une chute considérable du nombre de membres actifs est observée suite à la fermeture d'une plateforme, mais le niveau de fréquentation de ces sites web revient rapidement à celui existant avant l'intervention (Norbutas et al., 2020; van Buskirk et al., 2017).

Il est donc possible d'admettre que les participants maintiennent leurs activités au sein des cryptomarchés, et ce, malgré les tentatives de perturbation répétées de la part des forces de l'ordre. Les effets temporaires et limités ne semblent également n'avoir aucun impact sur les prix moyens des marchandises offertes dans les marchés et sur la capacité des participants à maintenir à niveau leur commerce. Ils ne semblent pas être suffisants, non plus, pour faire augmenter le niveau de perception des risques chez les participants (Munksgaard, Bakken et Demant, 2017). Toujours en se concentrant sur les impacts directement liés aux activités des marchés, d'autres

chercheurs se sont concentrés sur les impacts économiques des interventions. C'est d'ailleurs le cas de Décary-Hétu et Giommini qui, en 2017, ont cherché à décrire et expliquer les impacts qu'ont les opérations policières sur les cryptomarchés affectés. À l'aide d'une banque de données composée de 226 297 annonces uniques provenant des marchés, et de 7280 vendeurs uniques actifs dans l'écosystème, ils ont étudié les contrecoups de l'opération Onymous. Les résultats de cette étude sont sans équivoque et sont partagés par d'autres auteurs (Hull, 2017; Miller, 2019); les répercussions sur les prix, la demande et la capacité d'approvisionnement des cryptomarchés sont mineures et de courte durée.

L'étude menée par Décary-Hétu et Giommoni (2017) permet également de comprendre que l'implication des participants dans les cryptomarchés n'est guère affectée par les perturbations causées par les chocs externes. Dans les mois suivant l'intervention policière, ils ont été en mesure de retrouver et d'identifier 75% des vendeurs qui étaient actifs avant l'opération Onymous. Les auteurs estiment que les autres vendeurs peuvent avoir décidé de quitter les marchés, ou encore que ces derniers aient choisi de changer leur nom d'usager, afin de retrouver leur anonymat. Van Buskirk et al. (2017), pour leur part, dénotent une hausse du nombre de vendeurs actifs suite à l'opération Onymous. Bhaskar et al. (2019), pour leur part, remarquent l'absence d'effet dissuasif suite à la réalisation de ces interventions, notant même une hausse du nombre de cryptomarchés actifs, malgré la fermeture de Silk Road et l'opération Onymous. Bref, l'ensemble de ces études semble pointer vers le même résultat, soit que les interventions policières ne réussissent pas, à long terme, à ralentir les activités des cryptomarchés, et ne parviennent pas à décourager les participants dans la continuation de leur implication dans cet écosystème.

La confiance des membres ne semble également pas être ébranlée à long terme par les interventions policières. En se basant sur les discussions tirées de forums, à la suite de la fermeture de Silk Road, Lacson et Jones (2016) ont noté que les membres sont restés positifs et productifs, et étaient confiants que de nouveaux cryptomarchés surgiraient et combleraient le trou laissé par le départ de Silk Road; ce qui fut effectivement le cas. Ladegaard (2018) dénote également que la plupart des usagers disent toujours faire confiance en l'écosystème et ses

membres, et attribuent l'arrestation des administrateurs à une erreur humaine de leur part, et non une défaillance dans la sécurité mise en place.

1. 6. 2 Le phénomène du déplacement

Malgré les effets limités et temporaires observés au sein de la communauté des cryptomarchés, suite aux interventions policières y ayant lieu, plus de résultats pertinents furent retenus par les chercheurs. Ces derniers ont été témoins de l'importante capacité d'adaptation des participants, notamment grâce aux déplacements spatiaux et tactiques entrepris par ces derniers.

Caulkins (1993) décrit le phénomène du déplacement comme l'adaptation des marchés illicites en réponse aux chocs et aux pressions provenant des opérations des forces de l'ordre. En effectuant leurs opérations, les forces policières tentent de retirer aux criminels les opportunités de commettre leurs actes. Au lieu de succomber à la pression et s'effondrer, ces marchés adaptent en conséquence leurs activités dans l'espace et le temps. Windle et Farrell (2012), pour décrire ce phénomène, proposent l'image du « balloon effect », un terme fréquemment utilisé pour parler de l'adaptation des réseaux de trafic de drogues. Selon le concept du « balloon effect », sous la pression des forces de l'ordre, il est possible d'observer un mouvement hydraulique de la part du réseau criminel. Les auteurs associent la grosseur du ballon à la taille du trafic, et le volume d'air dans le ballon au volume de la production des actes illicites. En appliquant une pression (ici, cette pression est représentée par la pression provenant des activités policières) sur un ballon, ce dernier bondira, se déplacera dans un espace à proximité, et reprendra sa forme originale. Le mouvement du ballon représente donc le mouvement d'adaptation (le déplacement), qu'effectuent les marchés criminels dans ces situations (Windle et Farrell, 2012). Comment expliquer cette réaction? Il est possible de tirer la réponse de la théorie de Cornish et Clarke, la théorie du choix rationnel (Ratcliffe et Breen, 2011). Selon cette théorie, le délinquant est un être rationnel, et sa décision de commettre un acte criminel résulte d'un processus de prise de décisions, qui tient en compte différents facteurs présents dans sa réalité (Cornish et Clarke, 1987). Un calcul rudimentaire entre le coût et les bénéfices est effectué par l'individu, dans lequel les buts, les expériences, les habiletés, les motifs et opportunités seront pris en considération (Cornish et Clarke, 1987). Le phénomène du déplacement suit donc cette

ligne de pensée : la réalité du criminel ayant été bousculée par un événement, ce dernier réévaluera la situation et reproduira son calcul coût-bénéfice. S'il considère qu'il n'est plus avantageux pour lui de commettre le même acte, au même endroit et de la même façon, il aura deux options : se désister, ou s'adapter. Il cherchera à déplacer ses activités dans une réalité qui lui sera davantage favorable, donc une réalité qui n'est guère influencée par le choc externe produit par l'intervention policière.

Il existe plusieurs types de déplacement (Hamilton-Smith, 2002; Windle et Farrell, 2012). D'abord, il y a le déplacement spatial, lorsqu'il y a commission du même acte, mais dans un quartier ou une ville autre. Il s'agit du déplacement le plus fréquemment étudié (Windle et Farrell, 2012). Ensuite, il y a le déplacement temporel, soit la réalisation de l'acte dans une période différente (Hamilton-Smith, 2002). Le déplacement tactique est défini par la commission d'un même acte, mais grâce à une méthode – modus operandi - différente. Cela peut simplement se produire par l'introduction de la technologie dans la commission de l'acte illicite, l'introduction du padget dans le trafic de drogue, par exemple, pour faciliter et protéger la communication entre l'acheter et le vendeur (May et Hough, 2001). Viennent ensuite le déplacement du type de crime (commission d'un acte criminel différent, mais fait par les mêmes acteurs), et le déplacement de la cible (changement de clientèle, par exemple) (Hamilton-Smith, 2002; Windle et Farrell, 2012). Un sixième type de déplacement mentionné par les études est le déplacement de délinquant (Windle et Farrell, 2012). Lorsqu'un délinquant se fait arrêter ou décide d'interrompre ses activités, son absence crée une opportunité intéressante pour les autres membres. Il est donc possible de voir un second individu saisir cette opportunité, et prendre la place du premier délinquant. Il est fréquent de voir une combinaison des différents types de déplacement se produire suite à une même intervention, mais il n'est pas dit qu'à toutes les interventions, il se produira un effet de déplacement (Hamilton-Smith, 2002).

Il est également important de mentionner que, bien qu'une opération policière puisse causer un déplacement de l'activité criminelle, elle peut également générer une diffusion des bénéfices, un phénomène qui est, en quelque sorte, le contraire du déplacement (Hamilton-Smith, 2002). Green (1995) définit la diffusion des bénéfices comme l'effet positif d'une opération policière ou de mesures de prévention, car les opportunités criminelles sont réduites, non

seulement pour la cible initiale, mais également pour des cibles non attendues. Il s'agit d'un effet directement lié à l'augmentation des risques d'arrestation, perçus par les délinquants. La diffusion des bénéfices se produit, par exemple, lorsqu'une opération vise un certain quartier, mais que les effets dissuasifs se font sentir dans une autre section de la ville, sur d'autres délinquants ou sur d'autres formes de crime que ce qui est initialement visé. Tout comme les déplacements, il existe plusieurs formes de diffusion des bénéfices; spatiale et temporelle, d'abord, toutes deux liées aux déplacements du même nom. Un déplacement spatial d'une zone à une autre créera une augmentation des activités dans un quartier, alors qu'il pourrait résulter en une diminution des activités dans un autre (Windle et Farrell, 2012).

Suite à la fermeture d'un cryptomarché, les auteurs ont remarqué qu'une partie importante des vendeurs déplacent leurs activités vers le prochain marché actif (Afilipoaie et Shortis, 2015; Barratt et al., 2016; Miller, 2019; van Buskirk et al., 2017). C'est d'ailleurs ce qu'ont pu observer van Wegberg et Verburgh, (2018), en réponse à l'opération Bayonet, survenue en 2017 et qui a mené à la fermeture de deux importants marchés. En se servant du site Gram, qui sert d'outil de registre d'annonces et de vendeurs, et en répertoriant les clés PGP individuelles, ils ont pu suivre les mouvements des vendeurs actifs dans l'un des marchés récemment fermés. En effet, une quantité importante des membres ont migré vers un marché alternatif, DreamMarket. Les deux tiers des vendeurs n'ont pas pris de mesures évasives lors de la migration, alors que seulement 20% ont changé leur clé PGP, et que 8% ont modifié leur pseudonyme. La majorité des membres ont donc simplement déplacé leurs activités, sans apporter quelque modification qui soit. Il fut également observé que les membres ayant une meilleure réputation et une plus d'ancienneté étaient davantage sujets à se déplacer vers d'autres marchés, tout en maintenant une grande partie de leurs activités intactes (Ladegaard, 2019; Norbutas et al., 2020).

1. 6. 3 Des capacités d'innovation

Mis à part la capacité de déplacement spatial des usagers, les chercheurs ont été témoins des nombreux déplacements tactiques, sous forme d'adaptations et d'innovations entreprises par les participants pour permettre la poursuite des activités sur les cryptomarchés. Certains auront, par exemple, été contraints de changer leurs habitudes commerciales, entre autres en offrant des rabais à leurs clients pour les inciter à les suivre dans d'autres marchés (Childs, Coomber, Bull et Barratt, 2020), alors que d'autres ont émis l'idée de changer leurs habitudes d'achat (Barratt et al., 2016). Les études rapportent également un mouvement de centralisation des participants; suite à la fermeture de plusieurs marchés, les clients ont concentré leurs transactions vers un nombre plus réduit de vendeurs, présents à travers plusieurs plateformes (Décary-Hétu et Giommini, 2017; Norbutas et al., 2020). Plusieurs usagers se sont également tournés vers la pratique du « direct dealing », soit l'utilisation d'emails ou de chats cryptés pour effectuer les achats directement avec les fournisseurs, sans passer par les marchés (Barratt et al., 2016). Cette alternative leur permet ainsi d'éviter la pression exercée par les interventions des forces de l'ordre, tout en palliant au manque de stabilité dans l'écosystème des cryptomarchés (Barratt et al., 2016; Childs et al., 2020). Cependant, le « direct dealing » nécessite un contexte de confiance solide préétabli entre les participants, car cela expose grandement les membres impliqués dans ces transactions au risque d'escroquerie, et retire toute possibilité d'intervention d'une tierce partie régulatrice (Childs et al., 2020). Les participants des cryptomarchés démontrent, de plus, la capacité d'améliorer et d'innover l'infrastructure, tel qu'ils l'ont prouvé à la suite de plusieurs interventions policières. Après la fermeture de Silk Road, la communauté s'est rassemblée et a mis sur pied un projet d'amélioration du système en place et s'est organisée pour combler les faiblesses rendues évidentes par l'intervention. Ils ont donc procédé à la création d'un Silk Road 2.0 en se basant sur les éléments sauvegardés de la plateforme originale ainsi que de son forum et, grâce à la collection des clés d'identification des membres qui étaient actifs sur la première plateforme, ils furent en mesure d'authentifier les participants qui désiraient transférer leur profil vers la nouvelle version de la plateforme. Ils ont également créé des forums indépendants aux marchés, les distanciant des potentiels chocs futurs et protégeant ainsi le capital illicite qui s'y retrouve (Ladegaard, 2019). Finalement, un des aspects les plus remarqués par les chercheurs fut les innovations effectuées au niveau des technologies de protection. Les chocs causés par les

interventions ont poussé les participants à devenir plus conscients et réalistes des limites et des faiblesses technologiques existant dans leur écosystème, et ils se sont outillés de nouvelles de technologies plus efficaces pour y faire face (Childs et al., 2016; Horton-Eddison et Di Cristofaro, 2017; Munksgaard et al., 2017). Plusieurs membres ont donc préféré adopter des mesures de prévention et de sécurité opérationnelle plus élevée, afin de contrer ou de diminuer les risques engendrés par les chocs externes et internes subséquents aux interventions policières (Barratt et al., 2016; Soska et Christin, 2015).

1. 6. 4 Les effets pervers des interventions policières à l'endroit des cryptomarchés

Bref, les interventions policières orchestrées à l'endroit des cryptomarchés produisent des résultats limités et temporaires, alors que les participants démontrent des capacités d'adaptation et d'innovation qui leur permettent de contrer les difficultés et les obstacles qui surgissent. Plusieurs chercheurs craignent que la pression exercée par les forces de l'ordre à l'endroit de cette communauté risque de créer des effets pervers, soit en incitant les membres à prendre des mesures supplémentaires pour fortifier l'infrastructure contre les attaques externes (Martin, 2014a), en les encourageant à investir et innover dans les outils technologiques (Gupta et al., 2018; Hutchings et Holt, 2017; Lorenzo-Dus et Di Cristofaro, 2018) et en les poussant à recourir à des structures plus sécuritaires et solides pour poursuivre leurs activités (Afilipoaie et Shortis, 2018).

La fermeture d'un marché résulte normalement en un mouvement de déplacement de ses participants vers d'autres marchés ou d'autres vendeurs disponibles (Afilipoaie et Shortis, 2015; Barratt et al., 2016; Miller, 2019; van Buskirk et al., 2017). Cette mobilisation des participants rend la tâche plus difficile pour les forces de l'ordre qui tentent de contenir et ralentir les activités produites au niveau des cryptomarchés. Suite à la fermeture du cryptomarché Silk Road, qui détenait le monopole des activités de vente de produits illicites dans le darknet, une multitude de nouveaux marchés ont émergé et ont pris place dans l'écosystème. Cela a eu comme conséquence de décentraliser les activités des participants à travers un pus grand nombre de marchés et de multiplier les cibles d'interventions pour les agences d'application de la loi (Martin, 2014a). La décentralisation des marchés cause également une décentralisation des

systèmes de communication, ce qui a pour effet de rendre plus difficile leur réglementation par les forces de l'ordre, et contribue donc à la libre publication de contenu non éthique et illégal (Gupta et al., 2018).

Cette compétition nouvelle dans l'écosystème a eu comme conséquence d'augmenter les risques internes d'attaques entre les différents participants et marchés, chacun tentant d'accéder au niveau supérieur dans l'écosystème. Cette instabilité, jumelée aux nombreux mouvements dans l'écosystème, raccourcit la durée de vie des marchés. Ce phénomène crée donc de nouveaux enjeux pour les agences d'application de la loi. Les nombreux cryptomarchés éphémères compliquent l'allocation des ressources lors de la planification d'interventions : les agences d'application de la loi risquent de prendre une plateforme pour cible, et de la voir disparaître avant la fin de l'opération (Martin, 2014a). La perte de temps et de ressources orientés vers des plateformes qui disparaissent, ou encore vers des plateformes d'importance moindre, diminue l'efficacité des frappes policières contre l'écosystème. Les organismes d'application de la loi ont contribué à créer cet environnement instable, et ont participé à compliquer le travail de leurs enquêteurs, qui ont besoin d'un minimum de temps pour parvenir à compléter leurs enquêtes (Martin, 2014a).

Les participants des cryptomarchés apprennent des erreurs de leurs prédécesseurs : ils détectent les failles présentes dans leur environnement et comprennent les faiblesses utilisées par les forces de l'ordre pour les atteindre. Ils sont également actifs à remédier aux éléments jugés menaçants envers leur liberté et envers la continuité de leurs activités dans l'univers des cryptomarchés. Ainsi, suite à la fermeture du cryptomarché Silk Road, les administrateurs ont reçu l'aide de membres de la communauté et de spécialistes pour rendre plus difficiles le décryptage des communications et l'atteinte des serveurs par des acteurs externes (Martin, 2014a). L'augmentation de la sécurité personnelle des participants rend également plus complexe le travail des forces de l'ordre. La médiatisation des tactiques et des techniques d'enquêtes et des stratégies utilisées pour parvenir aux arrestations importantes a comme conséquence de permettre aux administrateurs d'augmenter leur vigilance envers les failles connues du système, ainsi qu'envers les participants potentiellement suspects qui pourraient tenter de pénétrer le noyau des marchés (Martin, 2014a).

Pour prévenir la saisie des serveurs des plateformes par les forces policières, les membres des cryptomarchés ont encore une fois innové, et ont créé un marché sans serveur central, du nom de Open Bazaar (Gupta et al., 2018). Open Bazaar n'est qu'un exemple appuyant l'hypothèse que la pression exercée par les forces de l'ordre (Lorenzo-Dus et Di Cristofaro, 2018), ainsi que l'amélioration de leurs capacités d'intervention dans le darkweb (Gupta et al., 2018) entraînent une augmentation des investissements technologiques et des progrès dans la sécurité et les technologies d'anonymat dans l'écosystème, causant d'importants obstacles aux réussites policières contre la communauté.

1. 6. 5 Opérations policières dans le cyberespace : Efficacité limitée et besoin d'innover

À la lumière des résultats provenant des différentes études, plusieurs auteurs considèrent que les méthodes de perturbations traditionnellement utilisées contre l'écosystème des cryptomarchés sont obsolètes, et appellent les forces de l'ordre à se tourner vers des solutions d'interventions innovatrices (DiPiero, 2017; Hutchings et Holt, 2017; Lane, Salmon, Cherney, Lacey et Stanton, 2019; van Hardeveld et al., 2017). Les opérations d'envergure, qui demandent du temps et de nombreuses ressources, n'ont pas conduit à des résultats importants et permanents, et ont même poussé les usagers à s'adapter et améliorer leur protection individuelle (Martin, 2014a). Pour parvenir à des résultats significatifs, il faut que les forces de l'ordre révisent et réorientent leurs techniques d'intervention dans le cyberespace, afin de suivre le mouvement d'innovation qu'empruntent les participants des marchés virtuels (DiPiero, 2017).

Plusieurs chercheurs qui ont étudié les impacts de l'une des multiples interventions passées contre les cryptomarchés ont émis des recommandations dans le but de diriger les pratiques vers des options plus efficaces. D'abord, Martin (2014a) suggère d'utiliser le partage de capital illicite et de l'intelligence accumulée à même l'écosystème. Le partage des connaissances est une pratique courante et importante dans les cryptomarchés. Les informations qui y sont produites sont gratuites et publiquement accessibles. Les profils des vendeurs, par exemple, permettent l'accès à des informations complètes qui énoncent la nature du produit

vendu, les quantités proposées, les prix offerts, le lieu d'origine de la livraison, mais également les mesures de sécurité opérationnelle utilisée lors de la transaction et de la livraison. Les plateformes tel que Kilo et Reckon, qui tiennent les registres des profils de vendeurs actifs, de leur différents alias, de leur clé PGP, et de l'ensemble des annonces et conditions de transactions peuvent s'avérer de véritables mines d'or. Dans les espaces de partage, comme les forums, les membres discutent des risques émergents et des tactiques visant à les déjouer. Également, y sont présentés de nombreux guides et tutoriels sur les différentes mesures et techniques permettant une meilleure protection. Ces sources permettent ainsi un aperçu presque complet des techniques utilisées par les participants des cryptomarchés. Ce sont là des informations facilement accessibles et détaillées, et qui seraient grandement utiles aux forces policières lors de leurs futures interventions (Martin, 2014a).

D'autres suggèrent une meilleure allocation des ressources, proposant de cibler d'abord les acteurs des marchés plutôt que les marchés en soi (Broséus et al., 2016; DiPiero, 2017). Comme il devient de plus en plus difficile de concentrer les ressources policières vers la fermeture des cryptomarchés, en partie en raison des innovations technologiques et des mesures d'adaptation prises par les membres, il serait judicieux d'orienter les initiatives ailleurs dans le processus, en ciblant, par exemple, les participants aux cryptomarchés ou encore les outils facilitateurs à la réalisation des activités des marchés (Gupta et al., 2018). En plus de générer de nombreux coûts en temps et en ressources, l'atteinte des cibles habituelles génère des résultats modérés qui ne semblent pas créer de perturbations importantes dans les activités régulières de la communauté. Certains auteurs proposent donc d'utiliser des données provenant des interventions passées, et de concentrer les efforts sur les aspects susceptibles de perturber davantage l'économie et le trafic à travers les marchés (Broséus et al., 2016; DiPiero, 2017).

Finalement, Martin (2014a) suggère d'utiliser des agents d'infiltration à l'intérieur des marchés, et de saisir des colis au sein des services postaux. Face au mouvement de décentralisation remarqué dans l'écosystème, les nouveaux acteurs font leur entrée en grand nombre, ce qui, ultimement, rend les tentatives de localisation des serveurs des plateformes et de leurs administrateurs inutiles. Une solution face à ce phénomène est d'accroître le nombre d'opérations d'infiltration, et de travailler conjointement avec différentes agences, afin

d'identifier les acteurs influents et à la source du trafic (DiPiero, 2017). Pour y parvenir, la création de comptes dans les marchés est suggérée; il serait alors possible de laisser des commentaires aux vendeurs et d'effectuer des transactions avec eux, pour ensuite établir un lien de confiance avec ces derniers. Les forces de l'ordre pourraient ainsi tenter de suivre le versement de cryptomonnaie envoyé lors d'une transaction, ou encore, pourraient tenter de retracer un paquet envoyé via les services postaux (DiPiero, 2017). Les instances douanières et les services postaux peuvent d'ailleurs jouer un rôle important dans la réussite des tentatives de perturbation des activités des cryptomarchés. Il s'agit de la première ligne de défense interne pour les états, qui peuvent intercepter les colis à l'entrée des frontières et pourraient potentiellement en retracer l'origine (Martin, 2014a).

Chapitre 2 : La problématique

La place occupée par les cryptomarchés dans le portrait du trafic de drogues est de plus en plus importante, et c'est la raison pour laquelle de nombreux chercheurs présentent un intérêt grandissant pour ce phénomène. En effet, malgré un rôle modéré dans le marché mondial de vente de drogue (Europol 2017), ces plateformes présentent des profits en constante croissance depuis les dernières années (Martin et al., 2019a). Suite à une baisse légère en 2018, l'activité économique des cryptomarchés a fait un bond de 70% en 2019, pour atteindre un chiffre de plus de 790M$ en cryptomonnaie (Chainalysis, 2020). Selon la plateforme Chainalysis (2020), ces hausses de revenus sont causées par une augmentation du nombre de transactions effectuées dans l'écosystème des cryptomarchés. Alors que le montant moyen des transactions complétées est stable, le nombre de transactions effectuées à partir de ces plateformes est passé de 9 millions, en 2018, à 12 millions en 2019. Ces chiffres suggèrent donc une importante vague de nouveaux usagers sur ces plateformes, ou encore le retour en activité d'anciens membres récemment inactifs. Cette popularité grandissante s'explique, entre autres, par deux aspects principaux, qui sont spécifiques au commerce de drogue en ligne. D'abord, les cryptomarchés offrent la possibilité d'effectuer des transactions de manières particulièrement simple, proposent une large variété de substances de qualité, le tout au coût d'un faible effort (Aldridge et al., 2018; Barratt, 2015; Bancroft et Reid, 2016; Evangelista et al., 2018; Martin et al., 2019b). De plus, les risques inhérents perçus suite à cette activité illicite sont moindres lorsqu'elle est effectuée via les cryptomarchés; les participants perçoivent moins de risques de violence (Aldridge et al., 2018; Aldridge et Décary-Hétu 2016; DiPiero, 2017; Evangelista et al., 2018; Martin, 2014a; Martin et al., 2019a), de compétition entre les vendeurs (Martin, 2014a), et de risques de détection de la part des forces de l'ordre que lorsqu'ils effectuent ces mêmes transactions au niveau de la rue (Holt et al., 2015; Martin, 2014a). En effet, la présence des nombreux outils technologiques visant la protection de leur identité et de leur localisation, tel que TOR (Evangelista et al., 2018; Shortis et al., 2020), de technologies permettant le cryptage des communications (Shortis et al., 2020) et l'utilisation de cryptomonnaie non retraçable (DiPiero, 2017; Europol, 2017; van Hardevald et al., 2017), rendent particulièrement difficile l'identification et l'arrestation des participants aux cryptomarchés. De plus, le caractère virtuel des cryptomarchés permet aux vendeurs de ne pas avoir à se déplacer afin d'atteindre des clients potentiels et leur faire parvenir

la marchandise. Cela réduit drastiquement leur exposition, et contribue à rendre l'identification des membres plus ardue (Aldridge et al., 2018; Evangelista et al., 2018; Martin, 2014a).

Au cours des dernières années, les forces de l'ordre ont tenté de perturber et de contrer les activités illicites ayant lieu dans le darkweb, notamment en ciblant directement les plateformes abritant les cryptomarchés (Leontiadis et Hutchings, 2015; Gupta et al., 2018; Martin, 2014a). Malgré la réussite de certaines interventions, qui ont mené à la fermeture complète de certaines de ces plateformes, les forces de l'ordre ne semblent pas être en mesure de ralentir la vente de produits illicites à travers le darkweb, et ne parviennent pas à dissuader les participants à y prendre part. Ce phénomène a donc attiré l'attention de nombreux chercheurs, qui se sont penchés sur les impacts des opérations policières menées contre les cryptomarchés. D'abord, ils ont trouvé que les effets de ces interventions sont limités et temporaires, autant au niveau des activités des marchés (Bhaskar et al., 2019; Ladegaard, 2019; Soska et Christin, 2015), qu'au niveau de la participation des membres (Norbutas et al., 2020; van Buskirk et al., 2017), qu'à celui des impacts économiques (Décary-Hétu et Giommini, 2017; Hull, 2017; Miller, 2019) et qu'à celui de la confiance qu'ont les participants envers leur environnement et leur communauté (Lacson et Jones, 2016; Ladegaard, 2018). Par ailleurs, au lieu d'observer l'effet dissuasif escompté par les forces de l'ordre, plusieurs chercheurs ont remarqué un mouvement de déplacement des participants vers une autre plateforme, suite à la fermeture d'un marché (Afilipoaie et Shortis, 2015; Barratt et al., 2016; Miller, 2019; van Buskirk et al., 2017; van Wegberg et Verburgh, 2018). Finalement, les chercheurs ont également rapporté que les chocs externes subis par les participants des cryptomarchés ont plutôt eu comme effet de les pousser à devenir conscients des faiblesses et des limites présentes dans leur écosystème, et qu'ils se sont adaptés afin de combler ces failles. Plusieurs ont relevé des changements dans les habitudes commerciales des membres (Barratt et al., 2016; Childs et al., 2020), alors que d'autres ont remarqué un changement dans le processus transactionnel en place dans les cryptomarchés (Décary-Hétu et Giommini, 2017; Norbutas et al., 2020). D'autres encore ont remarqué des innovations technologiques et l'adoption de mesures de prévention et de sécurité opérationnelle supérieure de la part des participants (Barratt et al., 2016; Childs et al., 2020; Horton-Eddison et Di Cristofaro, 2017; Munksgaard et al., 2017; Soska et Christin, 2015).

En résumé, les interventions policières traditionnelles ne parviennent ni à mettre un frein aux activités illicites produites dans les cryptomarchés, ni même à les ralentir, et motivent même les participants à améliorer leur infrastructure. Les forces policières sont donc venues à réaliser qu'elles devaient changer de stratégie, et ont récemment mené des interventions innovatrices, leur permettant de produire des résultats différents. Devant un tel constat, de nombreux chercheurs encouragent le recours aux interventions innovatrices de la part des forces de l'ordre dans leurs actions futures contre les cryptomarchés (DiPiero, 2017, Hutchings et Holt, 2017; Lane et al., 2019; van Hardeveld et al., 2017).

Cependant, peu de chercheurs se sont attardés sur ces interventions distinctes et sur leurs effets envers les participants des cryptomarchés. D'entrée de jeu, certains chercheurs soulignent des limites dans les connaissances de manière générale, en ce qui concerne les cryptomarchés et leurs participants (Goodison, Woods, Barnum, Kemerer et Jackson, 2019; Jones, 2020). Selon Jones (2020), ces limites empiriques créent des faiblesses dans les capacités des forces de l'ordre à mettre en place des interventions contre ce pan de la cybercriminalité. Également, comme le dénote Hurlburt (2017), le milieu de la cybercriminalité est en évolution continue, et ces changements perpétuels créent un besoin constant d'attention de la part des chercheurs dans ce domaine.

De plus, la majorité des recherches s'intéressant aux impacts des opérations policières sur les participants des cryptomarchés traitent d'interventions utilisant la stratégie traditionnelle de fermeture d'une plateforme de cryptomarché (Munksgaard et Demant, 2016), tel que fut le cas pour la fermeture du cryptomarché Silk Road (Lacson et Jones, 2016; Ladegaard, 2019; Martin, 2014a; van Buskirk et al., 2014), ainsi que lors des opérations Onymous (Barratt et al., 2016; Décary-Hétu et Giommini, 2017; van Buskirk et al., 2017) et Bayonet (van Wegberg et Verburgh, 2018). Peu d'études s'attardent donc aux innovations instaurées dans les pratiques et les stratégies policières en matière d'intervention au sein des cryptomarchés, qui s'attardent davantage à cibler les centres d'informations, et les sources de partage d'informations et de soutien à la communauté (Broadhurst, Ball, Jiang et Wang, 2021; Ladegaard, 2019; Martin et al., 2019a). Comme le soulignent Leukfeldt et Jansen (2020), les recherches portant sur les stratégies alternatives sont très limitées. Malgré l'importance que représentent les innovations mises en

place dans les pratiques d'intervention des forces policières, très peu d'études se sont attardées sur ce sujet. Il n'y a donc que peu de connaissances établies sur l'efficacité des nouvelles et différentes stratégies d'intervention et de prévention utilisées par les forces de l'ordre, au sein des cryptomarchés (Leukfeldt et Jansen, 2020). Il y a également peu, ou pas, d'études portant sur les impacts que ces interventions pourraient avoir sur la confiance des participants envers les infrastructures et la communauté des cryptomarchés (Aldridge et Barratt, 2020; Chan, He, Oiao et Whinston, 2019), sur les pratiques d'achat et de consommation des participants (Aldridge et Barratt, 2020; Chan et al., 2019) et sur la volonté des participants à maintenir leurs activités dans les cryptomarchés (Bradley et Stringhini, 2019; Leukfeldt et Jansen, 2020). Bref, il reste à déterminer si ces nouvelles pratiques et stratégies sont plus efficaces que les approches plus traditionnelles des agences d'application de la loi (Aldridge et Barratt, 2020), et surtout, quels en sont les différents impacts.

L'acquisition de telles connaissances pourrait non seulement permettre une meilleure compréhension du fonctionnement de la communauté distincte regroupant les participants des cryptomarchés, mais cela pourrait également mettre en lumière les motivations et le processus de prise de décision des participants des cryptomarchés. De plus, il serait utile de comprendre l'efficacité des différentes stratégies utilisées, afin de faire ressortir celles qui ont un plus grand impact et qui pourraient, dans un futur éventuel, perturber suffisamment l'écosystème pour potentiellement parvenir à ralentir leurs activités (Jones, 2020). Une meilleure connaissance de l'efficacité de ces pratiques policières innovatrices pourrait également s'avérer utile dans la formation et l'entraînement des corps policiers, ainsi qu'au niveau d'une meilleure allocation des ressources limitées pouvant être utilisées contre les cryptomarchés (Goodison et al., 2019; Jones, 2020).

C'est donc grâce à une étude de cas orientée sur deux interventions particulières que nous tenterons de combler, du moins en partie, ces limites identifiées dans les connaissances actuelles. L'objectif principal de notre étude sera de comprendre les impacts que ces opérations policières innovatrices ont eus sur les participants des cryptomarchés. Nous porterons une attention particulière sur trois aspects particuliers. D'abord, nous chercherons à comprendre comment ces interventions auront affecté la perception d'accessibilité et de facilité d'utilisation généralement partagées par les participants des cryptomarchés. En effet, malgré une interface simple et

accessible, il faut tout de même posséder un certain niveau de connaissances et d'informations afin de pouvoir naviguer de manière sécuritaire à travers les différents sites disponibles dans l'infrastructure du darkweb (Bancroft, 2017; Décary-Hétu, Mousseau et Vidal, 2018; Martin et al., 2019b). Aussi, une instabilité dans les ressources d'informations pourrait engendrer un ralentissement dans les activités présentes dans les cryptomarchés (Martin et al., 2019b). Nous tenterons également de comprendre comment ces interventions peuvent perturber la confiance que les participants ont, autant envers l'écosystème des cryptomarchés qu'envers leur communauté. En effet, Chan et al. (2019), émettent l'hypothèse que ces chocs externes pourraient affecter la confiance des membres envers l'infrastructure et sa capacité de protéger l'anonymat et la sécurité des participants lors des transactions effectuées via ces plateformes. Nous tenterons également de comprendre si ces interventions pourraient avoir un impact sur la perception des risques des participants des cryptomarchés, et si ces nouvelles stratégies d'interventions peuvent changer la perception selon laquelle les cryptomarchés représentent une alternative moins risquée au commerce de substance illicite, en comparaison avec la vente dans la rue. En dernier lieu, nous tenterons de comprendre comment les participants des cryptomarchés répondront à ces nouvelles stratégies d'intervention. Serons-nous témoins de signes de désistement, tel que l'abandon de certaines substances par certaines plateformes, ou de diminution du niveau d'activité de certains participants, tel que le suggèrent Broadhurst et al. (2021), ou est-ce que nos résultats abonderont dans le sens de l'étude de Lorenzo-Dus et Di Cristofaro (2018), qui suggère que les efforts des forces de l'ordre orientés vers la perturbation de l'écosystème des cryptomarchés ne seraient en fait qu'une source de motivation pour les membres de développer de nouvelles technologies et de nouveaux fonctionnements qui leur permettront de subsister aux chocs et se prémunir contre les tentatives futures?

2. 1 Les opérations à l'étude

Afin de répondre à nos objectifs, nous étudierons les réactions des participants des cryptomarchés à la suite de deux interventions innovatrices qui ont eu lieu récemment, soit l'intervention policière ayant mené à la fermeture de la plateforme DeepDotWeb, ainsi que l'opération DisrupTor.

2. 1. 1 La fermeture de la plateforme DeepDotWeb

Nous avons pu être témoin de nouvelles approches empruntées par les forces de l'ordre lors de leurs interventions récentes, et la fermeture de la plateforme DeepDotWeb en est un excellent exemple. En activité depuis octobre 2013 (Europol, 2019), DeepDotWeb représentait un outil très important pour les participants des cryptomarchés. Qualifiée de « passerelle vers le darkweb » (U.S. Department of Justice, 8 mai 2019), cette plateforme web était à la fois présente dans le darkweb et dans le web régulier, et permettait à de nombreux participants de se déplacer aisément à travers les différents sites et marchés. Les adresses URL des sites hébergés sur le darkweb ne sont pas comme celles hébergées dans le web régulier; l'adresse d'un .onion représente rarement le nom du domaine auquel il mène. Généralement, il s'agit d'une suite de lettres et de chiffres n'ayant pas de lien ensemble. Il est donc difficile pour les membres de retrouver facilement les adresses des sites vers lesquels ils souhaitent aller. DeepDotWeb fournissait une liste de ces liens, qui étaient vérifiés et validés. Il ne restait donc aux participants qu'à cliquer sur les liens suggérés pour être directement redirigés vers les marchés et sites web du darkweb (United States of America v T. Prihar et M. Phan*,* 2019; Martin et al., 2019a). Cet outil de référencement était largement utilisé par la communauté active dans les cryptomarchés : 23,6% des commandes effectuées sur le cryptomarché Alphabay, ainsi que 47,2% des commandes effectuées sur le cryptomarché Hansa, lors de leur fermeture, provenaient d'utilisateurs ayant eu recours à DeepDotWeb lors de leurs recherches (United States of America v T. Prihar et M. Phan*,* 2019). En plus d'être une source reconnue pour le partage de liens fiables menant vers les divers cryptomarchés (Caleb, 2019), DeepDotWeb proposait également de nombreux guides et tutoriels, en plus d'être une des sources primaires d'information et de

partage d'actualité, au sein de la communauté des participants des cryptomarchés (United States of America v T. Prihar et M. Phan, 2019; Martin et al., 2019a).

Le 6 mai 2019, une opération internationale fut menée contre la plateforme DeepDotWeb et provoqua sa fermeture définitive ainsi que l'arrestation de ses deux administrateurs, Tal Prihar et Michael Phan (United States of America v T. Prihar et M. Phan, 2019; Europol, 2019). Au moment des arrestations, les forces de l'ordre ont pris possession des portefeuilles des deux individus, saisissant un total de 15 489 415$, provenant des commissions sur les transactions de biens illicites (United States of America v T. Prihar et M. Phan, 2019; U.S. Department of Justice, 8 mai 2019). En effet, chaque fois qu'un participant utilisait l'un des liens exposés sur la plateforme DeepDotWeb et effectuait l'achat d'un bien illicite, les administrateurs de la plateforme recevaient une commission de référencement sur la vente (United States of America v T. Prihar et M. Phan, 2019; Martin et al., 2019a). C'est d'ailleurs sous le motif de profit fait sur la vente de produits illicites, ainsi que sous celui de blanchiment d'argent, que les deux administrateurs de la plateforme web furent interceptés par les agences d'application de la loi (Europol, 2019).

Ce qui distingue cette intervention policière des autres interventions traditionnelles est le fait que les forces de l'ordre aient ciblé une plateforme web qui servait d'outil facilitateur à l'utilisation des marchés, et non un marché en soi. Il s'agit en effet de la première intervention contre l'infrastructure supportant le darkweb et sa communauté (U.S. Department of Justice, 8 mai 2019). De plus, DeepDotWeb était un outil très important et largement utilisé par la communauté. Son retrait risque de réduire drastiquement la facilité d'accès aux différentes plateformes et de nuire aux activités des participants qui s'appuyaient sur les informations qu'elle publiait. C'est d'ailleurs l'un des buts visés par les forces de l'ordre : le FBI qualifia d'ailleurs cette opération de « perturbation la plus importante causée par les forces de l'ordre jusqu'à présent » (U.S. Department of Justice, 8 mai 2019). Ils souhaitaient également envoyer aux participants le message que « nous nous attaquions aux opérateurs de ces sites Web dangereux » (FBI, 2019) et que « le FBI ne ferme pas les yeux sur les activités criminelles qui se produisent sur ou hors du Darknet » (FBI, 2019).

2. 1. 2 L'Opération DisrupTor

La seconde opération à l'étude est l'opération DisrupTor, qui fut annoncée par le FBI le 22 septembre 2020 (U. S. Department of Justice, 22 septembre 2020). Malgré son annonce tardive par les autorités américaines, l'opération DisrupTor avait débuté plusieurs mois auparavant. Cette intervention découle directement de la fermeture du cryptomarché WallStreet Market, qui a eu lieu en avril 2019 (US Department of Justice, 22 septembre 2020a). Étant l'une des plateformes les plus populaires au moment de sa fermeture, WallStreet Market comptait plus de 5 400 vendeurs actifs et desservait 1,15 million de clients dans le monde (Europol, 2019a). C'est grâce à la mise en place d'une coopération internationale, impliquant les agences d'application de la loi provenant de plusieurs pays que le marché WallStreet Market fut saisi et ses administrateurs arrêtés (Europol, 2020).

Suite à cette réalisation des forces de l'ordre, ces dernières sont également parvenues à mettre la main sur les serveurs de la plateforme, obtenant ainsi accès à une quantité importante d'informations portant notamment sur les différents vendeurs et clients actifs sur le site (Europol, 2020; U. S. Department of Justice, 22 septembre 2020a). Grâce à ces informations, les forces de l'ordre sont parvenues à identifier de nombreux participants et, une fois ces informations traitées et vérifiées, ont procédé à l'arrestation de nombreux membres. Cette opération internationale permit l'arrestation de 179 vendeurs, la saisie de 6,5$ millions, de 64 armes à feu et de plus de 500 kg de drogues, comprenant du fentanyl, de l'héroïne, de la cocaïne et de nombreux opioïdes (Europol, 2020; U. S. Department of Justice, 22 septembre 2020a). Parmi les 179 individus arrêtés, certains se sont avérés être des membres importants dans le commerce de drogues en ligne. Notamment, les autorités sont parvenues à mettre la main sur les membres derrière le compte Stealthgod (U. S. Department of Justice, 22 septembre 2020a; U. S. Department of Justice, 22 septembre 2020b), et qui auraient effectué plus de 18 000 transactions de méthamphétamine via les plateformes de cryptomarchés (U. S. Department of Justice, 22 septembre 2020a). Les forces policières ont également appréhendé Arden McCann, l'individu derrière les pseudonymes DrXanax et RcQueen (U. S. Department of Justice, 22 septembre 2020a; Barratt et Aldridge, 2020). Ce Canadien avait la capacité de vendre plus de 10kg de fentanyl et plus de 300 000 capsules contrefaites de Xanax par mois (US Department of Justice,

22 septembre 2020). Les autorités ont aussi arrêté les participants connus sous le nom de Pill Cosby (U. S. Department of Justice, 22 septembre 2020b; Barratt et Aldridge, 2020), qui furent accusés d'être responsables de la vente de plus de 1 million de doses contrefaites, contenant du fentanyl. D'autres vendeurs importants, derrière des comptes tels que DrugPharmacist, RickandMortyShop, NeverPressedRX (NPRX), TenderwoodCock, QuartersetUp, ainsi que Colsadersdreams (U. S. Department of Justice, 22 septembre 2020b) furent également appréhendés lors de cette intervention.

En ciblant ainsi plusieurs individus à la fois, et non seulement une seule plateforme et ses administrateurs comme il en est coutume, les forces de l'ordre cherchaient d'abord à faire prendre conscience aux participants des cryptomarchés que, malgré le fait qu'ils parviennent à enfouir leurs activités illicites dans les coins reculés du web, ils ne pourront pas toujours échapper aux forces de l'ordre (Europol, 2020). Ils cherchaient également à leur faire comprendre que l'anonymat complet n'existe pas, et que l'internet caché n'est désormais plus un lieu sûr pour les criminels. Ils visaient donc l'ébranlement de la confiance des participants des cryptomarchés, en leur faisant prendre conscience des risques qu'ils courent en maintenant leurs activités illicites, même à partir du darkweb (Barratt et Aldridge, 2020).

L'opération DisrupTor a donc démontré les capacités des forces de l'ordre de rivaliser avec la constante évolution du cyberespace, en innovant eux-mêmes et en créant de nouvelles stratégies pour identifier et atteindre un nombre important de participants (U. S. Department of Justice, 22 septembre 2020). Ils ont également démontré qu'en coopérant ainsi, les instances légales de différentes provenances étaient capables de mener une frappe efficace contre le trafic de stupéfiants en ligne, plus spécifiquement au trafic d'opioïdes. Cibler ainsi plusieurs individus séparément, au lieu de s'orienter vers une plateforme et ses administrateurs, visait également à ébranler la confiance des participants de tous les niveaux; il était question de faire passer le message que les forces policières n'en ont pas seulement contre les marchés, mais également contre les plus petits criminels qui vendent et achètent des biens illicites via ces marchés (Europol, 2020).

Chapitre 3 : La méthodologie

3. 1 La collecte des données

La section suivante détaillera les différentes étapes de la collecte de données qui ont servi à la réalisation de cette étude. Nous avons analysé des messages extraits de discussions sur des pages forums traitant de l'univers des cryptomarchés et du darkweb. Nous débuterons donc en expliquant l'intérêt d'inclure des données émanant des forums comme bases de données, en prenant soin d'énumérer les principaux avantages et les principales limites d'une telle manœuvre. Nous énumérerons ensuite les différentes étapes de notre collecte de données, en prenant soin de justifier les choix que nous avons posés, et nous dresserons un portrait de notre échantillonnage.

3. 1. 1 L'utilisation des forums

L'importance grandissante de la technologie dans notre vie courante a eu un impact sur les différents moyens de communication dont nous disposons. Grâce, entre autres, aux plateformes de partage, tels que les réseaux sociaux ou encore les forums web, les échanges sociaux sont instantanés, internationaux et peuvent traiter de n'importe quel sujet (Holt, 2010). Il s'agit donc d'outils facilitant grandement la communication et le partage d'informations, qui permettent aux groupes criminels et aux individus déviants, présents sur le web, de communiquer entre eux malgré de longues distances. Ils facilitent également la transmission de connaissances nécessaires à l'accomplissement des activités propres à ce groupe d'individus, qui peuvent désormais être acheminées d'un membre à l'autre sans besoin de contact physique ou d'effort de déplacement quelconque (Holt, 2010). Les activités de ces individus sur les espaces en ligne ne servent pas uniquement aux criminels; ils facilitent aussi grandement de nouvelles méthodes de collecte de données (Holt et al., 2015; Paquet-Clouston et al., 2018). Que ce soit grâce à l'observation des traces laissées par les usagers lors des transactions émises sur les marchés, ou suite à l'étude des forums de partage, de nombreux chercheurs se sont servis des données cumulées en ligne pour étudier le cyberespace, permettant donc d'étudier les marchés de drogues illicites en ligne (Enghoff et Aldridge, 2019). En effet, sur les sites de marchés et de forums, se

retrouve une quantité importante et variée d'informations accessibles : elles proviennent des profils des vendeurs, des commentaires publiés sur les forums, visant à indiquer les performances et la fiabilité des membres, les détails sur les livraisons et la marchandise, etc. (Smith et Frank, 2020), et permettent de dresser un portrait détaillé des activités qui ont lieu sur ces plateformes. D'autre part, l'étude des publications sur les forums permet d'analyser le processus de pensée, les perceptions et les expériences des usagers (Bradley et Stringhini, 2019; Childs et al., 2020), éléments qui ne sont pas accessibles dans les marchés de drogues illicites réguliers.

L'utilisation des messages publiés sur les forums comme base de données comporte de nombreux avantages, et plusieurs chercheurs s'en sont d'ailleurs déjà servis dans le cadre de leurs études (Bradley et Stringhini, 2019; Cho et Wright, 2019; Ladegaard, 2019; Kamphausen et Werse, 2019; Aldridge et Askew, 2017; Childs et al., 2020; Ladegaard, 2018; Barratt et al., 2016). D'abord, les forums sont synonymes d'abondance de données (Holtz, Konberger et Wagner, 2012; Seale, Charteris, Black, MacFarlane et McPherson, 2009). En effet, il y a une multitude de sites de forums présents sur internet, qui traitent de tous les sujets, sur lesquels des milliers d'usagers partagent des millions de publications (Holtz et al., 2012). Ils permettent d'entrer en contact avec des communautés plus difficiles à rejoindre. L'aspect virtuel permet, en effet, d'atteindre des individus isolés géographiquement ou socialement ainsi que des sous-cultures déviantes plus rares et difficiles d'accès (Enghoff et Aldridge, 2019; Seale et al., 2009). L'anonymat que permettent ces plateformes procure un sentiment de liberté aux participants, qui se sentent plus à l'aise dans leur partage et partagent librement, parfois même en s'incriminant. Ils peuvent alors donner des détails qui, habituellement, ne seraient pas divulgués (Seale et al., 2009).

En plus de fournir d'impressionnantes quantités de données, les forums en permettent facilement la récupération. Les discussions et commentaires publiés sur ces plateformes sont simples à trouver et à échantillonner (Holtz et al., 2012; Im et Chee, 2006). Comme il s'agit de matériel public et ouvert, il est facile de retracer le processus d'échantillonnage effectué par les chercheurs. Cela procure un aspect de transparence ajouté dans leur analyse, ainsi qu'un aspect de traçabilité, un critère important dans la réalisation d'une recherche qualitative valide (Holtz et

al., 2012). L'aspect ouvert et public des publications sur les forums abaisse également le souci éthique qui, habituellement, est lié à l'utilisation de matériel provenant des paroles partagées par des individus; dans le cas des forums, il s'agit d'un partage fait de manière libre et autonome par l'usager, sur une plateforme qu'il sait déjà publique (Seale et al., 2009). Finalement, les données que l'on retrouve dans les forums de discussion en ligne présentent des caractéristiques temporelles qui leur sont propres. Une fois publiée, à moins d'une suppression du commentaire, de la discussion ou de la plateforme, la publication reste accessible et ce peu importe le temps qui s'écoule. Cela procure une flexibilité de récupération importante pour le chercheur; ce dernier évite le fardeau du temps investi dans la participation de l'échange avec sa source, et réduit également la pression du temps qui passe et les risques de maintien du matériel, dans l'accumulation des données (Im et Chee, 2006). Cette flexibilité temporelle offre également la possibilité au chercheur de voir de façon asynchrone, le développement des idées et des opinions des membres; il a accès aux réactions ayant eu lieu avant, pendant et après un certain nœud temporel, et peut voir l'évolution des réactions des usagers (Im et Chee, 2006). Chaque nouveau commentaire publié risque de soulever d'autres participations des membres, et en tout temps il est possible de voir une opinion ou une idée se développer davantage, se préciser, ou encore un nouveau dialogue se créer (Holtz et al., 2012). De manière générale, les participants sur un forum font partie d'une sous communauté distincte. Par exemple, un forum traitant de la pêche regroupera majoritairement des adeptes de cette activité. La collecte de données provenant des forums permet donc une analyse des discours typiques qui ont lieu dans de telles communautés (Holtz et al., 2012; Enghoff et Aldridge, 2019). Se déroulant librement dans un contexte naturel virtuel et anonyme, il y a peu de contraintes sociales qui pourraient dénaturer les données ou restreindre le partage libre des opinions des membres. Les discussions se déroulent sans la présence d'un observateur; il n'y a donc pas de risque d'interférence ou d'influence de sa part, sur l'expression de la pensée des participants (Holtz et al., 2012; Seale et al., 2009). Ce type de données permet donc de mettre en lumière le processus de pensée et les opinions des participants, sans interférence et presque sans limites (Bradley et Stringhini, 2019).

Malgré les nombreux avantages énumérés, l'échantillonnage se basant sur les messages publiés dans les forums de discussions comporte également certaines limites. D'abord, il existe une inégalité dans l'accès à internet, provoquant l'impossibilité pour certains individus faisant

partie de la communauté étudiée à participer aux discussions. Cette réalité restreint donc la collecte de données aux individus possédant le matériel et les capacités leur permettant d'avoir accès à une plateforme web (Seale et al., 2009). Cette réalité ne s'applique cependant pas à notre cas, car la nature même de la communauté que nous étudions se retrouve sur le web.

Ensuite, certains contributeurs peuvent être très actifs et partager, à de nombreuses reprises leur façon de penser, alors que d'autres membres de ces communautés peuvent tout simplement faire le choix de ne pas participer aux conversations (Bradley et Stringhini, 2019). L'observation des forums ne permet donc pas de prendre en compte les paroles de tous les membres étudiés, mais seulement les plus loquaces. L'aspect virtuel des échanges empêche également de valider la véracité des messages partagés (Bradley et Stringhini, 2019; Childs et al., 2020; Enghoff et Aldridge, 2019; Barratt, Ferris, Zahnow, Palamar, Maier et Winstock, 2017). Le contenu se retrouvant sur ces plateformes est publié de manière anonyme; les participants ne ressentent donc pas de pression ou de responsabilité par rapport à ce qu'ils écrivent. Il est donc probable que certains d'entre eux décrivent une réalité altérée, ou encore des objets de leurs fantasmes ou de leur imagination. Il n'y a aucune garantie que ce que l'usager partage soit véridique (Seale et al., 2009). Malgré la présence de ces limites dans la réalité de notre étude, leurs impacts sont minimes : grâce à l'importante quantité de données recueillies, provenant de multiples ressources variées, nous sommes parvenus à effectuer une couverture étendue des messages publiés par la communauté des participants des cryptomarchés sur les forums. Bien que nous ne puissions prétendre avoir récupéré la totalité des échanges, nous avons effectué une collecte suffisamment large pour couvrir le mieux possible les réalités partagées par les membres. La présence de pseudonyme ne permettant d'identifier distinctement chacun des individus participants aux échanges – certains d'entre eux pourraient utiliser plus d'un pseudonyme à la fois – notre échantillon laisse tout de même paraître un nombre important de pseudonymes distincts, ce qui nous permet de croire que nous avons recueilli des données provenant d'un grand nombre de participants. Nous pouvons ainsi prétendre que, tout d'abord, notre collecte de données couvre une majorité des perceptions des membres, et pas seulement celle des plus loquaces. Évidemment, il nous est impossible d'atteindre les pensées des individus préférant s'abstenir de partager sur les forums, mais le but de notre étude est d'obtenir une vue d'ensemble des perceptions de la communauté, non pas individuelle. La représentativité n'est pas

un enjeu pertinent dans notre cas (Barratt et al., 2017), et l'absence de ces informations ne nous infortune donc aucunement. De plus, malgré l'impossibilité de valider la véracité de chacun des messages retenus, nous nous sommes attardés sur les lignes directrices des messages recueillis, tout en prenant soin de ne pas donner plus d'importance aux messages extravagants ou qui ressortaient de manière distinctive du lot. Encore une fois, la vision d'ensemble était notre cible d'intérêt, et nos résultats reflèteront donc les thèmes dominants présents dans les données recueillies.

Finalement, l'observation des discussions de forums limite le chercheur dans son rôle. Alors que lors des entretiens face à face, il lui est possible de clarifier certains points, revenir sur des détails ou poser des questions pour relancer certaines idées, il lui est impossible de le faire lorsqu'il prend un rôle d'observateur anonyme en ligne (Seale et al., 2009). Il est donc limité dans l'approfondissement des pensées et réflexion des usagers, ne pouvant aller plus loin que les écrits partagés. Notre recherche étant principalement menée par un processus exploratoire, cette réalité ne nous a cependant pas affectés outre mesure. Nous cherchions justement à nous laisser guider par les données, tel qu'elles furent publiées. Ainsi, nous avons pu être dirigés vers des sujets inattendus et insoupçonnés qui n'auraient potentiellement pas été explorés si nous avions occupé un autre rôle que celui d'observateur invisible (Seale et al., 2009).

3. 1. 2 Processus et étapes de la collecte de données

Dans le but de cumuler le plus de données provenant de sources multiples et variées, nous avons eu recours à divers moteurs de recherche ainsi qu'à quelques répertoires de liens afin de cibler les sites de forums pertinents à notre étude. Les sites web hébergés dans le darkweb ne sont pas indexés; il faut connaître leur lien Onion exact pour pouvoir y accéder. Plusieurs outils ont donc été utilisés. Nous nous sommes, entre autres, référés à Google, ainsi qu'au site Dark.fail, une plateforme qui offre une liste des principaux sites et forums actifs dans le darkweb. Ce site est accessible via le web de surface, ainsi qu'à travers Tor. Nous avons également utilisé des moteurs de recherche dans le darkweb, tel que DuckDuckGo, Ahmia, Torch Search Engine, Not Evil et Candle. Tous ces sites sont hébergés dans le darkweb. Nous

avons également eu recours à des sites proposant des répertoires de liens, tel que Deepweblinks, Deeponionweb, Onion.live et Flashlight.

Dans le cadre de la recherche de forums, plusieurs mots clés furent utilisés, tel que : « Forum », « Darknet Forum », « Drug Forums », « TOR Forums », « TOR website », « Darknet website ». Il s'agit d'une liste non exhaustive, mais qui représente les mots clés ayant permis d'atteindre la majorité des sites retenus. Il était important pour nous que nos données proviennent de plusieurs sources différentes, afin d'accéder à un échantillon de messages le plus complet et varié possible. Chaque site héberge une sous-communauté particulière, et transpose ainsi une opinion distincte. Pour qu'un forum identifié soit considéré comme pertinent à notre étude, il devait répondre à certains critères. D'abord, nous nous sommes restreints aux forums anglophones seulement. Malheureusement, il existe une quantité considérable de forums d'autres langues, mais la barrière linguistique nous a contraints à ne sélectionner que ceux de langue anglophone. La majorité des forums retenus présentent un contenu entièrement dédié à la communauté des cryptomarchés et à la vente de produits illicites sur le web. Dans l'optique d'accéder à une base de données des plus complètes, nous avons aussi retenu les discussions provenant des forums dont les sujets de discussion variaient, allant de la vente de drogues, aux cryptomonnaies, à la sécurité et la privatisation informatiques, et au cyberenvironnement plus général. Dans ces cas précis, les discussions devaient cependant porter directement sur les cryptomarchés. La majorité des forums consultés dans le cadre de cette recherche sont des forums ouverts au public; c'est-à-dire qu'ils ne nécessitaient aucune inscription ou création d'un compte d'utilisateur pour avoir accès à leurs contenus. Certains, cependant, étaient seulement ouverts aux membres. Pour ces sites, nous avons donc créé des profils d'utilisateurs, dans le but de couvrir le plus de données possible. Par souci de maintenir une invisibilité et une passivité complète dans les discussions, et ainsi ne pas influencer la nature des discussions et des réactions des usagers, nous nous sommes assurés de ne pas intervenir dans aucune discussion, en ne participant pas aux échanges et en ne prenant contact avec personne (Holt, 2010). Nous sommes, en tout temps, demeurés dans un rôle d'observateur invisible.

Étant donné la nature instable du darkweb, ainsi que la distance temporelle entre les deux collectes de données, les forums utilisés pour cumuler les données de chacune des interventions

varient quelque peu. Pour chacune des interventions étudiées, les principales sources de données furent Reddit, dans le web de surface, et Dread, son équivalent dans le darkweb. Reddit est un populaire site de partage de nouvelles et de discussions, ouvert à tous, et qui couvre un nombre infini de thèmes. Consulté par 52 millions usagers par jour en 2020 (Patel, 2020; Kastrenakes, 2020), Reddit permet les partages sur presque n'importe quel sujet. Les publications sont organisées en sous-sections, et regroupées selon des catégories d'intérêt spécifiques, appelées des Subreddit (Porter, 2018). Dread, pour sa part, est en tout point semblable à Reddit, mais est hébergé sur le darkweb. Il s'agit de l'endroit privilégié par les usagers des cryptomarchés, où y sont partagés le capital illicite, les dernières nouvelles, les impressions entourant des vendeurs et des marchés, les événements importants et des discussions sur tous les sujets. À eux seuls, ces deux sites représentent plus de la moitié de notre collecte de données. Les autres forums utilisés dans la collecte de données sont les suivants : pour l'opération policière ayant mené à la fermeture de la plateforme DeepDotWeb, nous nous sommes servis des sites DNStars, Blackhat World et Shroomery, hébergés dans le web de surface, ainsi que des forums The Hub, DNM Avengers, Envoy, Torum, NZ Darknet Market Forums et Hidden Answer, hébergés dans le darkweb. Les forums retenus pour la collecte de données portant sur l'opération DisrupTor sont, dans le web de surface, ycombinator, Blackhat World, Twitter, Slashdot et Shroomery, et dans le darkweb, The Hub, DNMHQ et DNM Avengers.

Une fois l'étape d'identification des forums complétée, nous sommes passés à l'identification et la sélection des conversations pertinentes à notre étude. Nous avons débuté le processus en procédant à des recherches de discussions traitant des interventions étudiées. Pour chacune des deux opérations, nous avons établi une liste de mots clés qui nous ont permis de faire ressortir les conversations traitant de l'intervention. Pour chacune des interventions, nous avons utilisé le nom de l'opération, ainsi que l'organisation derrière l'intervention et les individus impliqués. Pour ce qui est de l'intervention menée contre DeepDotWeb, nous avons utilisé les mots clés suivants : d'abord, « DeepDotWeb » et son abréviation, « DDW ». Ils nous ont fourni un nombre important de discussions retenues pour cet événement. Dans le but d'étendre davantage les résultats et afin de parvenir à une collecte plus complète, nous avons également utilisé des mots clés ayant une portée plus large, tel que « takedown », « shutdown », « bust », « seize », « darknet », « DNM shutdown », « feds », « police », et « FBI ». Dans le cas de l'opération DisrupTor, nous avons sensiblement procédé de la même façon. Nous avons

entamé nos recherches à l'aide du mot clé « DisrupTor ». Cependant, dans ce cas précis, les discussions retenues furent moins nombreuses. Nous avons donc également utilisé les termes suivants : « bust », « JCODE », « Law enforcement », « vendors arrest », « 179 arrest », « Darknet », « Darknet bust », « crackdown », « raid », « DNM », « feds », « operation », « seized », « vendors », « raid » et « takedown ». Le but de notre étude étant de comprendre les impacts des interventions étudiées sur les usagers des cryptomarchés, et non seulement de comprendre les impacts de l'annonce publique de celles-ci par les forces de l'ordre, nous avons jugé pertinent d'inclure les noms des principaux vendeurs arrêtés lors de l'opération DisrupTor. Selon nous, il s'agit d'un élément important à prendre en considération; alors que l'annonce officielle de l'opération a pu ébranler les membres de la communauté, la disparition continue de vendeurs populaires est également sujette à causer un dérangement chez les usagers habitués à faire affaire avec eux. Nous avons donc passé en revue les différentes publications officielles des forces de l'ordre, afin d'identifier quels vendeurs furent interceptés lors de l'intervention. Les pseudonymes utilisés par ces individus pour mener leurs activités sur les cryptomarchés furent donc ajoutés à notre liste de mots clés : Arden McCann, connu sous le pseudonyme de DrXanax et RcQueen, DrugPharmacist, RickandMortyShop, NeverPressedRX (NPRX), Pill Cosby, Stealthgod, TenderwoodCock, QuartersetUp, ainsi que Colsadersdreams. De nombreux résultats sont ressortis de ces recherches, nous permettant d'atteindre une vaste étendue de conversations utilisées pour notre étude.

Nous avons débuté la collecte des données pour chacune des interventions à des moments différents. L'intervention ayant mené à la fermeture de DeepDotWeb ayant eu lieu le 6 mai 2019, nous avons donc pris en considération les discussions publiées à partir de cette date. Nous avons étendu la collecte des données jusqu'à 6 mois après l'intervention, soit jusqu'en novembre 2019. Les tentatives de cumuler des messages pertinents après cette période étaient très limitées, nous avons donc constaté que nous avions atteint un niveau de saturation dans les discussions publiées concernant la fermeture de la plateforme DeepDotWeb.

L'annonce de l'opération DisrupTor a eu lieu le 22 septembre 2020. La majorité des données collectées proviennent d'ailleurs de cette date, et des jours suivants. Cependant, le début de la période d'arrestation des membres visés remonte à plus tôt que cela, et, pour plusieurs, leur

disparition avait déjà été remarquée et commentée. Étant donné que l'opération DisrupTor part de la saisie des serveurs du cryptomarché WallStreet Market, fermé par les forces de l'ordre en mai 2019, nous sommes jusqu'à cette date, en faisant bien attention de ne sélectionner que les discussions qui traitaient de l'arrestation des usagers impliqués. Cependant, les premières discussions retenues portant sur la disparition de ces usagers remontent au mois de juillet 2019, soit le temps que les membres s'aperçoivent de la disparition des vendeurs ciblés. Nous avons terminé cette seconde collecte de données au mois de novembre 2020, soit deux mois après l'annonce publique de l'intervention par les forces de l'ordre. Comme ce fut le cas lors de la fermeture de DeepDotWeb, le nombre de conversations pertinentes retenues après cette période était alors minime, et nous nous sommes donc aperçus que nous avions atteint un niveau de saturation dans les données disponibles.

Lorsqu'une conversation fut identifiée, nous avons scanné visuellement les messages qui la composent, afin de déterminer s'il s'agit réellement de matériel utile à notre étude. Les conversations pertinentes à notre travail étaient ensuite conservées en entier. Dans certains cas, lorsque c'était de longues conversations ne comportant que quelques messages pertinents, alors nous ne sélectionnions que les données ciblées en prenant soin d'exclure le surplus, pour éviter de créer une surcharge de messages dans notre échantillon. Pour qu'un message soit conservé et analysé, il devait répondre à certains critères. Premièrement, les messages retenus devaient correspondre aux réalités temporelles propres à l'intervention. Un message publié avant la date d'une intervention était automatiquement rejeté. Ensuite, les messages faisant partie des conversations dont le sujet était orienté vers l'une des opérations à l'étude furent conservés. Il en fut de même pour chacun des messages mentionnant le nom des opérations ou encore des individus impliqués. De plus, certains messages ne mentionnant pas explicitement ces éléments furent conservés, mais à certaines conditions. Ils devaient, sans nécessairement faire mention directe des opérations, discuter des impacts ressentis par les participants de la communauté. Ainsi, les discussions traitant de tout changement récent au niveau des activités transactionnelles, des aspects pratiques, des émotions ressenties ou des perceptions des participants par rapport à leur écosystème et leur communauté furent conservées pour être par la suite analysées. Afin d'éviter de donner un sens ou d'interpréter à tort certains messages plus vagues, nous n'avons pas retenu les conversations où le lien entre leur contenu et les interventions à l'étude n'étaient

pas clair et évident. Finalement, les messages satiriques ou sarcastiques ne furent pas considérés, afin de ne pas fausser les analyses finales.

Nous avons pris soin de conserver les conversations complètes lorsque possible; les messages superflus nous permettent donc une compréhension du contexte dans lequel la discussion a pris forme, et ils permettent parfois une compréhension plus complète des idées et opinions transmises. Les conversations et les messages retenus varient en longueur, et peuvent avoir lieu entre des vendeurs, des acheteurs, des administrateurs, ou tout type d'usager des plateformes de discussion liées aux cryptomarchés. Une fois une discussion retenue, nous ajoutions son URL dans une liste, qui était ensuite destinée à un outil de web scraping.

C'est grâce à la méthode de web scraping que nous sommes parvenus à retirer l'ensemble des discussions identifiées de leur plateforme et à les transférer vers nos documents. Cette méthode permet l'extraction d'éléments provenant d'une variété de sources, tels que les sites de forums et les sites de marchés, ainsi que les profils d'utilisateurs, les listes de produits vendus et autres éléments jugés pertinents. C'est un outil discret et utile, qui facilite l'étude des populations plus difficiles d'accès tel que les marchés illicites, et qui fut déjà utilisé par de nombreux chercheurs (Broséus et al., 2016; Décary-Hétu et Giommoni, 2017; Décary-Hétu et Quessy-Dore, 2017; Demant et al., 2019; Dolliver et Kenney, 2016; Paquet-Clouston et al., 2018; Tzanetakis, 2018 et Van Buskirk et al., 2017).

Ce processus de collecte de données nous a permis d'extraire, pour l'intervention menée contre DeepDotWeb, 74 discussions et 2841 messages, et pour l'opération DisrupTor, 176 discussions et 3827 messages. Les tableaux 1 et 2, ci-dessous, permettent un meilleur aperçu du portrait des données recueillies ainsi que de leur provenance parmi les différentes ressources consultées. Pour chaque message extrait, nous avons retenu le titre officiel de la discussion d'où il provient, l'heure et la date à laquelle il a été publié, son contenu textuel, son ordre d'apparition dans la discussion d'origine et le nom de l'utilisateur à l'origine de sa publication. L'ensemble de ces variables fut rassemblé dans un document Excel, que nous avons ensuite révisé, afin de corriger les potentielles erreurs d'extraction, de doublons ou de variables mal formulées. Une fois cette étape complétée, nous nous sommes tournés vers l'analyse de nos données.

Tableau 1. Distribution des données relatives à la fermeture de la plateforme DeepDotWeb, selon leur source de provenance

	Données relatives à la fermeture de la plateforme DeepDotWeb			
	Nombre de discussions	**% des discussions**	**Nombre de messages**	**% des messages**
Shroomery	2	2,7%	56	1,9%
DNStars	1	1,3%	3	0,1%
BlackHatWorld	2	2,7%	13	0,5%
DNM Avengers	7	9,5%	314	11,1%
Envoy	6	8,1%	201	7,1%
Hidden Answer	2	2,7%	11	0,4%
NZ Darknet Market	2	2,7%	7	0,2%
The Hub	10	13,5%	263	9,3%
Torum	6	8,1%	75	2,6%
Reddit	15	20,3%	792	27,9%
Dread	21	28,4%	1106	38,9%
Total	**74**	**100%**	**2841**	**100%**

Tableau 2. Distribution des données relatives à l'opération DisrupTor, selon leur source de provenance

	Données relatives à l'opération DisrupTor			
	Nombre de discussions	**% des discussions**	**Nombre de messages**	**% des messages**
Shroomery	4	2,2%	76	2,0%
Slashdot	1	0,6%	151	4,0%
BlackHatWorld	1	0,6%	10	0,3%
ycombinator	1	0,6%	342	8,9%
Twitter	4	2,2%	61	1,6%
The Hub	7	4,0%	274	7,2%
DNMHQ	1	0,6%	8	0,2%
DNM Avengers	8	4,5%	97	2,5%
Reddit	61	34,7%	1301	34,0%
Dread	88	50,0%	1507	39,3%
Total	**176**	**100%**	**3827**	**100%**

Les tableaux ci-haut exposent la provenance des données formant notre échantillon. Chaque tableau correspond à l'une des interventions. La première colonne présente la liste des forums utilisés lors la collecte des données. Les colonnes suivantes indiquent, pour chacun des sites, le nombre de discussions et de messages retenus, ainsi que le pourcentage que représente l'apport de chaque forum. Cela permet donc, d'abord, la démonstration en détail de l'utilisation de sources variées dans le cadre étude. Nous pouvons aisément voir que, d'une étape de la collecte de donnée à l'autre, les forums Reddit et Dread restent les principales sources de données retenues. Malgré le fait que certaines sources n'aient contribué que minimalement à l'échantillon total, ces tableaux démontrent tout de même l'étendue et la variété des sources utilisées. Cet exercice fut effectué par souci d'atteindre le plus de participants, et ainsi offrir prendre en considération les perceptions et les points de vue du plus grand nombre d'individus

différents et de refléter les perceptions d'une plus large partie de la communauté des cryptomarchés.

3. 2 Méthode de recherche

La section suivante présentera la méthode de recherche utilisée dans cette étude. Afin de répondre à nos objectifs, nous avons eu recours à la méthodologie de recherche qualitative. Nous avons procédé à l'étude des deux opérations policières présentées précédemment, soit la fermeture de la plateforme DeepDotWeb, ainsi que l'opération DisrupTor. L'analyse de nos données fut effectuée grâce à l'approche inductive, qui nous a permis de sonder nos données brutes en profondeur et ainsi en faire ressortir les thèmes s'y retrouvant naturellement (Hadlington, Lumsden, Black et Ferra, 2021; Fereday et Muir-Cochrane, 2006; Zhang et Wildemuth, 2009). La codification des données eut ensuite lieu et un accord interjuge fut effectué dans le but d'attester de la rigueur et de la fiabilité entretenues tout au long du processus par les chercheurs impliqués (O'Connor et Joffe, 2020; Burla et al., 2008).

3. 2. 1 L'étude qualitative

Un grand nombre des recherches qui portent sur les cryptomarchés et les impacts qu'ont eus les opérations policières sur leur écosystème ont été effectuées à l'aide d'études quantitatives (Soska et Christin, 2015; Décary-Hétu et Giommoni, 2017; Ladegaard, 2019; Van Buskirk et al., 2017; van Wegberg et Verburgh, 2018); d'autres études, moins nombreuses, se sont servies des données provenant des forums et ont eu recours aux méthodes qualitatives (Lacson et Jones, 2016; Horton-Eddison et Di Cristofaro, 2017; Bradley et Stringhini, 2019). C'est à ce deuxième groupe que s'ajoute notre étude, en tirant nos données des publications provenant des forums de discussions axées sur les cryptomarchés. Ces plateformes, qui sont les principaux lieux de partage et discussion de la communauté qui rassemble les participants des cryptomarchés, procurent une quantité considérable de données qualitatives facilement accessibles (Paquet Clouston et al., 2018).

Il existe deux types de méthodologies utilisées en recherche : la méthode qualitative et la méthode quantitative. Généralement, les études quantitatives sont composées de quelques variables qui engendrent des données numériques (Hancock et Algozzine, 2016). Les résultats de ces recherches sont généralement analysés et manipulés au moyen de méthodes statistiques variées (Zhang et Wildemuth, 2009), dans le but de tester une hypothèse prédéfinie (Jones, 2020; Merriam et Tisdell, 2015) ou encore d'expliquer les phénomènes observés (Boucherf, 2016). La méthodologie de recherche qualitative, quant à elle, correspond davantage aux données textuelles, constituées d'un plus grand nombre de variables (Anadòn et Guillemette, 2007), et génère des résultats sous forme de descriptions ou de typologies (Zhang et Wildemuth, 2009). Cette méthode de recherche est utilisée dans le but de décrire ou de comprendre des phénomènes sociaux, et permet de porter une attention orientée sur la signification de ces phénomènes, plutôt que sur leur fréquence (Anadòn et Guillemette, 2007; Van Manen, 1990). Elle permet également la compréhension de la nature et la force des interactions des variables entre elles, et ouvre la voie à la compréhension de réalités sociales de manière scientifique et subjective (Zhang et Wildemuth, 2009). La méthode qualitative permet donc de mettre l'emphase sur l'interprétation et la vision complète d'un phénomène social, en tenant compte des contextes environnementaux et sociaux qui lui sont propres (Tewksbury, 2009; Zhang et Wildemuth, 2009).

Cette méthodologie est particulièrement utile, en criminologie, lorsque l'objectif de la recherche est de comprendre la provenance de la criminalité (Tewksbury, 2009; Jacques et Bonomo, 2017). Selon les chercheurs Jacques et Bonomo (2017), les criminels et les délinquants représentent la source première d'information qui permet l'obtention de connaissances sur les actes criminels; ils offrent une perspective de premier plan sur les motivations derrière la commission des délits et des actions délinquantes. Avoir accès à leur point de vue peut également nous permettre d'explorer la réalité sociale de ces individus, et même de susciter l'émergence de nouvelles dimensions de connaissance jusque là restées inconsidérées (Poupart, 1997). Il est donc possible d'élargir notre compréhension de la rationalité du choix derrière l'acte, les pensées et les perceptions de ces acteurs, leur mode opératoire, ainsi que les stratégies mises en place dans le but de contourner les mesures préventives instaurées. La méthode qualitative offre ainsi l'opportunité de comprendre comment prévenir plus efficacement les

activités criminelles, de faire l'évaluation des stratégies de prévention utilisées, et de guider vers la création de mesures plus efficaces (Jacques et Bonomo, 2017).

Il s'agit donc des raisons pour lesquelles nous avons choisi d'utiliser la méthodologie qualitative pour mener notre étude. Notre objectif principal étant de comprendre les impacts qu'ont eus deux opérations non traditionnelles sur les participants des cryptomarchés, il s'agit de la méthode la plus efficace pour accéder aux perceptions de ces derniers, et avoir accès à une vision en profondeur de leur réalité sociale et de la façon dont leur communauté et leur écosystème réagissent aux chocs.

3. 2. 2 L'étude de cas

Il y a six principaux courants de conceptions de recherche en méthodologie qualitative; la recherche qualitative de base, la phénoménologie, l'ethnographie, la théorie ancrée (« grounded theory »), l'enquête narrative et les études de cas qualitatives (Jones, 2020; Merriam et Tisdell, 2015). Couvrir en détail chacun de ces courants ne serait pas pertinent pour notre recherche; c'est pourquoi nous ne nous attarderons que sur le courant utilisé, soit l'étude de cas qualitative. La méthode de recherche de l'étude de cas est une méthode qui cherche à explorer, expliquer et offrir une description d'un phénomène social précis (Baxter et Jack, 2008; Ellinger et McWhorther, 2016; Yin, 2003), par laquelle le chercheur tente de découvrir de nouvelles problématiques et de nouvelles hypothèses (Crosset, 2020; Hamel, 1998; Villemagne, 2006). L'étude de cas est produite dans le contexte unique et naturel du sujet à l'étude, et doit prendre en considération sa réalité contextuelle et temporelle particulière (Crosset, 2020; Ellinger et McWhorter, 2016, Hamel, 1998). Cela permet donc un accès en profondeur et portant sur les multiples aspects d'un phénomène social précis (Feagin, Orum et Sjobert, 1991; Hamel, 1998). Lors d'une étude de cas, le chercheur a recours à plusieurs types de sources de données différentes (Crosset, 2020; Ellinger et McWhorter, 2016; Feagin, Orum et Sjobert, 1991). Cela offre la possibilité d'explorer et de prendre en considération la diversité des aspects composant le phénomène, et permet la couverture et la compréhension totale des multiples facettes présentes dans la réalité du phénomène à l'étude (Feagin, Orum et Sjobert, 1991). Nous avons donc

procédé à une étude de cas multiple à deux volets, portant sur chacune des deux interventions visées par notre étude, soit la fermeture de la plateforme DeepDotWeb, et l'opération DisrupTor.

La première étape de cette méthode est de déterminer l'objet de l'étude. Le choix du cas est un aspect crucial de la recherche, car il représentera son unité d'analyse. Il est donc important de déterminer ce qui sera analysé en premier lieu (Baxter et Jack, 2008). Yin (2003) indique que la délimitation du cas doit se faire à plusieurs niveaux, afin de ne pas viser trop large et de manquer sa cible. Il faut d'abord limiter l'aspect spatio-temporel de l'élément étudié, ainsi que la nature de l'objet (Baxter et Jack, 2008). Dans notre cas, par exemple, nous souhaitons étudier les participants à la communauté des cryptomarchés, et leurs réactions suite à deux interventions policières au sein de leur écosystème. Nous limitons donc nos recherches aux sites hébergeant cette communauté, et aux mois suivant les deux interventions à l'étude. Le choix des opérations a également été fait en fonction de l'objectif principal de notre recherche, soit d'orienter nos analyses sur les effets d'interventions innovatrices. Comme expliqué plus haut, la fermeture de la plateforme DeepDotWeb ainsi que l'opération DisrupTor divergent à plusieurs niveaux des interventions traditionnelles.

L'étude de cas est donc une méthode intéressante et pertinente dans une étude comme la nôtre. Le sujet d'étude étant les participants d'une cybercommunauté anonyme et moins accessible, l'étude de cas pourra permettre de comprendre et d'atteindre ce phénomène social (Baxter et Jack, 2008). Il s'agit également d'une stratégie de recherche qui génère la découverte de nouveaux savoirs et permet une compréhension plus développée des réalités sociales à l'étude (Villemagne, 2006). L'observation à partir de l'intérieur permet également une meilleure compréhension des actions et des structures sociales du groupe peu connu, ainsi que des réseaux, des valeurs, et des significations sociales propres à cette communauté (Feagin, Orum et Sjobert, 1991). Compte tenu du rôle passif joué par le chercheur, il se peut cependant que certains détails restent vagues ou mal définis. Il faut s'assurer de ne pas répondre soit même aux questions qui semblent être trop larges ou qui semblent encore posséder peu de réponse satisfaisante (Baxter et Jack, 2008). Il est finalement important de ne pas influencer les analyses par les motivations inhérentes à nos objectifs de recherche, mais plutôt de laisser les réponses et les informations émaner des données cueillies à même le terrain (Baxter et Jack, 2008).

Dans le but de découvrir le plus grand nombre d'éléments portant sur les événements ciblés, notre démarche fut guidée par un processus inductif (Gammelgaard, 2017). Une lecture détaillée de l'ensemble des données recueillies nous a permis de découvrir les différentes catégories des thèmes émergents de notre échantillon. Les données recueillies furent influencées par les outils de collecte utilisés, ainsi que par nos objectifs de recherche, mais, cela sans limiter l'émergence de catégories inattendues.

3. 2. 3 L'approche inductive

Nous avons bâti notre étude à l'aide de l'approche inductive. Lorsqu'une recherche est effectuée avec l'approche inductive, cela implique que le développement des thèmes ne provient pas des intérêts ou des objectifs des chercheurs, mais plutôt des éléments contenus dans les données recueillies (Hadlington et al., 2021; Fereday et Muir-Cochrane, 2006; Zhang et Wildemuth, 2009). Contrairement à l'approche déductive, dont le but principal est de tester la cohérence d'une hypothèse ou d'une théorie grâce aux données recueillies (Martineau et Blais, 2006; Thomas, 2006; Woo, O'Boyle et Spector, 2016), l'approche inductive vise plutôt la découverte des thèmes émanant naturellement des éléments bruts et provenant des sources d'informations consultées (Thomas, 2006; Martineau et Blais, 2006). Cette approche permet également de rassembler de grandes quantités de données en un texte bref et concis (Ritchie, Spencer et O'Connor, 2003), d'établir des liens clairs entre les objectifs identifiés (Woo et al., 2016), et de développer un nouveau modèle ou une nouvelle théorie supportée par les expériences partagées dans les informations amassées (Thomas, 2006).

L'approche inductive présente plusieurs avantages qui justifient son utilisation dans notre étude. D'abord, cette approche implique la lecture attentive et détaillée des données, nous offrant alors l'opportunité de donner un aperçu plus profond des éléments contenus dans notre échantillon (Braun et Clarke, 2006; Fereday et Muir-Cochrane, 2006). Cela ouvre également la porte à une plus grande flexibilité d'interprétation des données, et permet de facilement résumer et souligner les points clés s'y retrouvant, et qui n'auraient éventuellement pas été évidents, parce qu'étant examinés qu'en surface (Braun et Clarke, 2006). Finalement, il s'agit d'une

approche efficace pour les recherches à caractère exploratoire, car elle permet d'étudier des sujets qui sont plus difficiles d'accès ou dont le cadre théorique est moins fréquent dans la littérature (Martineau et Blais, 2006).

Réaliser une étude avec l'approche inductive doit être faite en suivant certaines étapes. Premièrement, les chercheurs doivent se familiariser avec les données recueillies (Hadlington et al., 2021; Ritchie et al., 2003). Nous avons donc entamé notre processus de recherche avec la lecture de chacun des messages identifiés, ligne par ligne, tout en développant un cadre de codes initial. Les données furent lues plusieurs fois, dans le but d'identifier de façon plus précise les différents thèmes s'y retrouvant (Thomas, 2006). Alors que certains thèmes peuvent être évidents et simples, d'autres requièrent plus de réflexion de la part des chercheurs, et peuvent même revêtir un aspect plus symbolique (Ryan et Bernard, 2003). Une fois la familiarisation avec les données complétées, il faut générer un cadre de codification (Braun et Clarke, 2006; Hadlington et al., 2021); nous avons donc procédé à la réflexion sur les codes ressortissants de la lecture des données, afin d'organiser et de développer les thèmes qui seront présentés dans notre étude. La sélection des codes est dirigée grâce à l'identification des répétitions, des similitudes et des différences repérées dans les données (Braun et Clarke, 2006; Ryan et Bernard, 2003). Une discussion entre les deux chercheurs impliqués dans notre étude a permis d'établir un cadre de codes, qui a servi lors du traitement des données. Nous avons ensuite rassemblé les codes en différentes catégories, afin de conceptualiser plus précisément nos thèmes (Hadlington et al., 2021). Une révision de ces thèmes fut également effectuée par les deux chercheurs, afin de les raffiner et d'assurer un accord commun sur leur signification. Les messages provenant de forums de discussion génèrent une grande quantité de données; notre échantillon présentait donc beaucoup de messages non génératifs, et certains thèmes qui ont émergé de cette banque de données n'étaient pas liés aux objectifs centraux de l'étude. Malgré le fait qu'ils furent identifiés, ils furent laissés de côté lors de l'analyse, afin que nous ne gardions que les éléments pertinents (Childs et al., 2020).

3. 2. 4 La subjectivité en méthodologie qualitative

La méthode de recherche utilisée pour cette étude préconise de se laisser guider par la découverte des données, et ainsi laisser émerger les thèmes qui seront utilisés. Cela signifie donc que le chercheur se doit d'être objectif et d'influencer le moins possible les analyses par ses perceptions ou son point de vue personnel. Malgré les efforts investis, affirmer qu'une recherche qualitative puisse être entièrement objective et neutre ne saurait être juste. L'aspect de la subjectivité se retrouve dans chacune des phases de la recherche auxquelles participe le chercheur. Du choix du sujet d'étude jusqu'à l'analyse des données récoltées, le chercheur interprétera ce qui s'offre à lui (Becker, 1998; Ratner, 2002). Même s'il cherche à garder un rôle passif, il partage des liens avec le contexte social qu'il étudie (Ratner, 2002). Il ne peut faire fi de ses valeurs, de ses expériences et de son vécu (Becker, 1998; Ratner, 2002) et, malgré la bonne foi et les prédispositions prises pour en minimiser l'influence, la culture et les connaissances du chercheur auront un impact sur son interprétation et sur ses perceptions des acteurs et du milieu qu'il étudie.

En effet, la recherche qualitative sera toujours une interaction sociale entre le chercheur et son sujet d'étude (Anadòn et Guillemette, 2007). La subjectivité est donc présente dans chacune des étapes de la recherche. Lors du choix du sujet d'étude, le chercheur ne peut omettre totalement ses connaissances théoriques ou ses préjugés personnels. Il se positionne donc d'entrée de jeu par rapport au sujet, avec une approche qui n'est pas totalement neutre, ce qui aura une incidence jusque dans les résultats des analyses (Anadòn et Guillemette, 2007). Il en va de même lors de l'échantillonnage; le chercheur aborde et observe le terrain selon ses connaissances et ses valeurs, notamment lors de la sélection des données et le choix des cas pertinents (Anadòn et Guillemette, 2007). Par défaut, toute recherche qualitative inductive possèdera donc des éléments qui reflèteront certains aspects subjectifs propres au chercheur qui la réalise.

Afin d'amoindrir les impacts que cette subjectivité peut avoir sur l'intégrité et la crédibilité de la recherche, le chercheur peut avoir recours à la réflexivité, soit au processus de réflexion sur ses valeurs, ses perceptions et ses préjugés – bref, sur les éléments susceptibles

d'influencer les résultats et les conclusions de ses analyses (Jootun, Mcghee et Marland, 2009). En d'autres mots, il s'agit de l'exercice de réalisation qu'il n'est pas indépendant de la culture et de la réalité sociale dans lequel son sujet d'étude réside et, par cette réflexion, réalise que certains éléments pourraient influencer sa vision, sa perception et sa compréhension des données lors des analyses de ces dernières (Anadòn et Guillemette, 2007).

Dans la volonté d'offrir une plus grande transparence à notre étude et à nos lecteurs, nous avons donc pris soin de nous soumettre à cet exercice. Notre sujet d'étude étant les interventions policières au sein des cryptomarchés, nous devons nous réfléchir sur nos préjugés et nos perceptions de ces deux groupes. Bien que nous n'ayons appartenu ni à la communauté des forces de l'ordre, ni à la communauté des cryptomarchés, notre cheminement scolaire nous a amené à étudier les mesures de préventions et les stratégies policières parmi divers types de criminalité. Provenant d'un milieu criminologique, nous ne pouvons nier aborder ce projet avec une base théorique, des concepts appris et des valeurs cultivées depuis plusieurs années. Uniquement le choix de notre sujet, soit celui d'étudier les diverses interventions policières, témoigne de notre position de recherche et de nos analyses, orientées vers l'application de la loi et de l'ordre. Donc, malgré les efforts investis pour rester le plus neutre possible lors de la réalisation de chacune des étapes de cette recherche, il est nécessaire que le lecteur soit conscient de cette limite propre à notre étude.

3. 2. 5 Le processus de codification

Une fois les thèmes identifiés et le cadre de codes formé, nous avons procédé à la codification des données. Plusieurs logiciels qualitatifs existent pour appliquer les différents codes aux segments correspondants; dans le cadre de cette étude, ce fut le logiciel QDA Miner qui fut utilisé. En général, la codification d'une base de données regroupant un nombre important d'éléments est effectuée par plus d'un codeur. Ceci est fait dans le but, premièrement, d'augmenter l'efficacité du processus de codification, mais également afin de perfectionner la compréhension des éléments recueillis, d'améliorer l'interprétation des données, et par souci de

garantir un niveau d'intersubjectivité lors du processus (Burla, Knierim, Barth, Liewald, Duetz et Abel, 2008; O'Connor et Joffe, 2020).

Il existe plusieurs façons d'assurer un respect des critères de rigueur scientifique lors de cette étape : la réalisation d'un accord interjuge entre les différents codeurs, la vérification de la compréhension des catégories de codes parmi les chercheurs impliqués, et la vérification des concepts et des thèmes auprès des participants à l'étude (Martineau et Blais, 2006). Dans le cadre de notre étude, il fut impossible d'utiliser cette troisième méthode; les données ayant été recueillies anonymement via des forums de discussion également anonymes, il devenait impossible de discriminer l'opinion des participants.

Pour chacune des deux interventions à l'étude, un accord interjuge fut effectué préalablement au processus de codification des messages. De manière générale, lors de cette étape de la codification, les codeurs retiennent aléatoirement entre 10% et 25% de leur échantillon (O'Connor et Joffe, 2020), qu'ils codifient simultanément. Une fois cette étape effectuée, le logiciel utilisé lors de la codification fournit un indice numérique témoignant de la force de l'accord existant entre les codeurs, en ce qui concerne la définition des codes et l'application de ces derniers sur les différents segments (O'Connor et Joffe, 2020; Gwet, 2015). Dans le cadre de notre étude, les deux codeurs ont utilisé un échantillon de 200 messages pour la fermeture de la plateforme DeepDotWeb, et de 400 messages pour l'opération DisrupTor, tous sélectionnés de façon totalement aléatoire.

L'utilisation de l'accord interjuge permet de démontrer la rigueur et la transparence dont ont fait preuve les chercheurs lors du processus de codification des données (O'Connor et Joffe, 2020; Burla et al., 2008). Un fort accord interjuge permet d'indiquer que le cadre de codes a bien été développé et communique efficacement les thèmes (O'Connor et Joffe, 2020; Hayes et Krippendorff, 2007), ce qui assure la crédibilité des résultats et rend possible l'identification des faiblesses dans le processus de codification. Cela permet également de stimuler le dialogue et la réflexion entre les chercheurs; ils peuvent ainsi discuter des désaccords mis en évidence et des différences de perception rencontrer au niveau de certaines définitions des thèmes (O'Connor et Joffe, 2020; Martineau et Blais, 2006; Burla et al., 2008). Un résultat trop faible ou négatif de

l'accord interjuge indique, cependant, un déséquilibre dans la compréhension des codes, et nécessite une révision de la part des chercheurs participants (O'Connor et Joffe, 2020; Joffe et Yardley, 2003; Burla et al., 2008).

Il existe plusieurs tests qui permettent de mesurer l'indice de fiabilité de l'accord interjuge (Hayes et Krippendorff, 2007), dont le coefficient de Kappa, le coefficient de Gwet et l'alpha de Krippendorff (Gwet, 2015). L'alpha de Krippendorff est le plus populaire et le plus fréquemment utilisé des trois (O'Connor et Joffe, 2020); il fournit une mesure de fiabilité juste, il peut être utilisé peu importe le nombre de codeurs impliqués, peu importe la taille de l'échantillon codé, et n'est pas affecté par la présence de données manquantes (Krippendorff, 2004).

Nous avons d'abord effectué un premier accord interjuge sur les données traitant de l'intervention menant à la fermeture de la plateforme DeepDotWeb. Composé d'un échantillon de 200 messages, ce premier essai fut infructueux; le seuil minimal acceptable de l'alpha de Krippendorff doit se trouver au-dessus de 0,67 (Krippendorff, 2004; Oleinik, Popova, Kirdina et Shatalova, 2014), et ce résultat ne fut pas atteint. Nous avons donc procédé à une analyse des désaccords de codification mis en évidence par le logiciel, afin d'assurer un niveau adéquat dans la compréhension des concepts chez les deux chercheurs. Suite à notre discussion, nous avons sélectionné de façon aléatoire un nouvel échantillon de 200 messages provenant de la banque de données rattachée à la fermeture de DeepDotWeb. Cette deuxième tentative nous a permis d'atteindre un résultat de 0,93, ce qui représente un niveau de fiabilité fort. Un second accord interjuge fut effectué à l'endroit des données récupérées pour l'opération DisrupTor. Un échantillon de 400 messages fut sélectionné de façon aléatoire. En se basant sur le même cadre de codes, nous avons atteint un alpha de Krippendorff de 0,98, ce qui est nettement supérieur au seuil minimal acceptable. Suite à ces deux accords interjuge, nous étions confiants du niveau de fiabilité atteint dans notre processus de codification. Après un dernier examen final des accords et des désaccords entre les chercheurs, réalisé dans le but de garantir une compréhension commune supérieure de la signification de chaque thème, nous avons procédé à la codification de l'ensemble des messages présents dans la banque des données recueillies.

3. 2. 6 Les thèmes

Lors de la réalisation d'une recherche par l'approche inductive, les thèmes émanent naturellement des données recueillies (Hadlington et al., 2021; Fereday et Muir-Cochrane, 2006; Zhang et Wildemuth, 2009). Lors des lectures détaillées et répétées de nos données, nous avons retenu quatre thèmes principaux qui ont servi à guider notre processus de codification et qui ont orienté nos analyses.

Le premier thème exploré est celui des impacts que chacune des interventions policières aura eu sur la perception des participants quant à l'accessibilité et la facilité d'utilisation des plateformes dans le darkweb. Cette facilité d'accès aux cryptomarchés est l'une des principales motivations qui justifient la présence des usagers sur ces sites. Leur configuration d'utilisation conviviale, semblable aux populaires sites de commerce électronique tel qu'eBay et Amazon (Martin, 2014a), et la facilité avec laquelle il est possible d'accéder à un répertoire diversifié de substances de qualité (Martin et al., 2019a) font partie des justifications de leur popularité grandissante. L'abondance d'information qui y est partagée et l'appartenance à une communauté distincte (Martin et al., 2019a), figurent également parmi les raisons d'adhésion aux cryptomarchés pour plusieurs clients et vendeurs. Nous portons donc une attention particulière à la perception d'accessibilité facile aux ressources d'information, tel que les répertoires de liens ou les tutoriels permettant la réalisation facile des activités dans le darkweb, mais également à l'accessibilité aux vendeurs, aux plateformes de marché et aux substances recherchées. Ainsi, nous tentons de déterminer comment est-ce que la fermeture d'une plateforme informative de premier plan, tel que l'était DeepDotWeb, et l'arrestation de plusieurs membres importants de cette communauté, lors de l'opération DisrupTor, a affecté la perception des participants en ce qui concerne l'accessibilité et l'utilisation des cryptomarchés.

En second lieu, nous explorons les impacts qu'ont eus ces deux interventions sur la confiance ressentie par les participants. Dans un environnement où l'anonymat de chacun est requis et où la majorité des activités accomplies sont illégales, il est nécessaire d'établir un système qui permette aux membres d'effectuer leurs activités commerciales sans craindre d'être victime de fraude ou d'arnaque à tout coup (Pace, 2017). C'est d'ailleurs pour cette raison que

différents mécanismes et systèmes, tel que système de régularisation des transactions et les systèmes de réputation, sont mis en place par la communauté (Lorenzo-Dus et Di Cristofaro, 2018). Nous cherchons à comprendre comment ces deux interventions ont affecté la confiance des participants sur deux différents niveaux : d'abord, nous examinons les impacts de ces interventions sur leur confiance envers les autres membres de leur communauté. Nous portons donc attention aux discussions traitant des erreurs de sécurité opérationnelles des membres interpelés. Nous nous attardons ensuite aux discussions traitant de la confiance que les participants semblent avoir envers les technologies et l'infrastructure soutenant les cryptomarchés. Notamment, nous étudions les échanges qui portent sur les vulnérabilités technologiques de l'écosystème telles que perçues par les participants, et sur causes présumées qui pourraient justifier la réussite des interventions policières.

Le troisième thème étudié est celui des impacts que ces interventions ont eus sur la perception qu'ont les participants des cryptomarchés sur les risques encourus lors de la réalisation de leurs activités dans le darkweb. La perception de l'absence de risque est un autre aspect important expliquant les motivations des participants dans leur décision de prendre part aux activités des cryptomarchés. Selon ce que croient ces derniers, ils courent moins de risques d'être victimes de violence de la part de leurs compétiteurs (Martin et al., 2019b; Evangelistaet al., 2018; Martin, 2014a; DiPiero, 2017) et d'être détectés par les forces de l'ordre dans le darkweb que lorsqu'ils effectuent leurs activités dans la rue (Martin, 2014a). Nous tentons de comprendre comment la disparition de la plateforme DeepDotWeb, ainsi que l'annonce de l'arrestation de 179 membres auront affecté cette perception de sécurité partagée par les participants. Nous étudions d'abord leur perception des risques encourus individuellement, tels que les risques d'identification et d'arrestation. Nous portons également attention à la nature des risques perçus – soit internes ou externes – suite à chacune des interventions policières. Finalement, nous analysons les discussions portant sur les sanctions possibles et attendues après chacun des événements.

Le dernier thème étudié porte sur les réactions des participants. Lors de la lecture des données, nous avons identifié trois réactions différentes discutées par les participants. Certains ont indiqué leur intention de délaisser leurs activités et quitter tout simplement l'environnement

des cryptomarchés. À cet effet, nous portons attention aux différentes motivations énoncées par les participants ayant fait ce choix. Les déplacements spatiaux des activités par les participants, ainsi que les adaptations et innovations possibles dans le quotidien des usagers sont également observés. En effet, les messages étudiés démontrent la volonté de plusieurs de simplement déplacer leurs activités ailleurs, soit en cherchant d'autres sources d'informations ou d'autres vendeurs. De plus, une partie importante des discussions observées traitent des adaptations et des innovations possibles afin de rendre l'écosystème plus sécuritaire, et ainsi éviter les dommages causés par les interventions policières. Nous cherchons finalement à comprendre les impressions des membres vis-à-vis les nombreuses suggestions émises pour fortifier l'infrastructure, et en quoi l'application de ces nouveaux mécanismes pourrait affecter la réalisation de leurs activités quotidiennes.

Chapitre 4 : Les résultats

Dans la section qui suit, nous discuterons des résultats obtenus suite à l'analyse de nos données. Ils seront présentés en quatre parties distinctes, chacune d'entre elles correspondant à l'un des thèmes présentés ci-haut.

4. 1 Facilité d'accès et d'utilisation des cryptomarchés

La facilité d'accès et d'utilisation des plateformes des cryptomarchés est l'un des principaux avantages justifiant leur popularité grandissante; la facilité d'atteindre un répertoire diversifié de substances de qualité (Evangelista et al., 2018; Martin et al., 2019a; Bancroft et Reid, 2016) sans même bouger de son domicile continue d'en attirer plusieurs. La possibilité de toucher un revenu intéressant tout en réalisant des transactions qui demandent peu d'effort motive également plusieurs vendeurs participant aux échanges via ces plateformes (Martin et al., 2019a). La perte d'une plateforme tel que DeepDotWeb, qui servait principalement à guider et aider les participants dans la réalisation de leurs activités au sein de l'écosystème, semble avoir causé divers impacts dans la perception des membres quant à l'accessibilité des ressources et la facilité d'utilisation des plateformes. Tout d'abord, certains soulignent le fait que la fermeture de la plateforme est, d'abord et avant tout, une stratégie pour entraver le partage d'information au sein des cryptomarchés. Ils prétendent faire face à une guerre à l'information, à la connaissance et à la liberté d'expression, laissant sous-entendre que le but des forces de l'ordre est plus complexe que simplement faire disparaître une plateforme facilitant la vente de produits illicites.

> "[...] Ce n'est pas seulement une guerre contre la drogue, c'est une guerre contre la liberté de parole et d'expression. La liberté de poursuivre la connaissance et la liberté d'avoir une vie privée de base. […] N'oublions pas que le réseau Tor a été créé dans le but de lutter contre la tyrannie et l'oppression. Il est important que nous protégions cette communauté et que nous l'améliorions. C'est tout ce qui fait obstacle à ceux qui veulent contrôle ce que nous savons et ce que nous disons. Le

> fait qu'ils se battent si fort contre cela montre exactement ce en quoi ils croient. Cela montre également que cet outil est plus puissant qu'on ne le pense parce que les tyrans de ce monde ne l'aiment pas, mais ils le craignent. […]"
> B**********h

> "[...] Et c'est pourquoi ils font de petits gestes comme saisir un site d'actualités légitime pour exprimer sa liberté d'expression, ou attaquent constamment les échanges légitimes et les commerçants de cryptomonnaie qui essaient de se comporter selon les normes acceptées dans des choses comme le commerce boursier, parce qu'ils savent qu'ils aident l'infrastructure de l'économie sur laquelle nous comptons pour faire des affaires. La plupart du temps, ils ne peuvent pas toucher les gens ici qui commettent des crimes réels parce qu'ils se protègent, alors ils s'en prennent à ceux qui ne ressentent pas le besoin de se cacher parce qu'ils croient qu'ils font quelque chose de légitime et tout à fait décent [...]"
> B**********h

Ces propos sont appuyés par les messages de plusieurs autres membres, qui expriment les impacts que la perte d'une ressource d'information tel que DeepDotWeb a sur la poursuite et le maintien de leurs activités dans les cryptomarchés. En plus de diriger les usagers en toute sécurité vers les nombreuses plateformes actives dans l'écosystème, DeepDotWeb fournissait également l'information au sujet de l'état d'activité des différents sites. La perte de cette ressource semble causer des difficultés aux membres qui tentent d'accéder aux différents marchés. Plusieurs membres indiquent être à la recherche d'une source alternative qui pourrait leur permettre d'accéder aux URL sûrs, et ainsi naviguer dans l'écosystème sans tracas. De nombreuses suggestions publiées par les participants les dirigent vers des plateformes ayant une utilité similaire à DeepDotWeb, alors que d'autres préconisent des stratégies de sauvegarde de liens valides et de recherches sécuritaires. Devant ce nombre limité d'alternatives, cependant, certains membres expriment leur crainte de voir le peu de ressource toujours active disparaître à leur tour et évoquent la nécessité de développer d'autres ressources pouvant remplir le même rôle.

"Alors, où pouvons-nous obtenir l'adresse des sites maintenant? Certains marchés sont encore actifs."
i******************4

"S'IL VOUS PLAIT, EST-CE QUE QUELQU'UN PEUT M'AIDER AVEC UN NOUVEAU SITE QUI FONCTIONNE COMME www.deepdotweb.com??"
D*********o

"Bien, je vais les trouver comme je le faisais dans le vieux DNM reddit et ***….en fouillant dans les forums."
M******2

Les participants dénotent plusieurs impacts que la fermeture de DeepDotWeb a eus sur leurs activités dans les cryptomarchés. D'abord, ils disent que l'accès aux différents marchés s'est complexifié davantage, et ils dénotent également un ralentissement des activités économiques sur les plateformes. Certains semblent mécontents des efforts et du temps supplémentaires nécessaires pour atteindre les différents sites.

"Littéralement en manque d'alternative de marché, c'est fou. Imaginez si Dread était saisi ou n'importe quoi, ce serait comme si le deepnet faisait un bon 10 ans dans le passé"
L**********e

"Et je n'ai jamais eu de problèmes, mais avec la suppression de deepdotweb et les attaques DDoS, c'est tellement capricieux. Il faut littéralement passer en revue chaque détail. Je suis généralement très prudent, et je viens vraiment de m****r ici. Tout change et je n'utilise plus autant les marchés qu'avant."
p*********4

Finalement, la plateforme DeepDotWeb était également reconnue pour ses publications servant de tutoriels, ainsi que le partage de capital criminel effectué par ses usagers. De nombreux membres se référaient à cette ressource, autant les débutants cherchant à en apprendre plus le fonctionnement des cryptomarchés, que ceux possédants de plus faibles capacités informatiques à la recherche de conseils pour améliorer leur sécurité opérationnelle. La perte d'accès à ces informations a fait réagir de nombreux participants, qui indiquent se sentir perdus lorsqu'ils ont besoin d'aide. D'autres témoignent se sentir exposés aux différents risques et individus mal intentionnés présents dans l'écosystème.

> "Ils ont supprimé deepdotweb parce qu'il s'agissait de LA passerelle permettant au joe moyen d'accéder aux marchés, en fournissant des liens, de l'information sur comment accéder aux marchés et en donnant des conseils de sécurité opérationnelle tout en un. Je ne suis pas d'accord avec la fermeture, mais de leur perspective il s'agit d'une cible logique. Ça a définitivement cause du chaos et rendu plus difficile pour les débutants de retrouver leur chemin dans les DNM. Honnêtement, c'était une plus grosse fermeture que n'importe quel marché."
> B********r

L'opération DisrupTor semble également avoir perturbé la facilité qu'ont les participants à accéder et utiliser les cryptomarchés. Ces impacts sont cependant de différente nature, et semblent être d'importance moindre, en comparaison avec ce qui a pu être observé suite à la fermeture de la plateforme DeepDotWeb. D'abord, l'arrestation des 179 vendeurs dans l'écosystème a perturbé la compétition présente parmi les vendeurs; en réduisant le nombre de vendeurs actifs, les membres ont perçu une moins grande distribution des actifs à travers les marchés, et ils disent percevoir un impact sur les activités commerciales des cryptomarchés. Certains indiquent avoir remarqué une stagnation des prix, alors que d'autres témoignent d'une hausse des coûts reliés à leur marchandise.

“tous les revendeurs qui ne se sont pas fait arrêter ont juste augmenté leurs prix et accaparé un peu plus leur marché respectif depuis que le DOJ a éliminé leurs concurrents.”
Z**********r

“L’ajout de risque signifie une hausse des prix. Ils contrôlent le trafic international des drogues”
R**********2

L’opération DisrupTor a également compliqué l’accès des clients à leur vendeur. Suite à l’annonce des arrestations, de nombreux clients ont tenté de retrouver leur contact habituel. Ils sont nombreux qui ont tenté de savoir si leur vendeur faisait partie des usagers arrêtés, et ils ont partagé dans l’espoir d’obtenir plus d’informations sur leur état. Dans les commentaires discutant de la perte d’un vendeur, certains clients témoignent leur déception de perdre un contact de qualité, et tentent de trouver remplacement. Plusieurs membres ne savent pas où aller ni vers quelle ressource se diriger; ils se tournent donc vers la communauté pour trouver de nouvelles options, qui s’avèrent cependant être limitées et insatisfaisantes pour plusieurs.

“Il y a un article tout frais de BBC et Europol d’il y a quelques minutes, qui dit que trois vendeurs autrichiens ont été attrapés. Je me demande lesquels [...]”
_******r

“Je me **** encore dessus en vérifiant si quelqu’un sur qui je dépends fait partie des arrêtés.”
J*****z

“NeverPressedRX a malheureusement été arrêté après n’avoir donné rien d’autre que des produits pharmaceutiques légaux pour un moment déjà ... est ce que quelqu’un aurait d’autres solides vendeurs d’alprazolam? [...]”
g*********p

La disparition d'un grand nombre de vendeurs actifs a également eu un impact sur l'accès à la marchandise dans les cryptomarchés. Les usagers indiquent que les vendeurs ciblés étaient majoritairement vendeurs d'opioïdes, et les participants consommateurs de ces substances consommateurs de ces substances remarquent la difficulté d'accéder à leurs substances habituelles, et dénoncent une qualité inférieure lorsqu'ils réussissent à s'en procurer. Alors que certains membres décrient le fait de cibler en particulier une sorte de substance comme étant une atteinte au droit du libre choix du consommateur, d'autres semblent être en accord avec la situation, car ils jugent que les opioïdes produisent plus de dommages aux consommateurs que les autres substances.

> "Apparemment, une sécheresse s'en vient"
> m**********s

> "en partie vrai, mais la plupart des raids ciblaient des vendeurs d'opioïdes. Vraiment important de s'en débarrasser, ils tuent des tonnes de gens sans aucun égard"
> b**********8

> "qu'est-ce qui est arrive aux dnm [...]. Je comprends l'interdiction du fentanyl afin qu'ils ne soient pas fermés, mais tout message qui pose des questions sur le sujet est reçu par une gang d'adolescents qui répondent hurr durr c'est dangereux on sait, merci. si je ne peux pas en acheter, je vais apprendre comment en faire [...]"
> t****p

4. 2 Les impacts sur la confiance des membres

La confiance, dans un écosystème où l'anonymat règne, est cruciale pour le succès et la survie à long terme des différentes plateformes (Pace, 2017). C'est pour cette raison que certains mécanismes permettant une régularisation des transactions, tel un système de réputation des membres, ont été mis en place (Lorenzo-Dus et Di Cristofaro, 2018). Les commentaires partagés

par les participants traitant des impacts que ces opérations ont eus sur leur confiance envers les cryptomarchés ont été séparés en deux tendances distinctes. D'abord, nous avons remarqué qu'une partie des commentaires discutaient des impacts sur la confiance des participants envers leur communauté et les autres membres. Ensuite, nombreux ont partagés leurs impressions sur la confiance allouée à l'infrastructure des cryptomarchés et son avenir.

4. 2. 1 Confiance envers la communauté

La plateforme DeepDotWeb procurait à ses usagers des liens sûrs, qui avaient pour but d'abaisser les risques de tomber sur des liens frauduleux. De nombreux usagers se fiaient donc à cette ressource et accédaient aux liens publiés sur la page, sans procéder aux vérifications eux-mêmes. La fermeture de la plateforme força donc les participants à valider les liens par leurs propres moyens. De nombreux membres ont indiqué ne pas avoir les connaissances pour le faire, ou encore ne pas avoir l'envie d'y investir les efforts – ils sont donc plusieurs à avouer utiliser des liens non validés. Plusieurs individus au sein de la communauté ont vu cette situation comme une opportunité de soutirer de l'argent aux autres membres, et une hausse des liens d'hameçonnage et de fraude a été remarquée. Alors que certains participants indiquent être récemment devenus victimes d'hameçonnage, d'autres caractérisent l'écosystème comme étant devenu « le paradis de la fraude ».

> "Faites la double vérification de vos domaines Onion. Étant donné que le .onion moyen ressemble à quelque chose comme 7aj5bhidezdbb4ov (il s'agit de celui du marché Empire au moment de la publication), il est facile pour un doigt maladroit ou un lien de phishing d'ajouter un caractère faux vers un site semblable qui va garder votre crypto et vous expédiera la racine carrée de zéro à votre porte. En raison du retrait du site de nouvelles Deepdotweb plus tôt cette année, il ne reste plus beaucoup de guides DNM fiables dans le clearnet […]"
> K*****e

“Ouais, les fédéraux ont saisi AB, Agora, yellow, etc. Mais ddw était différent. C’est comme si la version Darknet de CNN était supprimée. Et ils ont survécu à beaucoup de ddos, sauf celui-ci. Phishers Paradise comme vous dites, tout le monde devrait faire profil bas pendant des mois, je crois. Et n’utilisez pas les liens d’hameçonnage ou les liens des feds qui seront mis ici. Et si l’un d’entre vous obtenez un lien miroir légitime ou un lien vers un marché sous peu, ne le partagez pas ici, parce que les feds et les phishers sont sur ce subreddit comme du blanc sur du riz en ce moment.”

g*********g

Ce phénomène semble avoir eu un impact négatif sur la confiance qu’ont les participants envers les membres de leur propre communauté. Certains font même la promotion du mantra « ne crois personne », indiquant dans leurs commentaires que n’importe quel usager des cryptomarchés peut être malhonnête. D’autres restent cependant plus optimistes, et encouragent la communauté à se serrer les coudes, notamment en partageant avec d’autres membres des plateformes proposant des répertoires de liens sécuritaires ou en encourageant les membres à faire eux-mêmes leur vérification.

“Propager le message N’AIE CONFIANCE EN PERSONNE est toxique pour la communauté, c’est comme dans la vraie vie, il faut faire ses recherches sur les personnes avec qui vous faites affaire. Est-ce que ce sont des personnes de confiance qui sont responsables, prenez cela en considération et faites votre choix […]”

W**********s

“Personne n’est digne de confiance sur le DN, la m**** est pognée”

D******r

Finalement, plusieurs commentaires pointent vers les administrateurs des plateformes. Selon les participants, les administrateurs de DeepDotWeb pratiquaient de mauvaises habitudes de sécurité opérationnelle, et c'est pour cela qu'ils auraient été attrapés. Certains pensent que les administrateurs d'autres plateformes auraient la même attitude, ce qui mettrait à risque non seulement la plateforme pour laquelle ils travaillent, mais les usagers qui la fréquentent également. Les participants partagent ne pas leur faire entièrement confiance.

> "Il y a aussi les publicités, et n'ont-ils pas utilisé des mixeurs? Et maintenant que leurs emails/logs de discussion/PC ont été saisis, qui sait ce qui va apparaître? (Rappelez-vous comment Plutopete a juré qu'il ne vendait que des articles légaux et était parfaitement sécuritaire, et quand il a été perquisitionné, il s'est avéré qu'il avait un tas de drogues personnelles?). DDW n'a jamais fait attention pour rester du bon côté de la ligne."
> g***n

L'opération DisrupTor a également eu des impacts négatifs sur la confiance des participants envers leur communauté. La majorité des commentaires retenus discutent des mauvaises habitudes ou de l'incompétence des membres, qui sont pointés comme éléments responsables des arrestations répétées dans l'écosystème. L'importance de l'utilisation des technologies de cryptage, d'un VPN ou encore les habitudes de manipulation des cryptomonnaies ressortent à plusieurs reprises. De plus, de nombreux commentaires traitent de l'erreur commise de faire confiance aux technologies mises en place par les cryptomarchés pour effectuer les transactions. Selon ces derniers, lorsqu'un marché est renversé ou infiltré par les forces de l'ordre, tous les membres qui n'ont pas pris de mesure supplémentaire que celles établies par la plateforme se retrouvent alors complètement à découvert.

> "As-tu lu ce p***** d'article? Les erreurs d'OpSec?! Il mérite d'être arrêté. Des coins envoyés directement au coinbase...."
> a*****s

> “Si tu utilises correctement le cryptage (et que ton vendeur utilise une OpSec appropriée), ton colis ne devrait pas être identifié comme quelque chose d’inhabituel de toute façon.”
> J*******8

> “Corrige-moi si je me trompe, mais l’utilisation du système de cryptage des marchés est la raison pour laquelle toutes ces arrestations ont lieu?”
> B**********M

Certains participants décrivent la cause des erreurs commises par les membres comme un manque de connaissance. Selon eux, la plupart des membres sont satisfaits des connaissances de base qu’ils possèdent. Ils les accusent même d’être trop paresseux pour combler le manque évident de formation qu’ils ont, les rendant ainsi complètement responsables de leur arrestation.

> “L’ignorance et la paresse, comme tant d’autres choses. Ils ont probablement fait beaucoup d’autres erreurs stupides qui peuvent avoir ou non contribué.”
> V**********n

> “Eh bien, c’est idiot. Tu peux rester anonyme, mais cela demande des connaissances, du temps et de l’argent. Et la plupart des gens n’ont pas les 3. Si tu le fais, il faut aussi de la discipline (la complaisance est énorme). C’est ça. Ils disent que la confidentialité n’est ni bon marché ni facile. Idem avec l’anonymat”
> f****L

Finalement, l’opération DisrupTor semble avoir affecté la confiance des membres envers les vendeurs. D’abord, de nombreux commentaires traitent de la négligence perçue de certains vendeurs. Selon ce qu’avancent certains participants, plusieurs vendeurs conserveraient les données des consommateurs avec qui ils font affaire, non cryptées et à la vue de tous. Ils sont donc réfractaires à l’idée de faire affaire avec de nouveaux vendeurs, par crainte de mettre leur identité à découvert.

“Je pense que la plupart des vendeurs conservent un certain nombre d’adresses. Il faut faire preuve de diligence pour supprimer toutes les informations [...] Nous aimerions penser que nos informations sont supprimées après la finalisation de la transaction, mais la réalité est qu’elles disparaissent rarement complètement.”
b**********t

“Je pensais que les vendeurs supprimaient quand même ces informations si elles sont cryptées ou non? Mon vendeur principal l’indique en grosse majuscule sur sa page NOUS SUPPRIMONS TOUTES LES INFORMATIONS SUR LES CLIENTS LORSQUE LA TRANSACTION EST TERMINÉE”
s*********0

D’autres discutent de l’intégrité des vendeurs, et de comment ces derniers seraient prompts à offrir les informations de leurs clients pour faire diminuer leur peine. Finalement, nombreux sont ceux qui indiquent vouloir éviter tout contact avec un membre qui est dans la mire des forces de l’ordre, par crainte d’être identifié dans la foulée. Une liste énumérant les usagers qui, selon certaines informations, feraient l’objet d’une surveillance policière élevée a d’ailleurs été créée et est partagée dans la communauté, créant du même coup un impact très négatif sur leur réputation.

“ [...] Les vendeurs tiennent des registres. La seule raison de le faire est de réduire le temps en dedans. Surtout aux États-Unis où on obtient beaucoup plus de clémence en livrant les autres. L’histoire de Wired le confirme [...] ”
j**********s

“Toujours une bonne idée d’éviter ce fournisseur si c’est possible. Une fois que le vendeur figure sur la liste des cibles du NCIDETF, il ne tarde pas à joindre la liste des arrêtés”
C*********n

4. 2. 2 Confiance envers l'infrastructure

La fermeture de DeepDotWeb a causé un effet de surprise chez les participants des cryptomarchés. Plusieurs commentaires partagés témoignent du choc et de l'inquiétude générés parmi les membres de la communauté. Les usagers partagent leur surprise quant au fait qu'une plateforme et ses activités puissent être considérées comme étant criminelles, et sa disparition rappelle aux membres que l'infrastructure dans laquelle reposent les cryptomarchés est fragile et vulnérable.

> "C'est un précédent inquiétant. Je n'ai jamais entendu parler d'arrestation pour avoir partagé des liens de site web avant"
> O**********r

> "J'imagine qu'on oublie tous comment tout cela est fragile. et on se le fait rappeler quand la m**** prend."
> T********l

La perte d'une ressource tel que DeepDotWeb semble avoir déstabilisé la communauté et créé un climat de méfiance envers l'écosystème. Plusieurs disent se tourner désormais vers les forums lorsqu'ils sont à la recherche d'informations, mais ils indiquent ne pas toujours avoir confiance en ce que les membres y écrivent. Les liens frauduleux et d'hameçonnage sont de plus en plus présents, et les membres hésitent à utiliser les ressources alternatives à DeepDotWeb. La combinaison de la disparition de DeepDotWeb, des fermetures récentes de plusieurs cryptomarchés et de la présence accentuée d'usagers malintentionnés semble avoir ébranlé la confiance des usagers envers leur écosystème en général.

> "Toutes ces fermetures et ces fraudes vont me faire exploser. comme, même avoir le culot de fermer DeepDotWeb… et aujourd'hui j'ai découvert que la CIA a créé son propre site .onion… wtf… plus rien ne semble sécuritaire à présent"
> L******u

“Peut-être que je descends dans la paranoïa, mais les problèmes de ddos avec tor, ça ressemble à une coïncidence, et je crois que ça rend plus facile le démasquage des adresses IP et des trafics. Ça me semble comme une géante opération combinant plusieurs forces policières. Je m’attends à beaucoup plus d’histoires dramatiques avec l’arrivée des nouvelles plateformes et une abondance d’exit scam et d’arrestations, restez prudents et videz vos maisons, juste en cas, faites-le!”
D********z

Plusieurs usagers se demandent donc à quel avenir s’exposent les cryptomarchés, et le discours partagé semble être pessimiste. L’instabilité de l’écosystème, les fréquentes attaques DDOS menées contre de nombreuses plateformes, et la disparition volontaire récentes de certains sites laissent entrevoir un affaiblissement de l’infrastructure. Ils perçoivent la fermeture de DeepDotWeb comme un pas supplémentaire dans cette direction. La perte de cette importante ressource, qui servait également de lieu de rassemblement pour la communauté, semble avoir ébranlé la confiance de ses membres quant à sa capacité de subsister dans l’avenir.

"Aujourd’hui est un jour triste pour les dnms et leur futur! Merci deepdotweb pour tout!”
B***************5

“Il s’agit de la perturbation la plus importante de la part des agences d’application de la loi à ce jour, a déclaré le procureur américain Scott W. Brady. Bien qu’il y ait déjà eu des réussites contre divers marchés du Darknet, cette intervention est la première à s’attaquer à l’infrastructure prenant charge du Darkweb lui-même. Tal Prihar et Michael Phan auraient possédé et exploité DDW […] Yo, les Américains doivent être mis en échec… ça devient ridicule. Le darkweb va souffrir dans les prochains mois. Je parie que c’est le début d’un long processus et ils vont ramasser beaucoup de monde pendant tout ça”
D********3

Alors qu'une partie des usagers semble blâmer l'incompétence et la paresse des membres pour l'opération DisrupTor, d'autres partagent leur inquiétude face à l'infrastructure technologique soutenant l'écosystème. Selon ces derniers, les vulnérabilités technologiques de TOR pourraient être responsables d'une perte de garantie d'anonymat des utilisateurs appréhendés. Alors que certains pointent les lacunes importantes dans l'étanchéité et la sécurité du réseau, d'autres se rabattent sur l'origine de TOR, créé originalement par le gouvernement américain, et disent croire que les forces de l'ordre pourraient l'avoir infiltré depuis le début. La cryptomonnaie Bitcoin et ses services de « mixage » sont également pointés comme cause potentielle de l'identification des membres arrêtés.

> "Je crois que le dark web est pratiquement juste un gros piège maintenant. Qui est-ce qui a confiance? Tor a très clairement été compromis, ce qui ne devrait pas surprendre personne"
> P**********1

> " TOR a été créé par l'establishment militaire américain. Il a été assez facile pour les autorités de désanonymiser TOR pendant un certain temps déjà, simplement en inondant les nœuds des machines virtuelles, ce qui leur permet essentiellement de déterminer le réseau de nœuds par lequel passent vos échanges, et d'identifier presque tout le monde sur le réseau."
> S**********1

> ""et vos activités anonymes ne sont pas anonymes." Eh bien, duuh, la majorité d'entre eux utilisent encore Bitcoin, le système de paiement le plus transparent jamais inventé..."
> t***d

Finalement, plusieurs membres ont indiqué percevoir que les forces de l'ordre représentent désormais une menace plus sérieuse. Lors de l'opération DisrupTor, elles sont parvenues à mettre la main sur les serveurs du cryptomarché WallStreet Market, et à y retirer les informations permettant l'identification de nombreux participants aux marchés. Cette réussite,

combinée aux récentes opérations menées contre l'écosystème qui sont de plus en plus développées et complexes, fait craindre aux usagers que les forces de l'ordre soient en train de développer leurs compétences et devenir plus efficaces. Ils sont désormais en mesure d'identifier les faiblesses des technologies soutenant l'infrastructure, et de profiter des erreurs des participants des cryptomarchés.

> "Ouais, je suis d'accord qu'ils ne peuvent pas arrêter à 100%, mais je crois qu'ils pourraient certainement augmenter leurs restrictions sur l'importation, sur le processus, ou développer des technologies qui sont davantage orientées vers certaines substances spécifiques (par exemple, peut-être des machines style X-ray qui détectent certaines substances, au lieu de la densité des os). Je ne sais rien sur ce type de techno, mais je crois juste qu'on doit être proches de quelque chose dans le genre."
>
> t**********d

> "Le FBI gère des noeuds compromis depuis des années maintenant. Depuis 2014 environ, je crois."
> n**********t

4. 3 Les impacts sur la perception des risques

Nous avons vu, dans la revue de littérature, que les participants aux cryptomarchés considèrent leur environnement comme étant moins risqué que ce qu'ils affrontent dans le monde physique, et qu'il s'agit là d'une des raisons principales derrière l'utilisation de l'infrastructure du darkweb pour conclure leurs transactions de produits illicites (Aldridge et al. 2018; DiPiero, 2017; Evangelista et al., 2018; Martin, 2014a; Martin et al., 2019a). Les deux opérations à l'étude semblent cependant avoir ébranlé cette perception, notamment en modifiant la perception de l'importance des risques présents à travers les plateformes. Les nombreux partages et questions émis par les participants laissent, en effet, voir une augmentation de leur perception des risques.

4. 3. 1 Perception des risques d'arrestation

Suite à l'annonce de la fermeture de DeepDotWeb et de l'arrestation de ses administrateurs, de nombreux usagers ont indiqué craindre pour leur propre sécurité. La principale inquiétude semble résulter de la possibilité que les forces de l'ordre aient eu accès à l'information personnelle des usagers de la plateforme DeepDotWeb lors de sa saisie, et ils craignent désormais d'être identifiés. D'autres membres mentionnent cependant ne pas être inquiets, car ils n'ont partagé aucune de leurs informations personnelles pour naviguer sur la plateforme, et en profitent pour faire la promotion d'une bonne sécurité opérationnelle.

> "J'utilisais le service de mixage de bitcoin de DeepDotWeb il y a environ un an. est-ce qu'ils préservaient des informations, comme l'adresse de depot pour les bitcoin, les retraits, etc.? Est-ce que je devrais m'inquiéter?"
> T*******e

> "tout d'abord, comment mes informations pourraient-elles en avoir la preuve? 2eme, quelle information quelqu'un a-t-il mis sur DDW qui conduirait les forces de l'ordre à lui? Je n'ai jamais eu à créer un compte sur DDW. Je ne connais personne qui l'ait fait. Et généralement, il ne faut pas donner aucune information personnelle juste pour créer un compte sur un site du deepweb. Donc, je ne vois pas comment le fait que les forces de l'ordre aient supprimé DDW pourrait affecter les utilisateurs le moins du monde"
> A*****0

D'autres membres disent percevoir le partage d'information sur les forums sous un nouvel angle. Suite à l'arrestation des administrateurs d'une plateforme dédiée au partage d'information et d'actualité tel que DeepDotWeb, ils se demandent si participer à de telles activités les place dans une situation d'illégalité qu'ils n'avaient pas préalablement perçue. Plusieurs disent également être pleinement conscients que les agences d'application de la loi surveillent les sites de discussions et de partage d'informations, et craignent que ce qui y est

partagé ne serve aux forces policières pour mieux sévir contre leur communauté. Ils interviennent donc contre certains usagers qui donnent trop d'information sur leur pratique et sur l'utilisation de technologies dédiées à augmenter leurs stratégies de sécurité opérationnelle.

> "Il faut que dark.fail, les forums, dntrust et tous les autres sites soient mis hors ligne maintenant! Comme ça, les forces de l'ordre n'auront pas de moyen de naviguer dans le deepweb!"
> S*******e

> "Ceci EST exactement le genre d'informations que les agences d'application de la loi recherchent ici. De plus, une discussion trop détaillée entraine des problèmes OpSec pour les vendeurs. Les flics sont comme n'importe qui d'autre. Ils cherchent pour de l'information et l'exploitent. Ils VONT utiliser l'information qu'on leur procure et l'utiliser pour attraper les acheteurs comme ils le peuvent. C'est préférable de ne pas perdre notre avantage en partageant nos savoirs d'OpSec avec les autorités. Content de te faire rire… mais pour certains, ceci est très sérieux.."
> l**********1

Alors que la perception des risques individuels est soulignée à quelques reprises dans les discussions suivant la fermeture de la plateforme DeepDotWeb, il s'agit du principal et quasi exclusif sujet d'inquiétude observé dans les discussions publiées suite à l'annonce de l'opération DisrupTor. De nombreux membres discutent des risques encourus par les différents acteurs actifs dans les cryptomarchés.

D'abord, ils semblent particulièrement inquiets pour les vendeurs, qui sont perçus comme la cible d'intérêt principal des forces de l'ordre. Lorsqu'un vendeur est inactif depuis un certain temps, les usagers se demandent rapidement s'il n'est pas impliqué dans l'une des arrestations de DisrupTor. Ils sont nombreux à spéculer qui seront les prochains à se faire arrêter. Ils sont d'ailleurs nombreux à souligner les absences ou les changements de comportement de certains

vendeurs, indiquant craindre que ces derniers aient été arrêtés ou remplacés par un agent d'infiltration.

> "Juste pour que les gens sachent, ce vendeur ne s'est pas connecté depuis le 7, quelque chose ne va pas, car il y a eu beaucoup de commandes finalisées depuis le 7, toutes de bonnes critiques. Espérons qu'il ne s'est pas fait prendre ou qu'il n'a pas fait une surdose."
> r**********9

> "'J'ai une sorte de mauvais pressentiment sur le fait que fft soit en vacances prolongées."
> m**********e

Les participants semblent également être particulièrement préoccupés par les membres appréhendés qui travaillaient en association avec d'autres vendeurs. Il est courant, dans les cryptomarchés, de voir plusieurs individus derrière un même pseudonyme de vendeur. À l'inverse, un individu peut participer à plusieurs pseudonymes de vendeurs à la fois. Il fut observé à quelques reprises, par les utilisateurs que, malgré le fait qu'un individu ait été arrêté, le pseudonyme derrière lequel il menait ses activités soit toujours actif.

Cette réalité génère donc un bon nombre de commentaires d'individus tentant de relier les différents pseudonymes entre eux, afin d'informer les usagers des membres à éviter. Les membres disent vouloir éviter tout contact avec les pseudonymes étant reliés à un vendeur appréhendé, par peur de se trouver face à face avec un agent des forces de l'ordre. Ils indiquent croire qu'un ou des agents des forces de l'ordre pourraient se faire passer pour le vendeur, et ainsi accéder à un plus grand nombre d'informations et de cibles potentielles. Certains croient que, dans le but d'alléger les conséquences pénales potentielles, des vendeurs pourraient être tentés de dénoncer leurs acolytes et leurs clients. Ainsi, lorsqu'une rumeur concernant un vendeur fraie son chemin dans les discussions, de nombreux membres indiquent vouloir éviter cet individu et ceux avec qui il aurait déjà travaillé. Cette perception de risque pousse également

certains membres à révéler l'identité des vendeurs derrière les pseudonymes, ce qui est contraire à l'une des règles les plus importantes de l'écosystème, soit la préservation de l'anonymat des membres à tout prix.

> "/u/killswitch Je sais que cela devrait être évident, mais je pense que KingCobraXanax, ThePasitheas, XanaxLabs and DrXanax et tous les comptes associés à Arden McCann (Vendeur canadien qui s'est fait arrêter en février dernier) devraient être ajoutés à la liste de vendeurs à éviter. Certaines personnes ne suivent pas DarkNetLive ou les forums de manière constante et pourraient ne pas savoir qu'il faut éviter ces noms."
> C**********n

> "Nolove2323 a débuté sous le pseudo hectorsmom ensuite HectorSalamanca sur Empire pour créer de la confusion et pour tenter et voler le commerce de Hector. 9K a publié cette information il y a quelques mois que nolove2323 est en fait Stealthgod et hectorsmom."
> [supprimé]

> "Beaucoup de gens disent que ce compte avec KingCobraXanax était géré par Arden McCann ou quelqu'un d'autre dans son équipe. Dans tous les cas je dirais à éviter."
> C**********n

> "Je peux nommer quelques vendeurs qui se sont fait prendre, mais qui n'ont jamais été mentionnés. Je ne peux pas dire qui à cause de la règle du semi-doxxing, mais cela n'a jamais été annoncé. "
> B******1

Plusieurs discussions traitent également des risques encourus par les acheteurs. Contrairement aux commentaires partagés après la fermeture de DeepDotWeb, de nombreux individus indiquent se soucier désormais des risques pris par les usagers qui ne sont que clients. Un important nombre de messages publiés traitent des risques encourus par les clients des

vendeurs appréhendés lors de l'opération DisrupTor. De nombreux membres semblent soucieux quant à la préservation de leur anonymat et sont conscients des risques que leurs informations personnelles soient désormais accessibles aux forces de l'ordre.

> " Bruh en tant que vendeur cette m***** me fait vraiment très peur"
> M******h

> " J'ai récemment commandé avec le dernier de la liste. Est-ce que je devrais être inquiet? "
> h*********e

> " F**k off je viens tout juste de donner mon adresse à realxanattitude! "
> C******************t

> " F**k. J'ai commandé de lui souvent. J'ai seulement commandé pour usage personnel. Est-ce qu'il y a quelque chose que je devrais ou ne devrais pas faire? Est-ce que je devrais supprimer mon compte avec Empire? Et est-ce que je devrais éviter de faire livrer à mon adresse dans le futur?"
> 1********1

Les publications recueillies laissent paraître un haut niveau d'inquiétude quant à la participation des membres dans le trafic de substances illicites. De nombreuses interrogations sont émises concernant la quantité de substance requise lors d'une transaction pour faire partie de la liste des membres d'intérêt des forces de l'ordre. En général, les participants estiment que les petits acheteurs sont moins à risque que les acheteurs fréquents et commandant en plus grande quantité.

"Dépend de la taille du client. S'il est dans les petits clients je doute qu'ils aillent après eux. S'ils sont dans les principaux clients, il serait possible selon les informations qu'ils possèdent. Toujours utiliser les outils de cryptage et d'OpSec pour limiter les chances d'être exposé. "
d******5

Le type de drogue acheté fait également sujet de plusieurs discussions. Le niveau d'inquiétude des membres varie selon la nature de la substance achetée. Plusieurs croient que les transactions comportant des substances tel que du fentanyl ou des opioïdes sont plus problématiques que les commandes de marijuana. Ils sont d'avis que les forces de l'ordre se concentrent sur certains types de drogues, à cause de leur potentiel mortel ou dangereux pour la vie des humains. Ils sont donc plusieurs à suggérer d'éviter l'achat de ces substances.

"N'achetez ou ne vendez pas de Fentanyl sur le darknet (Il s'agit de la seule drogue qu'ils ont mentionnée.. apparemment la seule à laquelle ils tiennent)"
w**********s

"Une autre raison de ne pas vendre de drogues dures dans un marché public. Beaucoup d'argent, mais tu as toujours une cible dans ton dos. C'est quand la dernière fois que les psychédéliques classiques ont été ciblés? "
e**********d

4. 3. 2 Risques internes et risques externes

La nature des risques énoncés par les participants diffère d'une intervention à l'autre. Tout d'abord, la fermeture de la plateforme DeepDotWeb semble avoir affecté plus particulièrement la perception de risques internes, soit les risques émanant de l'intérieur de l'écosystème. La perte de cette importante ressource d'information aurait contribué à créer un environnement plus instable et dangereux pour la communauté.

Ainsi, la majorité des messages discutant de la nature des risques encourus par les participants sont donc axés, tout d'abord, sur la présence importante de liens frauduleux et d'hameçonnage. DeepDotWeb n'étant plus présent pour suggérer des liens sécuritaires aux utilisateurs des plateformes, ces derniers se trouvent fréquemment confrontés à des liens frauduleux, sans avoir les connaissances et les outils nécessaires pour les éviter. Plusieurs décrient d'ailleurs avoir été victimes de pertes financières depuis la disparition de la plateforme DeepDotWeb, et ne semblent pas en mesure de trouver d'autres sources efficaces pour les aider à contourner ce risque de plus en plus présent dans l'écosystème.

> "Un de mes amis a perdu son compte après avoir utilisé dak.fail pour des liens. Il a seulement perdu moins de 10$, mais il n'est pas le seul dont j'ai entendu parler. "
> H******t

La nature des risques perçus suite à l'annonce de l'opération DisrupTor est plutôt orientée vers les risques externes, soit ceux provenant de l'extérieur de l'écosystème des cryptomarchés; les risques d'appréhension, d'arrestation et d'identification, par exemple.

> "Il semble que les seules nouvelles disponibles actuellement parlent de personnes qui se font arrêter. "
> J*****z

L'un des aspects le plus souvent mentionnés par les participants concerne la menace qui plane sur la préservation de leur anonymat. L'anonymat des membres est un élément essentiel des cryptomarchés. Les identifications et arrestations de plusieurs membres de la communauté par les forces policières font donc craindre aux participants que leur anonymat ne soit plus garanti par l'infrastructure et ses technologies. Certains indiquent même que cette opération n'est pas une guerre contre la drogue, mais contre leur droit à l'anonymat et à la vie privée, deux valeurs importantes pour la communauté regroupant les participants des cryptomarchés.

> "Ces arrestations ne sont pas une guerre contre la drogue. Ceci est une guerre contre l'anonymat. Apprenez à chasser les criminels, puis allez chasser les activistes. "
> D*********l

> "Et c'est la fin les amis. L'anonymat est mort. Des fois je suis nostalgique des années 2000 où l'internet comme tout le reste était beaucoup plus décentralisé, les sites web avaient leur propre forum et le dark web était inconnu de la majorité. Avec l'étendue de l'internet, les sous-cultures ont été déjouées. Engagez-vous dans les MAUVAISES CHOSES et non seulement vous serez doxxé par l'état, mais cela vous assurera également de ne jamais avoir de compte bancaire. "
> f***k

4. 3. 3 Certitude et sévérité des sanctions

Finalement, plusieurs discussions recueillies traitaient des sanctions potentielles auxquelles feraient face les participants ayant été appréhendés par les forces de l'ordre. Suite à la fermeture de DeepDotWeb, plusieurs questionnements ont surgi dans les discussions, portant d'abord sur la certitude de voir des sanctions pénales attribuées aux individus arrêtés suite à leur implication dans la vente de substances illicites dans les cryptomarchés. L'augmentation des opérations policières, qui ont mené à des arrestations et des fermetures de plateformes au cours des dernières années, semble être un élément qui entraîne l'augmentation de cette certitude de

sanction pour plusieurs individus. Certains indiquent même croire que certains administrateurs de marché ont préféré quitter leurs fonctions, ou encore volontairement ralentir leurs activités, afin d'éviter d'attirer l'attention des forces de l'ordre envers eux, et ainsi diminuer les risques de sanction.

> "C'est vraiment facile de critiquer quelqu'un d'autre quand ce n'est pas votre liberté et votre bien-être qui sont en jeu. Je serais certainement d'accord pour dire que certaines décisions différentes auraient pu être prises pour attirer moins d'attention et de chaleur sur CGMC, mais je ne peux pas blâmer les administrateurs d'être en sécurité. Autant ça craint que CGMC ferme, je préfèrerais que les gens derrière soient en sécurité pour le potentiel d'un retour ou quelque chose de mieux à l'avenir que de lire sur plus de gens qui se font arrêter pour des choses inoffensives"
> j*********n

> "Un autre scénario probable pour leur absence est qu'ils veulent rester petits. Nous avons vu que les grands marchés sont les cibles principales des LE. Peut-être qu'ils attendent qu'un marché prenne le rôle de marché principal et évite ainsi l'attention."
> M**********r

Malgré la disparition de la plateforme DeepDotWeb, les participants n'occupant qu'un rôle d'acheteur dans l'écosystème continuent à percevoir leur situation personnelle comme étant peu risquée. Ils indiquent ne pas se sentir particulièrement en danger, tout en soulignant les diverses conditions pouvant contribuer à augmenter leurs risques d'arrestation. Ils ne se sentent pas préoccupés par l'intervention des forces de l'ordre à leur égard, mais sont plutôt concentrés sur les nombreux risques internes présents dans l'écosystème.

> “[…] Donc, même si ton fournisseur est arrêté, la probabilité qu’il puisse obtenir ton adresse ou informations personnelles est TRÈS faible, d’autant plus que la plupart des fournisseurs supprimeront automatiquement les informations d’expédition après l’envoi des colis (c’est principalement pour leur propre protection, les autorités peuvent passer une commande et avoir la preuve concrète qu’il est un vendeur s’ils trouvent l’adresse enregistrée quelque part sur l’ordinateur de cette personne).”
> c********l

> “Oui, la plupart des acheteurs identifiés en masse sur Hansa n’ont pas été arrêtés. La police s’est juste contentée de dire bonjour et de leur demander s’ils ont eu quelque chose de bon sur le dark web ces derniers temps. Essentiellement effrayer les gens.”
> M**********r

Les réactions observées suite à l’annonce de l’opération DisrupTor diffèrent à ce niveau; les individus ne discutent plus de la certitude d’une éventuelle sanction, ils discutent plutôt de la sévérité que revêtira la sanction imposée aux individus appréhendés. Les commentaires portent notamment sur les années d’emprisonnement qui seront attribuées aux différents membres arrêtés, ainsi que sur les facteurs aggravants, tel que le type de substance vendue, ainsi que le rôle joué par l’usager. Selon les commentaires partagés, être administrateur de plateforme résulterait en une sanction supérieure à celle d’un simple vendeur.

> “Et ils ont été royalement cassés avec des peines s’étendant sur des décennies... ou vous avez oublié? Oui, ils étaient un peu bâclés, mais on pourrait penser que leurs marchandises attireraient moins l’attention – du moins c’était l’hypothèse. Ça s’est avéré être une fausse prémisse et maintenant plusieurs d’entre eux sont en prison pour la majorité de leur jeune vie”
> N***** **y

> “J’espère qu’il a été assez intelligent pour cacher certains comptes ou acquérir des biens au nom de la famille et des amis proches. La partie fentanyl et opioïdes va lui faire passer beaucoup de temps en dedans. ”
> [supprimé]

> “Un moment donné, personne ne voudra risquer d’être un administrateur de marché. On parle de prison à vie comme punition, et les autorités ne font que s’améliorer pour traquer ces gars. Il en va de même pour les vendeurs... non seulement ils sont sujets aux fluctuations cryptographiques en attendant le passage du paiement dans le système d’escrow, ils doivent également s’inquiéter des fraudes de sortie et également de se faire arrêter et faire face à des dizaines d’années en prison. ”
> j**********n

Finalement, certains membres discutent des bénéfices escomptés pour la participation aux cryptomarchés, et des coûts potentiels que cela implique. Selon eux, la certitude et la sévérité des peines encourues ne valent pas les bénéfices venant avec les rôles de vendeurs et d’administrateurs, et soulignent le manque de rationalité derrière cette décision.

> “ Je ne suis pas sûr que vendre et envoyer des drogues à des clients ait jamais été un bon travail à tenter. Les expéditions de drogues “en gros” peut-être, mais vendre à des clients uniques a toujours été trop risqué pour l’argent qu’il y a à faire là. On ne devrait pas assumer que les gens embarquent dans une business parce que c’est la chose rationnelle à faire. Ils voient les gains à court terme, non les risques à long terme.”
> d***4

4. 4 Les réactions des participants

Ces deux interventions policières ont dérangé la communauté des cryptomarchés, et ont généré du mouvement parmi les participants. Trois types distincts de réactions furent observées : alors qu'une minorité a évoqué l'intention de cesser toute activité au sein des cryptomarchés, d'autres ont discuté des divers déplacements et adaptations possibles afin de poursuivre leur parcours dans le darkweb.

4. 4. 1 Abandon des activités

Suite à la fermeture de la plateforme DeepDotWeb, certains membres ont évoqué leur intention de cesser leurs activités illicites sur le web, en effectuant un retour vers le trafic de biens illicites dans la rue. D'autres ont cependant indiqué se retirer temporairement, sans mentionner l'intention de se tourner vers d'autres alternatives pour maintenir leurs habitudes de consommation.

> "Trop stupide. On dirait qu'on va devoir retourner aux drogues de la rue"
> [supprimé]

> "LOL je retourne dans la rue. Je suis dans ton coin en ce moment."
> s**********h

> "Restez discrets pour un moment les gars. Augmentez votre OpSec aussi. Nous sommes dans des temps sombres maintenant."
> i*******y

Les membres ont évoqué plusieurs raisons motivant l'abandon des cryptomarchés. D'abord, un sentiment de risque est partagé par plusieurs. Certains expriment leur réticence à participer au partage d'information, par crainte de subir le même sort que les administrateurs de DeepDotWeb. La prolifération des liens d'hameçonnage et de fraudes, ainsi que la possibilité d'interpellation par les forces de l'ordre, figure également parmi les raisons évoquées par les

usagers. La complexité de l'utilisation sécuritaire des cryptomarchés, qui permettrait d'éviter d'être exposé à tous ces risques, est également la source de découragement de certains.

> "Le moment est vraiment venu où l'infrastructure du Deepweb est détruite au point où nous ne pouvons même plus partager de l'information. La plupart des marchés sont fermés, et c'est risqué de faire n'importe quoi parce que qui sait quel marché ou site va être le prochain à être saisi (et tous les achats de leurs utilisateurs et potentiellement des informations seront divulguées aux autorités fédérales)"
>
> L**********e

> "Je suis nouveau dans le jeu, mais je ne peux pas m'empêcher de me demander pourquoi les gens continuent d'utiliser ces marchés s'il est si facile de se faire hameçonner"
>
> O*****s

> "Je suis out des DNM pour l'instant cette m****e est trop deepdotweb WS et Dream ont été saisis par Europol et le FBI etc. Premier à confirmer que c'est un jour triste de se dire que les DNM sont en quelque sorte finis […] cordialement JR"
>
> J**********e

L'opération DisrupTor a également été la source de réactions de la sorte; certains commentaires émis par les participants témoignent de leur intention de délaisser leurs activités au sein des cryptomarchés, suite aux arrestations récentes. Les raisons invoquées pour justifier les raisons de leur départ sont multiples. D'abord, ils sont plusieurs à signifier les risques perçus entourant les activités dans les cryptomarchés. Ils indiquent ressentir plus d'anxiété et de crainte face aux risques d'arrestation qu'ils considèrent comme plus présents. D'autres indiquent que les tactiques et techniques utilisées par les forces de l'ordre ont été développées et perfectionnées dernièrement, et qu'elles plus efficaces. L'opération a créé une onde de choc au sein de la communauté. Les nombreuses arrestations de vendeurs connus et importants, ainsi que

l'accumulation des opérations d'envergure qui ont eu lieu dans les dernières années, commencent à faire peur aux usagers, qui préfèrent quitter l'écosystème plutôt que de se faire attraper.

> "Oui, j'ai posté dans un autre échange, mais c'est trop pour le moment, Je ne suis pas junkie en ce moment, et je n'ai pas besoin de tout risquer juste pour me fournir. Ce site qui ferme, les arrestations, Ava qui disparaît, probablement arrêtée, drugpharmacist arrêté, sinmed (peu importe qui il était, jamais entendu parlé) est arrêté. Il y en a d'autres et c'est bien trop dessiné et le timing n'est pas cool et tout. Mon conseil (de quelqu'un qui existe depuis l'original Silk Road), cessez si vous pouvez. Laissez quelqu'un d'autre prendre des risques pour le moment."
>
> d***4

> "[...] Les autorités fédérales commencent à utiliser davantage de ressources en ce qui concerne les ventes en ligne DNM (réception des livraisons, empreintes digitales sur l'emballage, adresses de retour suspectes... ETC). C'est pourquoi vous voyez beaucoup de bons vendeurs disparaître (partir en vacances) à l'improviste – malheureusement."
>
> m**********e

Quelques membres évoquent également l'instabilité de l'écosystème, ainsi que de la complexité d'utilisation grandissante comme motif justifiant leur l'abandon des cryptomarchés. Les arrestations répétées de vendeurs de confiance pour plusieurs clients ont généré une perte de repère et de confort, et les forcent à se tourner vers des inconnus et prendre le risque d'obtenir un service de moins bonne qualité. L'effort supplémentaire à effectuer pour se trouver de nouveaux vendeurs, ainsi que les contraintes des mesures et des technologies implantées pour contrecarrer les tentatives de perturbation des forces policières semblent décourager les membres. Plusieurs partagent que ces ajouts compliquent l'accès aux cryptomarchés et les rendent moins attrayants. Certains indiquent ne pas être en mesure de suivre ces développements technologiques, qui sont

devenus trop complexes pour leurs capacités, alors que d'autres indiquent plutôt ne pas être intéressés à y investir le temps et les efforts, et préfèrent mettre fin à leurs activités.

> "Ouais, je pense toujours que je ferais mieux d'acheter mon herbe dans la rue. Mon objectif avec le darknet maintenant est surtout juste d'essayer de le comprendre"
> P**********3

4. 4. 2 Déplacement spatial des activités

La majorité des réactions observées chez les participants, cependant, témoignent d'une volonté de s'adapter, afin de conserver et poursuivre leurs activités au sein des cryptomarchés. Tout d'abord, suite à la perte d'une ressource, certains participants partagent leur intention de déplacer leurs activités vers d'autres plateformes et d'autres usagers. Suite à la fermeture de DeepDotWeb, plusieurs commentaires publiés par les membres visaient à guider les participants vers d'autres sites pouvant servir de remplacement. La perte de répertoire et de publicité que rendait possible DeepDotWeb a également poussé les usagers à utiliser d'autres plateformes pour faire la publicité de leur commerce, afin que leur clientèle puisse les suivre à travers les différents sites de marchés.

> "Quoi qu'il en soit, voici le lien pour DarkNet, c'est exactement le même type de site, juste moins en ce qui concerne les liens vers les forums et les sites darkweb"
> t**********s

> "Quoi qu'il en soit, si tu es bon vendeur, les acheteurs vont te suivre sur n'importe quel marché. Si tu es nouveau, tu dois faire partie de tous les marchés et les forums ou du moins essayer."
> e****r

Un phénomène similaire est observable dans les commentaires publiés suite à l'opération DisrupTor. Les participants estiment que les acheteurs n'auront pas de difficultés à trouver de nouveaux vendeurs pour s'approvisionner. Cette pratique est d'ailleurs fréquente et déjà utilisée lorsqu'ils ne sont pas satisfaits de leurs précédentes commandes.

> "J'ai bougé et j'ai trouvé une meilleure offre, mais ce serait bien de savoir s'il est toujours là au cas où..."
> A*******t

> "reste à voir si les acheteurs trouveront de nouveaux vendeurs. Alerte spoiler : oui, il vont trouver."
> J*****o

Les commentaires publiés témoignent également de déplacements effectués par les vendeurs ayant évité les vagues d'arrestation. Lorsqu'un vendeur est appréhendé, son absence crée une opportunité pour les nouveaux membres qui souhaitent prendre sa place. Ce roulement parmi les vendeurs n'a pour effet que d'éliminer la compétition, ce qui provoque une hausse des prix et des profits, et par le fait même, attire de nouveaux participants dans le commerce de la drogue sur le dark web. Certains vendeurs font d'ailleurs ouvertement de la promotion sur les publications en lien avec l'opération policière.

> "120 nouveaux vendeurs viennent d'entrer dans le chat."
> t**********t

> "Coupe une tête, 2 autres vont pousser"
> i**********0

> "Si quelqu'un a besoin d'un nouveau vendeur. Sentez-vous libre d'aller nous regarder sur WHM et DM."
> g******r

4. 4. 3 L'adaptation et les innovations

Alors que certains membres préconisent le déplacement spatial de leurs activités, d'autres discutent des différents déplacements stratégiques qu'ils seraient en mesure de mettre en place afin de faire perdurer leurs activités illicites dans les cryptomarchés. Grâce aux données recueillies, nous avons pu identifier trois formes de déplacements stratégiques envisagés par les participants. D'abord, certains font la promotion du partage du capital illicite, en énonçant l'importance du rôle que peut avoir la communauté dans la survie de l'écosystème. Ensuite, certains usagers discutent des changements envisageables dans leurs habitudes de consommation, qui pourraient aider à rendre les cryptomarchés et leurs participants moins intéressants aux yeux des forces de l'ordre. Finalement, ils sont nombreux à discuter des adaptations et innovations possibles au niveau des outils technologiques en place dans l'infrastructure des cryptomarchés.

4. 4. 3. 1 Promouvoir le partage de capital illicite

Tout d'abord, de nombreux membres discutent de l'importance de l'apprentissage via le partage de capital illicite. La fermeture de DeepDotWeb a mis en lumière la difficulté qu'éprouvent plusieurs membres lorsqu'ils doivent valider eux-mêmes des liens, ou encore lorsqu'ils doivent se protéger contre les tentatives de fraude et d'arnaque. Même si les plateformes centralisées de partages de liens, tel que Dark.fail et Darknetlive sont fréquentés par plusieurs, certains membres préconisent des méthodes alternatives pour procéder à la validation des différentes ressources fréquentées dans le darkweb; certains suggèrent de valider manuellement les clés PGP des membres, d'autres d'activer les fonctions de doubles vérifications (2FA), et finalement, les derniers suggèrent fortement la sauvegarde des liens valides trouvés. De nombreuses discussions tournent donc autour des diverses façons de réduire les risques internes, rencontrés dans la communauté. Ils s'assurent d'expliquer en détail la méthode qu'ils utilisent, et partagent généreusement leurs connaissances avec les autres membres de la communauté.

“J’avais l’habitude d’utiliser DeepDotWeb avant qu’il ne soit saisi et je vérifiais mes URLs avec PGP pour être sûr. Mais depuis qu’il est parti, j’utilise Darknetlive et, bien sûr, je vérifie mes URLs avec PGP.”
G**********m

“N’utilisez pas aveuglément les ressources de liens, surtout les ressources hidden wikis connus pour distribuer des liens de hameçonnage et d’escroquerie. Utilisez plutôt des ressources plus fiables comme dark.fail ou la liste de .onion de Dread. Assurez-vous de recouper les liens que vous obtenez avec les autres listes de liens, car si le même lien de marché apparaît sur plusieurs ressources de liens de confiance, le risque qu’il s’agisse d’un lien d’hameçonnage est moindre. De plus, une fois que vous avez trouvé un lien légitime, ajoutez-le à vos favoris. Les marchés distribuent également généralement des miroirs légitimes sur leur site ou leurs forums. Assurez-vous de les mettre en signet dès que vous les voyez. N’attendez pas d’en avoir besoin, mais de ne plus pouvoir atteindre le marché, car il est en panne encore”
w**********t

Alors que de nombreux partages sont fait dans le but de réduire les risques encourus, un débat oppose les membres qui prônent le partage des connaissances à ceux qui estiment que partager ainsi ouvertement leurs stratégies de sécurité opérationnelle est une erreur. Selon ces derniers, ils courent le risque d’informer les forces policières sur les faiblesses de leurs interventions, et sur les mesures prises par les participants pour échapper à leur contrôle. Ayant conscience que les membres des forces de l’ordre sont présents dans l’écosystème et qu’ils sont à l’affut d’information de la sorte, ces membres considèrent qu’il faut être plus discret quant à la nature des informations partagées, et trouver une façon alternative de développer et parfaire ses connaissances.

> “Sois prudent mate, il y a une raison pour laquelle il ne téléchargera pas cet ebook aux yeux du public. Il suffit de rechercher l’ancienne archive de la bible des acheteurs dans le vieux r/darknetmarketnoobs.”
> S****e

> “(original) Le forum du marché Silk Road. Tout le monde était excité, tout le monde voulait aider, tout le monde voulait pratique un bon OpSec, tout le monde voulait apprendre un bon OpSec. Très actif dans l’aspect d’autorégulation de la scène. Comme nous l’avons appris au fil du temps, malheureusement, partager autant de connaissances et de pratiques si ouvertement n’est pas la meilleure option, comme les forces policières se cachent dans le coin, maintenant plus que jamais. Mais c’était vraiment excitant d’en faire partie”
> G**********y

Les réactions suite à l’opération DisrupTor diffèrent quelque peu. Il ne semble pas y avoir de soucis quant à l’interception d’information de la part des forces de l’ordre; au contraire, les participants demandent et partagent des conseils en grande quantité. En premier lieu, les membres mettent l’emphase sur l’importance d’apprendre de leur prédécesseur et de leurs erreurs, afin d’éviter de les reproduire à leur tour. Lorsque les détails d’une opération policière sont révélés au grand public, les participants ont tendance à partager les communications médiatiques et les publications officielles sur les forums de manière à informer les autres utilisateurs des manquements commis par les individus arrêtés. Les participants s’en servent pour accroître leur sécurité opérationnelle et de réduire les risques d’appréhension.

> “tout le monde devient un peu plus strict sur son OpSec en apprenant quelles erreurs ont fait arrêter ces gens”
> M*******l

> “Analyse du blockchain? Veuillez relire l’histoire. En fait, chaque utilisateur des DN devrait lire toute l’histoire plusieurs fois et en tirer des leçons.”
> M******e

Les participants génèrent également plusieurs discussions entourant les différentes tactiques à emprunter afin de déjouer les stratégies d'infiltration policières, et s'entraident à trouver des solutions pour combler les failles perçues dans leur sécurité opérationnelle. Certains, par exemple, semblent inquiets qu'il n'y ait pas de système préétabli entre les vendeurs et leurs clients afin de valider l'identité des deux parties. D'autres suggèrent donc d'établir un mot de passe afin de valider l'identité de chacun.

> "juste faire un message qui est signé qui dit bonjour? ou quelque chose. puis confirmez que c'est correct. Comment cela confirme-t-il exactement? Je comprends le principe, mais le code chiffré contient-il un code qui permet à la personne de savoir qu'il a été chiffré avec la clé privée de l'individu, puis le compare aux personnes publiques de la chaine ?"
> [supprimé]

4. 4. 3. 2 Modification des habitudes de consommation

En second lieu, certains membres ont suggéré d'adapter leurs habitudes de consommation, pour se diriger vers des habitudes moins à risque. La fermeture de DeepDotWeb a suscité un débat parmi les usagers. D'une part, certains indiquent que pour changer l'image des cryptomarchés et afin de détourner l'attention des forces de l'ordre, il faudrait créer des marchés qui visent seulement la vente de substances illicites en petites quantités et pour usage personnel. En effet, ces participants croient que commander en plus petites quantités diminuerait le risque de saisie et de fermeture des plateformes de marché. D'autre part, des participants critiquent cette idée en disant que peu importe l'importance des commandes effectuées, les forces de l'ordre n'hésiteront pas à intervenir contre les marchés dès qu'ils en auront l'occasion. Finalement, le concept d'éliminer les grosses commandes risquerait de coûter cher à certains vendeurs, qui menacent de déplacer leurs activités ailleurs pour conserver leur niveau de revenus.

> “Je n’ai pas vraiment entendu parler des livraisons surveillées pour de petites quantités. Cela ne vaut tout simplement pas la peine, et c’est aux États-Unis, où les autorités sont les plus dures. N’oubliez pas le déni plausible. Si vous maintenez votre OpSec en ordre, ce sera un enfer pour eux de vous attirer des ennuis pour quelques grammes de quoi que ce soit. 10g n’était qu’un exemple, cela pourrait être inférieur. […]”
> B********r

> “Je doute que l’image compte. Si les forces policières découvrent une vulnérabilité, ils ciblent quand même le marché, et ils diront au public à quel point le marché était terrible et à quel point eux sont formidables. Ce marché peut attirer les acheteurs, car il serait plus facile de trouver ce qu’ils veulent peut-être en raison d’une offre moindre. Mais je doute que les autorités les traiteraient différemment. Ils ont supprimé deepdotweb pour la publicité”
> X**********h

Des suggestions semblables furent émises suite à l’opération DisrupTor. Plusieurs discussions traitent des risques encourus par les plateformes et les vendeurs qui offrent des drogues dures, plus spécifiquement le fentanyl et les opioïdes. Les participants estiment qu’en bannissant ces substances des marchés, l’attention des forces de l’ordre se détournerait sur d’autres formes de criminalité plus critiques. Des participants rapportent d’ailleurs que certains administrateurs refusent déjà que les vendeurs offrent ce type de substances sur leur plateforme. Bien que ces substances rapportent des profits importants, les participants estiment que les risques encourus n’en valent pas la peine. Inversement, d’autres ont manifesté leur inconfort à l’idée de bannir certains produits du darkweb. Ils s’appuient sur une politique de libre marché et au respect du droit au choix libre et éclairé des individus.

> “Si les DNM ne proposent pas de choses que le fentanyl, il ne gagnera pas autant d’attention. J’en ai marre que ces sources tombent ou soient victimes de fraude”
> F********0

> “P*****, vous êtes qui pour nous dire comment vivre notre vie, nous pouvons consommer ce que nous voulons, le marché libre, c’est pourquoi le vendeur devrait être honnête, dire s’il contient ou non du fentanyl, c’est au consommateur s’il veut l’essayer”
> D***5

Parallèlement à l’idée de bannir certaines substances des cryptomarchés, des participants ont suggéré de favoriser la spécialisation des plateformes. Plutôt que d’offrir une variété de drogues aux propriétés pharmacologiques bien différentes (dont les risques diffèrent également), ils proposent de développer des marchés consacrés aux drogues douces, tel que le cannabis ou les psychédéliques. Les opioïdes et les amphétamines pourraient être vendus sur des marchés séparément, ce qui, selon plusieurs participants, détournerait l’attention des forces de l’ordre des marchés plus « inoffensifs ».

> “Que diriez-vous d’un service pour les psychédéliques, et les opis peuvent avoir leur propre marché, avec le plus de sécurité possible.”
> F********0

> “Ouais! Un totalement séparé pour les downers, puis un autre pour les uppers, les psychs, les RCs, etc..”
> T*********x

4. 4. 3. 3 Les innovations technologiques

Suite aux nombreuses interventions policières ayant eu lieu récemment dans le monde des cryptomarchés, plusieurs participants discutent de différentes stratégies pour augmenter leur sécurité opérationnelle. Au centre de ces discussions se trouvent les différentes mesures et technologies déjà existantes dans l’infrastructure, et les différents moyens réalistes qui pourraient permettre d’améliorer leur efficacité.

De nombreuses discussions traitent donc des différentes améliorations et innovations technologiques envisageables dans le but d'intensifier la sécurité opérationnelle des membres actifs dans les cryptomarchés. Ils sont nombreux à recommander aux autres utilisateurs d'effectuer des changements au niveau de leurs habitudes, notamment en suggérant d'apprendre à crypter les messages grâce au système PGP, et de ne pas utiliser les portefeuilles des marchés pour y garder de gros montants trop longtemps.

> "Je peux vous orienter rapidement dans la bonne direction L 1. Trouvez un marché, Empire semble sûr pour le moment. 2. N'achetez pas de BTC, achetez plutôt Monero, car vous pouvez utiliser xmr.to pour échanger contre BTC, vous pouvez cependant acheter BTC, envoyer via xmr.to dans Monero puis sur le marché de votre choix. 3. Utilisez toujours le navigateur Tor sur une machine virtuelle comme Tails ou un lvm crypté d'Ubuntu. 4. L'achat est simple, vous voulez trouver le produit que vous voulez, puis trouver un fournisseur fiable. La plupart des marchés ont un système de rétroaction et un autre système de notation, N'allez pas toujours cheap, et rappelez-vous que si c'est trop beau pour être vrai, c'est probablement le cas. 5. Dark.fail est un site web qui fait tourner les miroirs de certains marchés, et permet de choisir parmi des forums comme Dread ou The Hub qui ont plus d'informations sur l'utilisation de Tor pour acheter des trucs."
> m**********y

> "Allo, je suis /u/RIP_Meth_9000 :-) Si vous avez besoin d'aide pour un problème DNM, n'hésitez pas à me contacter. Je vois que Dark.Fail est listé. Maintenant, c'est très important, apprenez le cryptage PGP!!! N'utilisez JAMAIS un site DNM légal ou illégal sans cela !!!! Cela peut vous sauver 40 ans de prison !!! 9000"
> S**********0

D’autres discussions traitent également des améliorations qui devraient avoir lieu au niveau des plateformes des cryptomarchés et de l’infrastructure en soi. Alors que pour certains, les opérations policières qui ont lieu contre l’écosystème des cryptomarchés ne sont que des éléments perturbateurs, d’autres les perçoivent comme des incitatifs au développement. Selon eux, cette menace offre aux développeurs la possibilité de créer et développer de meilleures plateformes, ainsi que des technologies plus efficaces qui peuvent aider à perfectionner l’infrastructure. Plusieurs messages indiquent donc que l’écosystème s’adapte et ajuste son fonctionnement de façon à être moins vulnérable face aux menaces externes, ainsi qu’aux attaques internes. Entre autre, les administrateurs de certains marchés exigent l’utilisation de la cryptomonnaie Monero, jugée plus sécuritaire que les autres types de cryptomonnaies, ainsi que l’utilisation de la technologie de cryptage PGP par ses membres. Ils mettent également en place des mesures de filtrage de sécurité (Captcha) afin de limiter les opportunités d’attaques automatiques contre leur plateforme.

> “[…] Lorsque des endroits comme Dream sont fermés, cela crée l’opportunité pour les développeurs de créer de meilleurs marchés plus efficaces qui utilisent de nouvelles technologies et une meilleure infrastructure. Il en va de même pour les sites Web de ressources. Ils mènent une guerre impossible à gagne et je pense qu’ils en sont conscients. Le mieux qu’ils peuvent faire est de saisir les rênes et de prendre ce qu’ils peuvent obtenir pour avoir l’air de faire quelque chose.”
> B**********h

> “Les marchés survivants, et les nouveaux qui ont déjà fait leur apparition, ont adopté des mesures pour en faire des cibles plus difficiles pour les autorités. La plupart des marchés autorisent désormais les paiements dans des crypto-monnaies alternatives, comme Monero, qui sont conçues pour être plus difficiles à suivre.”
> 8***P

> “cryptonia a une bonne solution pour les DDOS, ils changent de miroir dès qu’il est attaqué, en dirigeant tout le trafic via un captcha sur un miroir spécifique”
> d*****C

Finalement, certains usagers indiquent qu'une façon de se protéger des fermetures de plateformes serait d'effectuer les transactions hors des cryptomarchés, directement via leur vendeur. Cette option est envisageable pour les individus possédant déjà des contacts de confiance; cependant, effectuer des transactions directes avec des membres inconnus est proscrit et pourrait potentiellement résulter en vol ou fraude. De nombreux membres indiquent ne pas avoir suffisamment de confiance envers les vendeurs et les autres membres pour utiliser cette façon de faire, et préfèrent continuer à utiliser le système des plateformes de marché.

> " [...] La communauté du darknet ne sera pas écrasée aussi facilement, tout le monde reste connecté. Traiter directement avec des fournisseurs qui existent depuis plus de 5 ans est aussi toujours une bonne chose! […]"
> G**********b

> " [...] Vous ne pouvez tout simplement pas obtenir ce type de sécurité lorsque vous traitez directement avec un fournisseur. Enfin, cela nous amène aux dangers des accords directs en tête-à-tête entre un acheteur et un vendeur. C'est simple. Un étranger qui peut profiter d'un autre, tout en évitant les retombées et les répercussions, va profiter de cette personne presque chaque fois. Dans les transactions directes, rien n'oblige le vendeur supposé à quelconque degré d'honnêteté ou de norme de responsabilité. Le « vendeur » peut sécuriser sa monnaie, tout en n'envoyant aucun produit en retour (arnaque à l'acheteur), lui volant ainsi son argent. Le « vendeur » peut envoyer n'importe quoi à l'acheteur (produit inactif ou produit nocif) sous prétexte qu'il s'agit du produit convenu, sans être confronté à un véritable retour documenté sur sa réputation. En d'autres termes, toute personne prétendant pouvoir effectuer une transaction avec un acheteur peut et va voler son argent, ou lui envoyer un produit incorrect, inadéquat ou autre nocif à la place, sans aucune répercussion […]"
> B**********t

L'opération DisrupTor a également généré une quantité considérable de commentaires qui traitent des différentes façons d'innover et d'adapter l'infrastructure des cryptomarchés, afin d'être mieux protégés contre les menaces externes. D'abord, de nombreuses discussions portent sur l'importance des technologies de cryptage des communications et des risques associés à l'option d'auto-cryptage offerte sur les cryptomarchés. Il appert, en effet, que malgré la multitude de messages et de ressources portant sur l'optimisation de l'anonymat en ligne, plusieurs participants éprouvent encore des difficultés à comprendre et à mettre en œuvre les meilleures pratiques de sécurité opérationnelle.

> "un autre qui mord la poussière, rappelez-vous, CRYPTEZ!"
> N**********y

> "Ne jamais utiliser le cryptage d'un site. Une fois que tu appuies sur le bouton d'envoi, tu envoies du texte brut de l'autre côté. Qui sait comment c'est vraiment stocké avant de subir un cryptage ou s'il y a un trou dans le tuyau qui rend visibles ces infos."
> O**x

La signature PGP peut être utile pour valider l'identité numérique d'un vendeur lorsqu'il opère sur différentes plateformes. Elle permet aux acheteurs de suivre leur vendeur favori à travers les différents marchés. Or, les signatures PGP impliquent également qu'en cas de compromission du compte, les forces de l'ordre peuvent déchiffrer tous les messages reçus à partir de la clé du vendeur, ce qui met donc en danger l'anonymat des autres usagers. Par conséquent, des participants considèrent que changer de clé PGP fréquemment pourrait contribuer à réduire ces risques. Des marchés requièrent d'ailleurs que les vendeurs changent de clé tous les six mois. Cette pratique a toutefois quelques inconvénients : les acheteurs doivent trouver d'autres moyens d'authentifier leur vendeur. Certains suggèrent la mise en place d'une question secrète ou d'un mot de passe, afin de valider l'identité de chacun. Or, cela ne permet pas de détourner la surveillance policière et n'empêche pas la révélation des liens entre les membres.

“Apparemment, il est bon pour l’OpSec de changer de clé PGP fréquemment. Il existe même un marché qui nécessitait généralement 6 mises à jour mensuelles de PGP pour les fournisseurs. Je ne comprends pas vraiment pourquoi ou comment c’est signe d’un bon OpSec cependant. ”
S**********1

“S’ils changent de clé PGP, ils doivent créer un message signé à l’aide de leur ancienne clé confirmant que la nouvelle est légitime. S’ils ne le font pas et qu’ils en font juste une nouvelle, je serais très suspect. C’est ce que font les forces de l’ordre quand ils prennent un compte vendeur, mais pas sa clé PGP.”
P*****3

Comme il fut le cas suite à la fermeture de DeepDotWeb, de nombreux membres ont suggéré de délaisser les plateformes de marché pour se tourner vers la vente directe. Encore une fois, les participants semblent partagés : certains estiment qu’il s’agit d’une méthode tout à fait légitime pour remplacer la vente et l’achat par le biais des cryptomarchés, dans la mesure où ces derniers sont désormais « trop » faciles d’accès pour les personnes dotées d’une mauvaise sécurité opérationnelle. Les cryptomarchés seraient alors uniquement utilisés pour repérer des vendeurs avec qui transiger à l’extérieur du marché.

D’un autre côté, plusieurs participants estiment que les transactions directes représentent une pratique contre-indiquée et qu’il ne s’agit pas d’une solution adéquate à l’instabilité de l’écosystème. Pour certains, il s’agit d’un recul. Ces derniers rappellent l’importance d’inclure un tiers parti dans la transaction afin de sécuriser les échanges, tel le permettent actuellement les cryptomarchés.

“Ne faites pas de transactions directes avec des fournisseurs que vous ne connaissez pas ou avec lesquels vous n’avez jamais fait affaire auparavant. À quelques exceptions près, les offres wickr sont des escroqueries garanties.”
A**********r

> “N’oublie pas que la meilleure source d’informations dans ce sub a toujours été les avis des utilisateurs sur les fournisseurs (avec photos!), on travaille avec eux et on connaît les fournisseurs actuels, alors il faut continuer à partager des informations honnêtes et à assurer la sécurité de la communauté! Merci d’aider à garder cette communauté en sécurité et la tête libre”
> C**********n

Malgré les nombreuses possibilités d’innovations énumérées, il ne semble pas y avoir de solution qui fasse l’unanimité parmi la communauté. L’une des principales explications permettant de comprendre la difficulté derrière l’implantation des différentes options d’adaptation et d’innovation est la nécessité de préserver un équilibre entre l’aspect sécuritaire des cryptomarchés, et la convivialité d’utilisation des plateformes. Bien que les nouvelles pratiques implantées soient faites dans le but de renforcer la sécurité des membres, les avis des utilisateurs sont partagés. Certains pensent que, par exemple, la fermeture de DeepDotWeb n’a aucun impact sur la façon d’utiliser les cryptomarchés, car le processus menant à ces plateformes est relativement simple : télécharger Tor, utiliser les liens disponibles, effectuer les transactions à l’aide de Bitcoin, etc.. Bref, ils sont d’avis que cela ne nécessite pas de connaissances particulières.

> “La disparition de Deepdot n’affecte pas du tout notre capacité à récupérer des choses en ligne. Il faut simplement enregistrer les liens miroirs et tout va bien aller”
> [supprimé]

> “Comme quoi? Télécharger Tor. Utilisez Tor pour avoir accès aux marchés du darknet – le message précédent vous donne justement une liste de liens. Achetez les Bitcoin – il existe des milliers de guides sur la façon d’acheter des Bitcoin. Dépensez les Bitcoin sur le marché. Il n’y a pas de secret ou de compétence nécessaire.”
> m**********r

D’autres utilisateurs possèdent une opinion plus nuancée quant à la difficulté d’apprentissage et d’utilisation des nouvelles technologies proposées. L’un d’entre eux indique que le temps et les efforts nécessaires pour y parvenir sont importants, mais diminueront avec le temps. Pour certains, utiliser les cryptomarchés de manière sécuritaire représente un lot important de travail, de recherche et de préparation. Le temps dédié aux vérifications de sécurité est substantiel. Afin d’assurer le plus haut niveau de sécurité qu’il soit, les membres doivent être constamment à l’affut des derniers développements.

La perte d’une ressource d’information, tel que DeepDotWeb, et la récurrence d’arrestations de membres, tel que fut causé par l’opération DisrupTor, force donc les usagers à perfectionner leur sécurité opérationnelle de manière ponctuelle. Certains témoignent de la difficulté qu’ils éprouvent à trouver des liens et des informations justes sans les ressources pour débutants proposées sur la plateforme DeepDotWeb, surtout dans un écosystème en mouvement constant. D’autres dénoncent la perte de contact de confiance, et les efforts et les risques que représente la création de nouveaux liens. Les utilisateurs dénoncent donc le travail supplémentaire requis pour maintenir et augmenter leur sécurité opérationnelle. Alors que certains disent comprendre l’importance de continuer les efforts et maintenir ces processus ennuyeux et redondants, d’autres avouent ne pas être disposés à mettre en œuvre ces fonctionnalités de plus en plus complexes. Ils indiquent leur intention de se contenter des outils et des technologies de base, mentionnant ne pas posséder les capacités ou les ressources pour en apprendre davantage. Il est donc peu probable de voir ces individus adopter les mesures de protection encore plus complexes et sophistiquées que celles déjà en place.

> “Merci pour l’effort, mais tu perds ton temps. S’il y a une chose que j’ai apprise au cours des dernières années sur le DN, c’est que les gens ne veulent pas : *Lire, *Apprendre ou * Réfléchir. Les gens sont simplement obsédés par l’obtention de leur substance de choix, et ils le veulent MAINTENANT! Ils ne peuvent littéralement pas penser à autre chose – même leur propre sécurité est secondaire,

comme en témoigne le nombre de personnes qui n'utilisent toujours pas le cryptage, même pour leur adresse de livraison."

C**********r

"Le succès ici, comme partout ailleurs, est le résultat de beaucoup de travail, de recherche et de temps. Personne ne peut te montrer comment le faire, mais si tu as plongé plus profondément dans ce monde et y trouve un foyer, soit tu apprendras ces choses, ou tu vas te faire manger et recracher dans une cellule de prison. Ralentis ton rythme. Oui, tu peux essayer et faire un achat et si tu ne te fais pas arnaquer, tu vas probablement réussir. Mais j'ai souvent vu ici que lorsque les gens font les premiers pas, ils dégénèrent rapidement."

B**********h

Chapitre 5 : La discussion

5. 1 Quels furent les impacts pratiques?

Tel que nous l'avons vu lors du premier chapitre de ce mémoire, les interventions policières menées contre les réseaux de trafic de stupéfiants visent l'un de ces deux résultats; provoquer la réduction de la demande au sein d'un marché, ou en réduire l'offre. Notre étude portait sur deux interventions distinctes, soit la fermeture de la plateforme DeepDotWeb par les forces de l'ordre, et l'opération DisrupTor. Chacune de ces deux opérations correspond à l'une des deux approches susmentionnées, et a mené à des résultats différents sur la communauté et leur écosystème.

Les impacts causés par les activités policières, tels que perçus dans les discussions publiées à la suite de la fermeture de la plateforme Deepdotweb, nous permettent de comprendre que les effets ressentis par les participants suite à cette opération concordent avec les objectifs souhaités lors d'une intervention visant la réduction de la demande. Le manque d'information accessible cause des difficultés pour les participants qui tentent d'atteindre de nouveaux vendeurs ou de nouvelles plateformes. Cela rend également plus ardu l'accès à la marchandise, et complique le processus de transaction. Le partage restreint du capital illicite génère également des difficultés pour certains membres; notamment, des usagers possédant moins de connaissances se plaignent de la perte de tutoriels et de guides qui leur servaient dans la réduction des risques. Ils sont également nombreux à se dire moins en mesure de se protéger et, par le fait même, moins en sécurité.

La fermeture de Deepdotweb a entrainé la perte d'une source primordiale d'information pour les membres de la communauté. Comme nous avons pu le voir, cette plateforme était un outil facilitateur important pour la navigation d'un site à l'autre, pour la connectivité des membres entre eux, ainsi que pour le partage d'éléments d'actualité. Les interventions policières visant la réduction de la demande cherchent à réduire le nombre de consommateurs actifs – et donc de substances achetées dans le marché (Hough et Natarajan, 2000) - de deux façons : en augmentant les risques perçus inhérents à la réalisation des transactions (May et Hough, 2001), et

en augmentant les obstacles et les difficultés rencontrées dans le processus d'achat. La disparition des listes de liens valides et sécuritaires publiées par DeepDotWeb a permis la propagation rapide et importante des tentatives de fraudes et des liens d'hameçonnage dans l'écosystème. De plus, sans l'accès aux guides et tutoriels présents sur la plateforme, les membres peinent à se protéger des participants mal intentionnés. Il semble donc que la perte de DeepDotWeb a créé un environnement plus risqué, tout en retirant une source d'information qui se serait avérée être particulièrement importante pour permettre aux participants de contrecarrer ces risques. Il est donc évident que la perte de la plateforme répond au premier objectif de la réduction de la demande. La deuxième stratégie de réduction de la demande, soit l'augmentation des obstacles, correspond aux objectifs de « l'inconvenience policing » de Moore (1990), soit de rendre le marché moins attrayant aux potentiels futurs membres. L'augmentation du temps et des efforts nécessaires à la réalisation d'une action démotivera certains usagers actuels ou potentiels de prendre part au trafic (Caulkins, 1993; Murji, 1993; Pearson, 1992; Moore, 1990; Kleiman et Smith, 1990). Le retrait de la ressource qu'était Deepdotweb a eu comme effet d'augmenter le temps et les efforts investis par les participants pour effectuer leurs activités habituelles. La majorité des individus qui ont réagi négativement à ces changements se disent eux-mêmes être moins expérimentés et habiles – alors que ceux se disant plus habitués ne semblent pas être affectés outre mesure. Cette intervention a donc eu davantage d'impacts sur les membres débutants et ceux dont les capacités informatiques sont moins développées. Le fait de cibler en particulier les membres novices d'un réseau est une stratégie généralement utilisée dans le but d'étouffer les marchés (Murji, 1993). Cette catégorie de membres est plus vulnérable aux changements et est moins motivée à investir le temps et les efforts de recherche supplémentaires nécessaires pour atteindre la marchandise. Ainsi, le fait de compliquer la tâche aux membres inexpérimentés risque de les convaincre d'abandonner leurs activités et, par le fait même, empêcher l'afflue de nouveaux membres vers le réseau (Murji, 1993). Étant donné l'important mouvement rotatif des membres au sein des plateformes de marchés (Christin, 2013), priver ainsi les cryptomarchés de leur relève pourrait naturellement mener vers l'étouffement de leurs activités commerciales. C'est d'ailleurs ce qui est actuellement observé; le dernier rapport de Chainalysis (2021) indique que le nombre des ventes effectuées par l'entremise des plateformes hébergées sur le darkweb serait inférieur à celui des années précédentes, laissant donc présager un ralentissement du niveau de fréquentation des cryptomarchés.

L'opération DisrupTor a mené à l'arrestation de 179 vendeurs qui offraient principalement des opioïdes. Cette intervention a eu comme effet direct de réduire l'offre dans les marchés. L'objectif principal de cette stratégie vise ainsi à augmenter la rareté des substances, afin de les rendre moins disponibles dans le réseau, et d'entrainer une augmentation des prix (Murji, 1993; Hough et Natarajan, 2000; Kerr et al., 2005). Le découragement et le retrait de vendeurs non ciblés par l'opération figurent également dans les buts souhaités – une diminution du nombre de fournisseurs entrainerait la diminution de disponibilité des substances (Fader, 2016; Moeller et al., 2016).

Suite à l'opération DisrupTor, de nombreux participants disent essayer de retrouver leur vendeur habituel. Lors de la perte d'un contact transactionnel, les usagers éprouvent des difficultés à créer de nouveaux liens commerciaux – soit ils ne parviennent pas à localiser les vendeurs, ou alors ils indiquent éprouver des réticences à faire confiance à de nouveaux contacts. La réussite commerciale des cryptomarchés réside dans la solidité des liens sociaux et de la confiance existant parmi les membres de la communauté (Munksgaard, 2021; Norbutas et al., 2020; Pace, 2017). Dans un environnement virtuel anonyme, la confiance se bâtit de deux manières : d'abord, grâce aux systèmes de notation et de réputation mis en place, mais également grâce aux expériences vécues individuellement (Norbutas et al., 2020). En effet, lorsqu'un client conclue plusieurs transactions positives avec un même vendeur, une relation se confiance se tisse entre les deux membres. Une succession de ces expériences satisfaisantes avec ce vendeur placera le client dans une position de confiance, et ce dernier sera plus à l'aise d'effectuer des transactions comportant des montants plus élevés (Norbutas et al., 2020; Munksgaard, 2021). Ces observations sont d'ailleurs les mêmes que celles effectuées dans le contexte de commerce électronique légitime (Huang et Liua, 2010). Les 179 arrestations de vendeurs actifs orchestrées lors de l'opération DisrupTor ont donc détruit de nombreuses relations de confiance construites par de nombreux clients, qui doivent désormais se tourner vers d'autres vendeurs et, les replongent dans un environnement où les risques de fraude et d'escroquerie sont élevés (Holt et al., 2015; Evangelista et al., 2018). En s'attaquant ainsi aux liens sociaux existant dans l'écosystème, il devient plus difficile de réaliser des transactions. Cette intervention a également fait ressortir l'intérêt de cibler un plus grand nombre de membres de moins importants, dans le cadre d'une intervention. Traditionnellement, les forces de l'ordre orientent leurs ressources vers

des membres influents et hauts placés. Or, ils sont rapidement remplacés et les participants retrouvent rapidement leur rythme habituel (Bhaskar, et al., 2019; Ladegaard, 2019; Soska et Christin, 2015). La disparition d'une multitude de membres moyens semble cependant avoir causé plus de perturbations, notamment au niveau de la disponibilité des substances. Il est désormais plus difficile de trouver un autre vendeur de confiance et disponible, car, d'abord, il y en a moins et de plus, la demande est trop forte pour qu'ils parviennent à y répondre convenablement.

Nous pouvons donc déterminer que ces deux interventions innovatrices ont produit des impacts pratiques distincts sur les activités des participants des cryptomarchés. La perte d'un outil facilitateur tel que DeepDotWeb, et le fait de cibler l'infrastructure de l'écosystème a notamment causé l'apparition de nombreux obstacles et difficultés dans la réalisation des activités quotidiennes de l'ensemble de la communauté, ce qui a eu pour effet de rendre l'environnement moins accessible et plus risqué pour tous. Ces complications pratiques attireront donc moins de nouveaux membres, ce qui contribuera à assécher le bassin de participants potentiels, ce qui aura un impact négatif sur la croissance des activités des marchés. Le but des interventions de réduction de la demande n'est pas de dissuader les membres actifs, mais plutôt de compliquer la venue de nouveaux membres. Tel que nous avons pu le voir, le fait de cibler ainsi l'infrastructure et de s'en prendre à l'architecture sur laquelle repose la communauté semble avoir été efficace en ce sens. De plus, l'opération DisrupTor proposait un changement important des individus habituellement ciblés; au lieu de s'attaquer à un ou deux membres influents et importants au sein de la communauté, les forces de l'ordre ont orienté leurs efforts vers un grand nombre de petits et moyens membres. Les effets pratiques qui en ressortent sont évidents : un plus grand nombre de vendeurs arrêtés est plus difficile à remplacer qu'un petit nombre d'importants membres. La disponibilité des substances est nettement diminuée et les membres peinent à combler la perte de leur vendeur.

5. 2 Une augmentation de la perception des risques

Selon quelques études parues, la perception de risque des participants des cryptomarchés ne serait pas ébranlée outre mesure à la suite d'une intervention policière au sein de leur écosystème (Lacson et Jones, 2016; Ladegaard, 2018). Les commentaires recueillis au sein de la communauté seraient positifs et orientés vers le futur, alors que la cause des arrestations serait attribuée aux erreurs humaines (Ladegaard, 2018). Nos résultats indiquent toutefois une réalité différente. La perte d'information causée par la fermeture de la plateforme Deepdotweb a augmenté la perception des risques de certains utilisateurs, particulièrement en ce qui a trait aux risques internes – soit les risques de fraudes et d'hameçonnage. La prolifération des liens frauduleux dans l'écosystème, jumelée au manque de connaissances et d'informations accessibles aux participants, ébranle la confiance que ces derniers ont envers les membres de leur propre communauté. D'autres considèrent que le partage d'information serait une arme à double tranchant, et que les forces policières s'en serviraient pour mieux orienter leurs interventions. Même s'ils n'ont pas tort, le partage de capital illicite s'avèrerait essentiel à la réduction et la mitigation des risques (VanNostrand et Tewksbury, 1999; Aldridge et Askew, 2017), et le manque de coopération entre les différents membres de la communauté risquent de laisser plusieurs individus à court de ressources pour se protéger.

Les impacts sur la perception des risques furent cependant nettement plus importants suite à l'opération DisrupTor. Le fait que les individus identifiés et appréhendés lors de cette intervention ne soient pas des administrateurs de marchés ou des vendeurs influents, mais plutôt des membres « réguliers », a fait réaliser aux participants qu'eux-mêmes pourraient constituer des cibles d'intérêt des forces de l'ordre, et que la préservation de leur anonymat n'est pas garantie dans cet écosystème. Plusieurs déclarent d'ailleurs percevoir cette intervention comme une attaque à leur droit à l'anonymat. Le fait d'être anonyme est un aspect primordial dans l'écosystème des cryptomarchés (Holt et al., 2015; Martin, 2014a), et porter atteinte à ce droit a généré une augmentation marquée du sentiment d'insécurité. Une baisse importante de la confiance, tant à l'endroit de la structure et de ses technologies, qu'à l'endroit des autres membres de la communauté, transparaît dans les messages partagés par les participants. Ils disent percevoir que les forces de l'ordre sont de plus en plus efficaces dans leurs interventions et

gagnent du terrain sur l'écosystème des cryptomarchés – une prise de conscience à l'encontre des conclusions émises par divers chercheurs (Lacson et Jones, 2016; Ladegaard, 2018).

De nombreuses discussions traitent également des craintes reliées aux sanctions auxquelles s'exposent les participants. Alors que cet aspect était pratiquement absent des discussions liées à la fermeture de Deepdotweb, la hausse de perception des risques d'arrestation et de sanction individuelle est flagrante dans les réactions à l'opération DisrupTor. Une étude réalisée en 2018, par Ladegaard, traitait des impacts de l'annonce de la peine imposée à Ross Ulbricht, l'administrateur et fondateur du célèbre cryptomarché Silk Road, sur la communauté des cryptomarchés. Selon ses analyses, malgré la sanction sévère infligée à Ulbricht, aucun impact négatif n'a été observé dans les activités de la communauté – au contraire, il aurait remarqué une hausse dans les transactions réalisées dans le réseau durant cette période. Il en aurait conclu que, malgré la médiatisation de l'importante sentence imposée à l'un des leurs, aucun changement n'aurait été détecté dans la perception des risques des participants de cette communauté. Notre étude présente, cependant, des résultats à l'opposé de ceux de l'étude de Ladegaard (2018). La réalité du risque de sanction semble être établie comme une certitude dans l'esprit des membres, et ces derniers en sont rendus à discuter des différents moyens à leur disposition pour atténuer la sévérité de leur peine potentielle, dans l'éventualité où ils seraient appréhendés. Suite à l'annonce des 179 arrestations, de nombreuses discussions portent sur les facteurs aggravants, tels que la quantité et la nature des substances commandées, le rôle occupé dans l'écosystème, la fréquence des transactions, etc.

Les disparités existant entre les conclusions de notre étude et celles des études menées par Lacson et Jones (2016) et Laadegard (2018) proviennent principalement du choix des opérations étudiées. En effet, les deux recherches citées ont utilisé l'intervention ayant mené à la fermeture de la plateforme Silk Road et à l'arrestation de son administrateur principal, en 2013 (Lacson et Jones, 2016). Cette opération policière s'avère d'ailleurs être le premier événement de la sorte à frapper la communauté des cryptomarchés, à l'époque et il s'agit d'une intervention typiquement traditionnelle. Ainsi, les disparités existant entre nos conclusions et les leurs sont tout à fait normales. Cela met d'ailleurs l'emphase sur nos réalisations, selon lesquelles les interventions

innovatrices seront parvenues à déstabiliser la communauté et à créer des réactions qui ne furent pas observées lors des interventions traditionnelles.

Il est également pertinent de noter que Silk Road était le premier cryptomarché d'importance dans l'écosystème (Martin, 2014a). Sa fermeture constituait donc la première opération policière d'envergure dans l'écosystème. Tel que Ladegaard (2018) l'a mentionné dans son étude, plusieurs membres ont attribué l'arrestation d'Ulbricht à des erreurs commises de sa part. Ils ne percevaient donc pas les forces policières comme des menaces envers l'écosystème, et ne voyaient pas encore les faiblesses présentes dans l'infrastructure. Cet environnement étant encore, à cette époque, peu connu du public, la communauté était constituée d'un nombre plus restreint de membres, qui ne croyaient pas être particulièrement une cible intéressante pour les forces de l'ordre. Les interventions policières innovatrices et répétées génèrent plus de résultats, et exploitent de plus en plus les faiblesses présentes dans l'écosystème. Les participants ne se sentent plus inaccessibles, et, comme observé grâce à nos analyses, ressentent désormais les risques comme étant plus présents. Le contexte actuel est donc totalement différent que le contexte qui régnait dans les cryptomarchés en 2011, lorsque Silk Road fut fermé, et l'ensemble des événements qui ont eu lieu depuis les dix dernières années viennent, en partie, expliquer les différences dans les réactions des participants.

5. 3 Les participants sont-ils découragés?

Nous avons donc remarqué que les participants semblent être plus conscients des risques inhérents à leurs activités sur les cryptomarchés, et que, pour plusieurs, réaliser ces activités est désormais plus compliqué. En dépit de ces constats, seulement quelques participants ont partagé leur intention de quitter l'écosystème, ou encore de mettre une pause à leurs activités. Ce résultat n'est cependant pas étonnant; en effet, plusieurs études qui se sont penchées sur les interventions policières dans les cryptomarchés dénotent également l'absence d'effets dissuasifs ou de signes de découragement, suite à un choc externe (Lorenzo-Dus et Di Cristofaro, 2018; Lacson et Jones, 2016; Ladegaard, 2018; Bhaskar et al., 2019). Ces résultats ne sont pas surprenants : il est, en effet, nettement plus compliqué de parvenir à des effets dissuasifs dans le monde cyber que dans le monde physique (Alinsato, 2012; Maimon, 2020). La réalité particulière du cyberespace rend

les mécanismes de dissuasion, efficaces dans le monde réel, inefficaces dans le web (Kerr, 2004); l'absence de frontières spatiotemporelles et le maintien de l'anonymat des membres rendent presque nulles les mesures traditionnelles au sein des cryptomarchés (Alinsato, 2012; Bossler, 2021; Nye Jr, 2017). L'incapacité des forces policières à attribuer les sanctions régulières aux cyberdélinquants a donc un impact négatif sur les trois facteurs de crédibilité de la sanction, particulièrement le facteur de certitude de détection et de sanction (Bossler, 2021), et justifie le manque d'effets dissuasifs observés.

Malgré l'absence de dissuasion complète, nos résultats nous permettent toutefois d'observer des signes de dissuasion restrictive chez les membres de la communauté. Deux types de réactions ont été principalement observés chez les participants. D'abord, les utilisateurs des plateformes ont indiqué vouloir modifier leur manière de mener leurs activités au sein des cryptomarchés, dans le but de contourner les obstacles et les nouveaux risques imposés suite aux interventions policières. En premier lieu, de nombreux participants discutent de la nécessité de restreindre les informations partagées dans les forums, dans le but de ne pas dévoiler trop de détails pouvant servir aux forces de l'ordre. D'autres discutent des possibles changements à effectuer dans leurs habitudes de consommation. Certains indiquent envisager la possibilité de délaisser certaines substances qui, selon eux, risquent d'attirer davantage l'attention des forces de l'ordre. Ils associent, en grande partie, l'intérêt des agences d'application de la loi envers leur écosystème au fait que certains produits plus dangereux pour la population générale soient couramment disponibles et vendus sur les plateformes de marché.

L'opération DisrupTor a, en effet, majoritairement ciblé les revendeurs d'opioïdes et de produits contenant du fentanyl. Il ressort donc des discussions la volonté de plusieurs de restreindre la disponibilité de ces produits à certains marchés désignés et spécialisés, ou encore d'en cesser complètement la vente. Des suggestions portant sur de nouvelles plateformes ne permettant les commandes qu'en petite quantité pour usage personnel furent partagées à plusieurs reprises. L'ensemble de ces réactions concordent avec ce que Broadhurst et al., (2021) ont remarqué, suite à la fermeture de plateformes de cryptomarchés; lorsque les participants perçoivent une augmentation des risques, ils entreprennent de modifier leur façon de faire afin de diminuer les risques reliés à la poursuite de leurs activités. Ces réactions confirmeraient donc

l'existence de dissuasion restrictive chez les participants comme impact aux interventions policières.

Les participants aux cryptomarchés étant des individus rationnels, ils tentent de poursuivre leurs activités de manière à atténuer les risques encourus, en apportant des changements dans leurs stratégies habituelles (Fader, 2016). Cependant, ces changements ont comme effet de causer un ralentissement dans les activités, ou peuvent même en occasionner la cessation dans certaines sphères complètes. L'utilisation de pratiques plus discrètes (Erickson et al., 2013; Jacobs, 1996), la diminution dans la fréquence des activités (Jacobs, 1996), le changement dans le choix des lieux et des stratégies pour effectuer leurs transactions sont des signes de la prévalence d'une dissuasion restrictive (Erickson et al., 2013). Bref, les aspects innovateurs des interventions étudiées ont tout de même forcé les participants à modifier certains de leurs comportements, et même délaisser certains aspects de leurs activités.

Selon Nye Jr (2017), l'effet de crédibilité de la menace de sanction n'est pas uniquement lié au « comment », mais peut également provenir du « qui » et du « quoi ». Les deux interventions à l'étude présentent des innovations importantes au niveau des cibles visées. DeepDotWeb, une plateforme non transactionnelle qui partage de l'information, ou encore 179 participants réguliers, ne correspondent pas aux cibles habituelles et attendues lors des interventions traditionnelles. Ces changements semblent avoir fait prendre conscience aux participants qu'ils ne peuvent désormais plus prévoir être à l'abri des risques de sanction. La modification des cibles lors de ces opérations a créé une perception de risque généralisée, et la certitude de sanction qui était jusqu'alors nulle, est devenue une réalité pour plusieurs. Cette prise de conscience pourrait donc de provoquer des effets dissuasifs plus généraux que restrictifs; tous les participants peuvent être concernés par les interventions policières futures. De plus, selon Sherman (1990), étendre et varier les cibles potentielles lors d'interventions pourraient produire des effets de dissuasion résiduelle plus efficaces que ceux émanant de la dissuasion initiale. Ainsi, le fait d'innover dans les stratégies et de varier dans les cibles lors des interventions innovatrices actuelles et futures continuera de déstabiliser les participants des cryptomarchés, et générera de plus en plus de perturbations dans la perception des membres, selon laquelle ils ne courent aucun risque de sanction légale.

5. 4 Solutions : déplacements et innovations

Dans une étude parue en 2018, les chercheurs Lorenzo-Dus et Di Cristofaro concluent que les interventions policières ayant lieu contre l'écosystème des cryptomarchés, seraient une source de motivation chez la communauté pour procéder à l'amélioration de leur infrastructure et à l'innovation de leurs outils technologiques. En observant les discussions publiées dans certains forums, suite à la fermeture de la plateforme Silk Road en 2014, ils ont remarqué que les participants ont pris connaissance des limites et faiblesses technologiques existant dans l'écosystème, et qu'ils ont discuté des nombreuses possibilités de déplacements stratégiques vers de nouvelles mesures de sécurité opérationnelle.

Nos résultats permettent une analyse semblable; de nombreuses discussions débattaient des différentes améliorations et innovations possibles afin de mieux outiller l'écosystème en prévision des prochaines frappes. Plusieurs suggéraient l'utilisation répandue de l'outil de cryptage PGP, allant même jusqu'à proposer qu'il soit obligatoire pour certaines plateformes. D'autres favorisaient l'utilisation d'une certaine cryptomonnaie et préconisaient l'abandon des autres. Les participants ont également discuté des diverses mesures optimales de sécurité à instaurer sur les plateformes actives, telles que la privatisation des sites ou encore l'utilisation des tests CAPTCHA pour accéder au marché. Un remaniement du fonctionnement de l'infrastructure est notamment souvent mentionné dans les intentions des participants : certains préconisent l'établissement de ventes directes comme façon de procéder, alors que d'autres sont d'avis que la décentralisation des plateformes serait la méthode la plus logique. Cette recherche d'amélioration et d'innovation de la part des participants est un effet qui fut également observé dans plusieurs autres études (Hutchings et Holt, 2017; Gupta et al., 2018; Childs et al., 2020; Barratt et al., 2016; Holt et al., 2015).

Cependant, et malgré les nombreuses possibilités énumérées lors des discussions, l'éventualité d'innover afin de rendre les cryptomarchés plus difficiles d'accès pour les forces de l'ordre ne semble pas faire l'unanimité auprès de l'ensemble de la communauté. De nombreux partages nous permettent de voir que l'enthousiasme manifesté par certains concernant les possibilités d'amélioration dans l'écosystème n'est pas ressenti par tous; de nombreux membres

expriment leurs réticences face à ces changements, et certains y sont même totalement opposés. La lecture des résultats obtenus nous permet d'établir trois raisons principales à ces réticences. D'abord, plusieurs ne possèderaient pas les capacités ou les connaissances nécessaires pour poursuivre leurs activités dans un environnement où les mesures de sécurité sont plus complexes et où les accès sont moins ouverts. Ils indiquent qu'il y aurait une scission entre les membres plus anciens et plus habiles en informatique, et ceux qui sont plutôt novices ou moins connaisseurs. Ce discours n'est pas nouveau – Kleiman (1988) arrivait à la même conclusion à propos des marchés de vente de drogue dans le milieu physique. Selon lui, les contrecoups des interventions policières sont différemment encaissés chez les membres plus expérimentés que chez les membres débutants. Les plus anciens possèderaient, entre autres, les ressources, les contacts et la motivation supplémentaires nécessaires pour persévérer et éviter les obstacles générés par les chocs. Cette réalité ne concerne plus seulement que l'univers des cryptomarchés; il faut un seuil minimal de connaissances pour accéder aux différentes plateformes et ressources, et pour naviguer de manière sécuritaire dans l'écosystème (Bancroft, 2017; Décary-Hétu et Giommoni, 2017; Décary-Hétu et al., 2018; Martin et al., 2019b). Les membres participant aux marchés dépourvus de ces capacités technologiques se mettent en position de vulnérabilité vis-à-vis des individus malhonnêtes ou des forces de l'ordre arpentant les différents sites (Evangelista et al., 2018). C'est d'ailleurs une des raisons pour lesquelles Deepdotweb était autant apprécié par la communauté; il offrait des outils et des ressources faciles et simples permettant aux individus moins compétents d'apprendre à se déplacer en sécurité à travers l'écosystème.

Une autre justification de la réserve de certains par rapport aux innovations suggérées concerne les risques inhérents aux déplacements spatiaux et tactiques qu'ils devront effectuer. En effet, changer de partenaire commercial, ou établir de nouvelles marches à suivre dans les habitudes des participants augmente les risques et les efforts rencontrés (Weisburd, Wyckoff, Ready, Eck, Hinkle et Gajewski, 2006). Plusieurs discussions laissent transparaître le manque de confiance ressentie envers les autres membres de la communauté et la réticence à effectuer des transactions directes avec des vendeurs inconnus. D'autres partagent l'impression que l'infrastructure et la technologie soutenant l'écosystème sont tout simplement corrompues et infiltrées, et attribuent les réussites policières à ces défaillances. Ils indiquent ne pas avoir confiance en ces outils et devoir ne dépendre que d'eux-mêmes, de toute façon.

Finalement, de nombreuses discussions soulèvent l'importance de conserver un équilibre entre l'aspect sécuritaire et l'aspect d'accessibilité et de facilité d'utilisation des cryptomarchés. L'ajout d'un trop grand nombre de mesures supplémentaires aurait comme effet bénéfique de rendre l'environnement plus sécuritaire, mais rendrait la réalisation des activités au sein des plateformes nettement plus difficile et moins accessible pour plusieurs. Alors que certains indiquent que l'accès vers les ressources d'informations est plus restreint et complexe, d'autres font état des étapes et du temps supplémentaires requis pour rejoindre certaines plateformes qui ont rendu leur accès plus sécurisé – notamment en établissant des tests CAPTCHA ou en imposant des facteurs restrictifs à l'admission de nouveaux membres. Quelques participants indiquent même posséder les compétences et les connaissances nécessaires, mais admettent perdre plaisir à fréquenter l'environnement devant les processus de plus en plus longs et complexes pour simplement accomplir une transaction.

5. 5 Les cryptomarchés – toujours un choix avantageux?

L'accès aisé aux plateformes (Martin et al., 2019b; Aldridge et al., 2018), leur facilité d'utilisation (Martin, 2014a), et l'aspect sécuritaire propre aux cryptomarchés étaient les principaux avantages que ces derniers détenaient sur les marchés de drogues physiques (Martin et al., 2019b; Evangelista et al., 2018, Aldridge et al., 2018; Martin, 2014a; Aldridge et Décary-Hétu 2016, DiPiero, 2017). L'aspect rationnel soutenant la décision d'entreprendre des activités dans ce milieu était évident : les participants investissaient moins d'efforts et de temps dans la réalisation de leurs transactions, tout en s'exposant à un nombre réduit de risques (Aldridge et Askew, 2017). À la lueur de notre étude, il est cependant plus difficile d'admettre que le calcul coût-bénéfice mène toujours au même résultat : les impacts pratiques sur les marchés sont nombreux, la confiance des membres est ébranlée et la perception des risques est à la hausse. Les participants doivent mettre davantage d'efforts pour se protéger et accéder aux différentes ressources. De nombreuses pistes de solutions sont suggérées dans les discussions, mais chaque suggestion génère des retenues de la part des membres. Une perception d'instabilité et d'insécurité semble s'être installée dans la communauté, et un essoufflement se fait sentir. Bien sûr, nous ne pouvons attribuer l'ensemble de ces effets seulement aux deux interventions à

l'étude; plusieurs commentaires recueillis font d'ailleurs état de la succession des opérations policières qui ont eu lieu contre l'écosystème dans les dernières années, et l'accumulation des chocs serait une cause de la fatigue ressentie par la communauté. Le plus récent rapport de Chainalysis (2021) indique que, malgré des revenus records en 2020, le nombre de transactions individuelles effectuées dans les cryptomarchés aurait chuté près de 20% par rapport à l'année 2019, ce qui sous-entendrait une diminution du nombre de clients actifs sur les plateformes. Il semble donc possible que l'accumulation des frappes successives des forces de l'ordre au cours des dernières années ait porté fruit : le calcul coût-bénéfice lié au fait de prendre part aux activités dans les cryptomarchés pourrait ne plus sembler attrayant pour plusieurs.

Conclusion

L'objectif principal de ce mémoire était de comprendre les impacts ressentis par les participants aux cryptomarchés suite aux opérations policières non traditionnelles. Pour y parvenir, nous avons procédé à une étude de cas impliquant deux interventions innovatrices qui ont eu lieu récemment. En mai 2019, la plateforme informationnelle DeepDotWeb était fermée par les forces de l'ordre (United States of America v T. Prihar et M. Phan, 2019; Europol, 2019). Ces derniers parvenaient ainsi à retirer un outil facilitateur important pour les membres de la communauté. Le 22 septembre 2020 fut annoncée l'arrestation de 179 vendeurs actifs dans les cryptomarchés, dans le cadre de l'opération DisrupTor (U. S. Department of Justice, 22 septembre 2020). Ces deux interventions sortaient du cadre traditionnel des interventions policières menées contre les cryptomarchés, où la majorité des opérations visent la fermeture d'une plateforme et l'arrestation de ses administrateurs dans une intervention de type « crackdown ». Étant donné que peu d'études se sont attardées à l'efficacité de ces interventions sur l'écosystème des cryptomarchés, il existe une carence dans la littérature à ce sujet. Nous avons donc porté une attention particulière aux effets ressentis au niveau de l'accessibilité ainsi qu'aux changements dans la perception des risques des usagers. L'utilisation des plateformes et de leurs ressources semblant désormais être plus difficile et risquée, nos résultats nous ont permis de remettre en question la rationalité derrière le choix des utilisateurs de poursuivre leurs activités au sein de cet écosystème. Alors que de nombreuses possibilités d'adaptation et d'innovation ont été suggérées par les participants, nous nous sommes également aperçus que l'application des potentielles mesures proposées ne pourrait pas être implantée et adoptée par une importante partie de la communauté. Les résultats de notre recherche nous permettent d'avoir une meilleure compréhension de la façon dont les participants ressentent et subissent les impacts d'un choc externe envers leur environnement. Cela pourrait servir aux forces de l'ordre dans le développement de nouvelles stratégies d'intervention, alors que nombreux sont ceux qui considèrent que les connaissances et les ressources des organisations policières amenées à intervenir contre les cybercriminels présenteraient d'importantes limites (Hadlington et al., 2021; Goodison et al., 2019).

Cette étude présente certaines limites. Dans le chapitre présentant notre collecte de données, nous avons déjà discuté des limites méthodologiques inhérentes aux données utilisées. D'abord, la véracité des messages recueillis est difficile à vérifier dans un contexte où ils ont été récoltés de manière anonyme, dans un espace virtuel (Bradley et Stringhini, 2019; Childs et al., 2020; Enghoff et Aldridge, 2019; Barratt et al., 2017 ; Seale et al., 2009). De plus, nous sommes restés limités à un rôle d'observateur, ne pouvant participer d'aucune manière aux discussions et au développement des idées (Seale et al., 2009). L'importante quantité de données amassées nous a cependant permis d'accéder à une vision globale suffisamment détaillée des thèmes dominants présents dans les messages recueillis, et cela ne nous a posé aucun problème dans l'atteinte de nos objectifs. L'utilisation d'interviews dans un contexte virtuel est plutôt rare et n'a pas été réalisée à maintes reprises (Hutchings, Clayton et Anderson, 2016 ; Barratt et al., 2016), mais pourrait s'avérer une piste intéressante pour une étude future. En effet, le fait de jouer un rôle actif dans la collecte de données qualitatives permet au chercheur de pousser la réflexion et d'approfondir certains sujets qui, autrement, resteraient inexplorés (Seale et al., 2019). Ainsi, une exploration plus en profondeur des résultats obtenus lors de notre étude pourrait être pertinente dans la consolidation de nos interprétations.

Utiliser la méthodologie quantitative pourrait également s'avérer être une approche intéressante, notamment dans le but de valider la base théorique avancée dans le cadre notre recherche. Alors que la méthodologie qualitative permet une compréhension d'un phénomène (Tewksbury, 2009 ; Zhang et Wildemuth, 2009), la méthodologie quantitative offre la possibilité de tester les hypothèses avancées (Jones, 2020 ; Merriam et Tisdell, 2015) et d'expliquer le phénomène exposé (Boucherf, 2016). Mises ensemble, ces deux méthodes de recherche se complètent (Boucherf, 2016) ; mener une étude quantitative pourrait donc permettre de valider nos interprétations et offrir un portrait statistique de certains des effets que nous avons identifiés.

Finalement, notre collecte de données s'est étendue sur une période de six mois après chacune des interventions. Au-delà de cette période, nous avons remarqué une saturation dans les données cumulées, et continuer notre collecte se serait avéré être non pertinent dans la réalisation de nos objectifs. Nous avons donc étudié les perceptions des participants sur une période limitée. Or, une importante majorité des études étudiant les impacts des interventions policières sur les

cryptomarchés observent que les résultats sont limités et de courte durée ; ces observations indiquent que la plupart des effets sont ressentis jusqu'à une période de six mois, avant un retour à la normale (Bhaskar et al., 2019; Ladegaard, 2019; Soska et Christin, 2015; van Buskirk et al., 2017; Norbutas et al., 2020). La limite temporelle de notre collecte de donnée ne nous permet donc pas d'analyser la longévité des impacts des interventions non traditionnelles et si, à l'inverse des interventions régulières, ces stratégies parviennent à ébranler l'écosystème sur une plus longue durée. Nous considérons qu'il serait donc intéressant de reproduire une étude semblable dans le futur, afin d'établir si les interventions innovatrices utilisées par les forces de l'ordre pour mettre fin aux activités des cryptomarchés créent des impacts à long terme et si elles permettent réellement une efficacité différente des interventions traditionnelles.

Références

Afilipoaie, A. et Shortis, P. (2018). Crypto-market Enforcement – New Strategy and Tactics, *GPDO Situation Analysis – June 2018*, 6p.

Aitken, C., Moore, D., Higgs, P., Kelsall, J., et Kerger, M. (2002). The impact of a police crackdown on a street drug scene: evidence from the street. *International journal of drug policy*, 13(3), 193-202.

Aldridge, J., et Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, 41, 101-109.

Aldridge, J., et Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, 35, 7–15.

Aldridge, J., Stevens, A. et Barratt, M. J. (2018). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction*, 113 (5), 789-796.

Alinsato, A. S. (2012). Relecture de la rationalité du cybercriminel : quelques éléments d'analyse théorique, *Revue d'Économie Théorique et Appliquée*, 2 (2), 155-176.

Anadòn, M. et Guillemette, F. (2007). La recherche qualitative est-elle nécessairement inductive?, *Recherches Qualitatives, Hors-série* (5), 26-37.

Bagley, M. B. (1988). The New Hundred Years War? US National Security and the War on Drugs in Latin America. *Journal of Interamerican Studies and World Affairs*, 30(1), 161-182.

Bancroft, A. (2017). Responsible use to responsible harm: Illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk and Society*, 19(7–8), 336–350.

Bancroft, A. et Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users : Purity, embodied experience, craft and chemical knowledge, *International Journal of Drug Policy*, 35, 42-49.

Barratt, M. J. (2015). Review of 'Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs' by James Martin. *Drug and Alcohol Review*, 34, 458– 459.

Barratt, M. J. et Aldridge, J. (2020) No magig pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions, *International Journal of Drug Policy*, [Article in Press].

Barratt, M. J., Ferris, J. A., et Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. *Addiction*, 109(5), 774-783.

Barratt, M. J., Ferris, J. A., Zahnow, R., Palamar, J. J., Maier, L. J. et Winstock, A. R. (2017). Moving on from representativeness: Testing the utility of the Global Drug Survey, *Substance Abuse: Research and Treatment*, 11, 1-17.

Barratt, M. J., Lenton, S., Maddox, A. et 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.

Baxter, P. et Jack, S. (2008). Qualitative Case Study Methodology: Study design and Implementation for Novice Researchers, *The Qualitative Report*, 13(4), 544-559.

Becker, H. S. (1998). The epistemology of Qualitative Research, dans R. Jessor, A. Colby et R. A. Shweder (eds), *Ethnography and human development : Context and meaning in social inquiry*, Chicago : University of Chicago Press, pp. 53-71.

Best, D., Strang, J., Beswick, T., et Gossop, M. (2001). Assessment of a Concentrated, High‐Profile Police Operation. No Discernible Impact on Drug Availability, Price or Purity. *British journal of Criminology*, 41(4), 738-745.

Bhaskar, V., Linacre, R., et Machin, S. (2019). The economic functioning of online drugs markets, *Journal of Economic Behavior et Organization*, 159, 426-441.

Bossler, A. M. (2021). Perceived Formal and Informal Sanctions in Deterring Cybercrime in a College Sample, *Journal of Contemporary Criminal Justice*, 37 (3), 452-470.

Boucherf, K. (2016). Méthode quantitative vs méthode qualitative? : Contribution à un débat, *Les cahiers du cread*, 116, 9-30.

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

Braun, V. et Clarke, V. (2006). Using thematic analysis in psychology, *Qualitative Research in Psychology*, 3(2), 77-101.

Brisset, K et Naegelen, F. (2008). Enchères en ligne et E-commerce, *Revue française d'économie*, 23 (1), 165-201.

Broadhurst, R., Ball, M., Jiang, C. X., Wang, J. et Trivedi, H. (2021). Impact of Darknet Market Seizures on Opioid Availability, *Research Report no. 18.* Canberra : Australian Institute of Criminology. 73p. https://www.aic.gov.au/publications/rr/rr18

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.

Buchanan, J. et Young, L. (2000) 'The War on Drugs – A War on Drug Users'. *Drugs: Education, Prevention Policy*, 7(4), 409-422.

Burla, L., Knierim, B., Barth, et Liewald, K. (2008). From text to codings: Intercoder reliability Assessment in Qualitative Content Analysis. *Nursing Research*, 57(2), 113-117. DOI:10.1097/01.NNR.0000313482.33917.7d

Buxton, J., et Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy Brief*, 7, 1-24.

Caleb. (2019, 7 Mai). What do we know about the deepdotweb seizure? *Medium*. Repéré à [https://medium.com/@c5/what-do-we-know-about-the-deepdotweb-seizure-98ca45de9987]

Caulkins, J. P. (1993). Local Drug Markets' Response to Focused Police Enforcement, *Operations Research,* 4(5), 848-863.

Caulkins, J. P. et Reuter, P. (1998). What Price Data Tell Us about Drug Markets, *Journal of Drug Issues* 28(3), 593–612.

Chalfin, A. et McCrary, J. (2017). Criminal Deterrence: A review of the literature, *Journal of Economic Literature,* 55 (1), 5-48.

Chainalysis (2020). The 2020 State of Crypto Crime : Everything you need to know about darknet markets, exchange hacks, money laundering and more. *Chainalysis*. https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

Chainalysis (2021). The 2021 State of Crypto Crime : Everything you need to know avbout ransomware, darknet markets, and more. *Chainalysis*. https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

Chan, J., He, S., Qiao, D., Whinston, A. B., (2019). Shedding Light on the Dark : The Impact of Legal Enforcement on Darknet Transactions. *NET Institute, Working Paper* #19-08

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.

Cho S.Y., Wright J. (2019). Into the Dark: A Case Study of Banned Darknet Drug Forums. In: Weber I. et al. (eds) *Social Informatics. SocInfo 2019*. *Lecture Notes in Computer Science* (11864). Springer, Cham

Christin, N. (2013). Traveling the silk road: a measurement analysis of a large anonymous online marketplace. *WWW '13*. 213-224

Cohen, J., Gorr, W., et 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.

Cornish, D. B., et Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4), 933-948.

Cox, J. (2016, June 14). More people than ever say they get their drugs on the dark web. *Motherboard, Vice*. Repéré à https://www.vice.com/en/article/8q88wv/more-people-than-ever-say-they-get-their-drugs-on-the-dark-web

Crosset, V. (2020). Être visible sur et par internet : Le cas de l'État islamique, Thèse de doctorat, Université de Montréal, 414p.

Curran, K., Dale, M., Edmunds, M., Hough, M., Millie, A., et Wagstaff, M. (2005). Street crime in London: deterrence, disruption and displacement.

Cusson, M. (1993). Situational deterrence: Fear during the criminal event, *Crime Prevention Studies*, 1, 55–68.

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.

Décary-Hétu, D., Mousseau, V., et Vidal, S. (2018). Six years later: Analyzing online black markets involved in herbal cannabis drug dealing in the United States. *Contemporary Drug Problems*, 45(4), 366-381.

Décary-Hétu, D. et Quessy-Dore, O. (2017). Are repeat buyers in Cryptomarkets Loyal Customers? Repeat Business Between Dyads of Cryptomarket Vendors and Users, *American Behavioral Scientist*, 61(11), 1341-1357.

Demant, J., Bakken, S. A., Oksanen A. et Gunnlaugsson, H. (2019). Drug dealing on Facebook, Snapchat and Instagram : A qualitative analysis of novel drug markets in the Nordic countries, *Drug and Alcohol Review,* 38, 377-385.

DiPiero, C., (2017). Deciphering Cryptocurrency: Shining a Light on the Deep Dark Web. U. Ill. L. Rev

Dolliver, D. S. et Kenney, J. L. (2016) Characteristics of Drug vendors on the Tor Network : A Cryptomarket Comparison, *Victims et Offenders,* 11(4), 600-620.

Edmunds, M., Hough, M., et Urquía, N. (1996). Tackling local drug markets (Vol. 80). London: Home Office Police Research Group.

Ellinger, A. D. et McWhorter, R. R. (2016). Qualitative Case Study Research as Empirical Inquiry, *International Journal of Adult Vocational Education and Technology*, 7(3), 1-13

Enghoff, O. et Aldridge, J. (2019). The value of unsolicited online data in drug policy research, *International Journal of Drug Policy*, 73, 1-9.

Erickson, P. G., van der Maas, M. et Hathaway, A. D. (2013). Revisiting Deterrence: Legal knowledge, Use context and arrest perception for cannabis, *Czech Sociological Review*, 49 (3), 427-448

European Monitoring Centre for Drugs and Drug Addiction [EMCDDA] (2016), The internet and drug markets, EMCDDA Insights 21, *Publications Office of the European Union*, Luxembourg. 80p.

Europol, (2017). Drugs and the Darknet. Perspectives for enforcement, research and policy, *EMCDDA*, 85p.

Europol, (2019a, 3 mai). Double Blow to Dark Web Marketplaces, *Press Release.* Repéré à [https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces]

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

Europol, (2020, 22 septembre). International Sting Against Dark Web Vendors leads to 179 Arrests, *Press Release.* Repéré à [https://www.europol.europa.eu/newsroom/news/international-sting-against-dark-web-vendors-leads-to-179-arrests]

Evangelista, A., Allodi, L., et Cremonini, M. (2018). Darknet Markets: Competitive Strategies in the Underground of Illicit Goods. *Eindhoven University of Technology*, 13, 14p.

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.

Feagin, J. R., Orum, A., Sjobert, G. (1991). *A case for the Case Study*. The University of North Carolina Press. 290p.

Federal Bureau of Investigation (2019). Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet. Repéré à [https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales]

Fereday, J. et Muir-Cochrane, E. (2006). Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development, *International Journal of Qualitative Methods*, 5(1), 80-92.

Flanagin, A. J., Metzger, M. J., Pure, R. et Markov, A. (2011). User, Generated ratings and the evaluation of credibility and Product quality in Ecommerce transaction, *44th Hawaii International Conference on System Sciences*, 1-10.

Gammelgaard, B. (2017). Editorial: The qualitative case study, *The International Journal of Logistics Management*, 28(4), 910-913.

Gibbs, J. P. (1975). Crime, punishment, and deterrence. New York: Elsevier, 259p.

Goodison, S. E., Woods, D., Barnum J. D., Kemerer, A. R., et Jackson, B. A., (2019). Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web, *RAND Corporation*, RR-2704-NIJ, 27p.

Goullé, J.-P., Mura, P. and Guerbet, M. (2017). Le cybermarché noir des drogues illicites, *Toxicologie Analytique et Clinique*, 29 (2), S20.

Green, L. (1995). Cleaning up drug hot spots in Oakland, California : The displacement and diffusion effects, *Justice Quarterly*, 12(4), 737-754.

Grimani, A., Gavine A. et Moncur, W. (2020). An Evidence Synthesis of Covert Online Strategies Regarding Intimate Partner Violence, *Trauma, Violence, et Abuse*, 1-13.

Gupta, A., Maynard S. B. et Ahmad, A. (2018). The dark web as a phenomenon: a review and research agenda. *The University of Melbourne*. 11p.

Gwet, K. L. (2015). On Krippendorff's Alpha Coefficient. Récupéré à [https://www.researchgate.net/publication/267823285_On_Krippendorff's_Alpha_Coefficient]

Hadlington, L., Lumsden, K. et Black, A. (2021). A qualitative exploration of Police Officers' Experiences, Challenges and Perceptions of Cybercrime, *Policing: A journal of Policy and Practice*, 15(1), 34-43

Hamel, J., (1998). Défense et illustration de la méthode des études de cas en sociologie et en anthropologie. Quelques notes et rappels, *Cahier Internationaux de Sociologie*, 104, pp. 121-138

Hamilton-Smith, N. (2002). Anticipated consequences: developing a strategy for the targeted measurement of displacement and diffusion of benefits. *Crime prevention studies*, 14, 11-52.

Hancock, D. R., Algozzine, B. (2016). Doing case study research: A practical guide for beginning researchers. New York, NY: Teachers College Press.

Hayes, A. et Krippendorff, K. (2007). Answering the call for a standard reliability measure for coding data, *Communication Methodes and Measures*, 1(1), 77-89.

Holt, T. J. (2010) Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using OnLine Data, *Journal of Criminal Justice Education*, 21(4), 466-487.

Holt, T. J., Smirnova, O., Chua, Y. T., et Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global crime*, 16(2), 81-103.

Holtz, P., Kronberger, N., & Wagner, W. (2012). Analyzing internet forums: A practical guide. *Journal of Media Psychology: Theories, Methods, and Applications*, 24(2), 55-66.

Horton-Eddison, M., et Di Cristofaro, M. (2017). Hard Interventions and Innovation in Crypto-Drug Markets: The ESCROW Example. *Policy Brief*, 11.

Hough, M. et Natarajan, M. (2000). Introduction : Illegal Drug markets, Research and Policy, dans M. Hough et M. Natarajan (dir.), *Illegal Drug Markets : From Research to Prevention Policy*, (Crime Prevention Studies Vol. 11), New York : Criminal Justice Press.

Huang, E., et Liu, C. C. (2010). A study on trust building and its derived value in C2C ecommerce. *Journal of Global Business Management*, 6(1), 186-95.

Hull, G. (2017). The Effects of Police Interventions on Darknet Market Drug Prices (Thèse Senior, Collège McKenna, Claremont). Repéré à [https://www.gwern.net/docs/sr/2017-hull.pdf]

Hurlburt G (2017) Shining light on the dark web. *Computer* 50(4), 100–105.

Hutchings, A., et Holt, T. J. (2017). The online stolen data market : disruption and intervention approaches, *Global Crime*, 18(1), 11–30.

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

Im, E.-O. et Chee, W. (2006). An Online Forum As a Qualitative Research Method : Practical Issues, *Nurse Researcher,* 55(4), 267-273.

Jacobs, B. A. (1996). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly*, 13(3), 359-381.

Jacques, S. et Bonomo, E. (2017). Learning from the Offenders' Perspective on Crime Prevention, In B. Leclerc, et E. Savona, *Crime Prevention in the 21st Century*, 9-18.

Joffe, H. et Yardley, L. (2003). Content and thematic analysis. Dans D. F. Marks et L. Yardley (Dir.) *Research methods for clinical and health psychology*, London : SAGE Publications, 56-68.

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

Jones, M. R. (2020). *Law enforcement techniques in Darknet Markets : A case Study*, [Thèse de doctorat, Capitol Technology University]. ProQuest. https://www.proquest.com/docview/2465820188?pq-origsite=gscholar&fromopenview=true

Jootun, D., Mcghee, G., et Marland, G. R. (2009). Reflexivity : promoting rigour in qualitative research, *Nursing standard: official newspaper of the Royal College of Nursing*, 23(23), pp. 42-46

Kamphausen, G., et Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy*, 73, 281-287.

Kastrenakes, J. (2020, 1er décembre). Reddit reveals daily active user count for the first time : 52 million. *The Verge*. Repéré à [https://www.theverge.com/2020/12/1/21754984/reddit-dau-daily-users-revealed].

Kerr, O. S. (2004). Virtual Crime, Virtual Deterrence: A Skeptical View of Self-help, Architecture and Civil Liability, *Journal of Law, Economics and Policy*, 1 (1), 197-214

Kerr, T., Small, W. et Wood, E. (2005). The public health and social impacts of drug market enforcement : A review of the evidence, *International Journal of Drug Policy*, 16(4), 210-220.

Kleiman, M. A., et Smith, K. D. (1990). State and local drug enforcement: In search of a strategy. *Crime and justice*, 13, 69-108.

Kleiman, M. (1988). Crackdowns: The Effects of Intensive Enforcement on Retail Heroin Dealing. *Working Paper #88-01-11*. Cambridge (Massachusetts): Program in Criminal Justice Policy and Management, Harvard University.

Krippendorff, K. (2004). Measuring the Reliability of Qualitative Text Analysis, *Quanlity et Quantity*, 38, 787-800.

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).

Ladegaard, I. (2018). We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *The British Journal of Criminology*, 58(2), 414–433.

Ladegaard, I. (2019). “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.

Ladegaard, I. (2020). Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows. *Social Forces*, 99(2), 532-559.

Lane, B. R., Lacey, D., Stanton, N. A., Matthews, A., et Salmon, P. M., (2019). The Dark Side of the Net: Event Analysis of Systemic Teamwork (EAST) Applied to Illicit Trading on a Darknet Market. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Sage CA: Los Angeles, CA: SAGE Publications, 62(1), 282-286.

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.

Leukfeldt, R. et Jansen J. (2020). Financial cybercrimes and situation crime prevention, dans Leukfeldt R. et Holt, T. J. (dir.) *The Human Factor of Cybercrime*, Routledge Studies in Crime and Society

Lorenzo-Dus, N., et Cristofaro, M. Di. (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.

MacCoun, R. J. (1993). Drugs and the law : a psychological analysis of drug prohibition, *Psychological Bulletin*, 113 (3), 497-512

Maimon, D. (2020). « Deterrence in Cyberspace : An Interdisciplinary Review of the Empirical Literature ». Dans : Holt T., Bossler A . (eds) *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham.

Maher, L. et 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.

Manchala, D. (2000). E-Commerce Trust Metrics and Models.. *IEEE Internet Computing*, 4, 36-44.

Martin, J. (2014a). Drugs on the Dark Net : How Cryptomarkets are Transforming the Global Trade in Illicit Drugs, Palgrave Pivot.

Martin, J. (2014b). Lost on the *Silk Road :* Online drug distribution and the 'cryptomarket', *Criminology et Criminal Justice*, 4(3), 351-367.

Martin, J., Cunliffe, J., et Munksgaard, R. (2019a) Cryptomarkets: A Research Companion. *Emerald Studies In Digital Crime, Technology and Social Harms*. Emerald, Bingley, UK, 214p.

Martin, J., Munksgaard, R., Coomber, R., Demant, J. et Barratt, M. J. (2019b). Selling drugs on Darkweb Cryptomarkets : Differentiated Pathways, Risks and Rewards, *British Journal of Criminology*, 60 (3), 12p.

Martineau, S. et Blais, M. (2006). L'analyse inductive générale : Description d'une démarche visant à donner un sens à des données brutes. *Recherches Qualitatives*, 26(2), 1-18.

May, T., et Hough, M. (2001). Illegal dealings: The impact of low-level police enforcement on drug markets. *European Journal on Criminal Policy and Research*, 9(2), 137-162.

Mayer, R. C., Davis, J. H. et Schoorman, F. D. (1995). An integrative model of organizational trust, *Academy of Management Review*, 20, 709-734.

Mazerolle, L., Soole, D. and Rombouts, S. (2007). Drug Law Enforcement. A review of the Evaluation Literature*, Police Quarterly*, 10 (2), 115-153.

McWilliams, JC. (1994). Book Review: Power, Ideology, and the War on Drugs: Nothing Succeeds Like Failure. *Criminal Justice Review*, 19(1), 143-145.

Merriam, S. et Tisdell, E. (2015). Qualitative research : a guide to design and implementation. New Jersey, USA : Jossey-Bass.

Mikhaylov, A. et Frank, R. (2016). Cards, Money and Thow Hacking Forums : An analysis of Online Money Laundering Schemes, *2016 European Intelligence and Security Informatics Conference*, IEEE, 80-83.

Miller, J. N. (2019). The war on Drugs 2.0: Darknet Fentanyl's rise and the effects of regulatory and law enforcement action, *Contemporary economic policy*, 38 (2), 246-257.

Moeller, K., Copes, H. et Hochstetler, A. (2016). Advancing restrictive deterrence : A qualitative meta-synthesis, *Journal of Criminal Justice*, 46, 82-93.

Moore, M. H. (1990). Supply reduction and drug law enforcement. *Crime and Justice*, 13, 109-157.

Morselli, C., Décary Hétu, D., Paquet Clouston M. et Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets, *International Criminal Justice Review*, 27(4), 237-254.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., et Voelker, G. M. (2011). An analysis of underground forums. Paper presented at the Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

Munksgaard, R. (2021). Trust and exchange : the production of trust in illicit online drug markets [Thèse de doctorat, Université de Montréal]. Papyrus. https://papyrus.bib.umontreal.ca/xmlui/handle/1866/25234

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

Munksgaard, R., Bakken, S., et Demant, J. (2017). Risk perception in emerging markets for illicit substances in Scandinavia: The effect of available information through online communities. Conference paper presented at *The Scandinavian Research Council for Criminology, Stockholm, Sweden*.

Murji, K. (1993). Drug Enforcement Strategies 1. *The Howard Journal of Criminal Justice*, 32(3), 215-230.

Nagin, D. S., Solow, R. M. et Lum, C. (2015). Deterrence, criminal opportunities, and police. *Criminology*, 53 (1), 74-100.

Norbutas, L., Ruiter, S., et Corten, R. (2020a). Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets. *International Journal of Drug Policy*, 76.

Norbutas, L., Ruiter, S., et Corten, R. (2020b). Believe it when you see it : Dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs, *Social Networks*, 63, 150-161.

Nye Jr., J. S. (2017). Deterrence and Dissuasion in Cyberspace, *International Security*, 41 (3), 44-71

O'Connell, D., Visher, C., Martin, S., Parker, L et Brent, J. (2011). Decide your time: Testing deterrence theory's certainty and celerity effects on substance-using probationers, *Journal of Criminal Justice*, 39(3), 261-267.

O'Connor, C et Joffe, H. (2020) Intercoder Reliability in Qualitative Research : Debates and Practical Guidelines, *International Journal of Qualitative Methodes*, 19, 1-13.

Oleinik, A., Popova, I. P., Kirdina-Chandler, S. et Shatalova, T. (2014) Reliability and validity in texts' content analysis : The choice of measures, *Quality et Quantity*, 48(5), 2703-2718.

Owen, G. and Savage, N. (2015). The Tor Dark Net, *Global Commission on Internet Governance Paper Series*, (20), 9p.

Pace, J. (2017). Exchange relations on the dark web, *Critical Studies in Media Communication*, 34(1), 1-13.

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.

Patel, S. (2020, 1er décembre). Reddit Claims 52 Million Daily Users, Revealing a Key Figure for Social-Media Platforms, *The Wall Street Journal*. Repéré à [https://www.wsj.com/articles/reddit-claims-52-million-daily-users-revealing-a-key-figure-for-social-media-platforms-11606822200]

Paternoster, R. (2010). How much do we really know about criminal deterrence? *Journal of Criminal law and Criminology*, 100 (3), Art. 6, 765-824

Pearson, G. (1992). The reduction of drug-related harm, *Drugs and criminal justice,* 15-29.

Porter, K. (2018). Analyzing the DarkNetMarkets subreddit for evolutions of tools and trends using LDA topic modeling. *Digital Investigation*, 26, S87-S97.

Poupart, J. (1997). L'entretien de type qualitatif : considérations épistémologiques, théoriques et méthodologiques. Dans J. Poupart, J.-P. Deslauriers, L.-H. Groulx, A. Laperrière, R. Mayer et A. P. Pires (Dir.) : *La recherche qualitative : enjeux épistémologiques et méthodologiques*. Boucherville, Québec : Gaëtan Morin éditeur.

Przepiorka, W., Norbutas, L. et Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs, *European Sociological Review*, 33(6), 752-764.

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

Ratner, C., (2002). Subjectivity and Objectivity in Qualitative Methodology, *Forum : Qualitative Social Research*, 3(3), Art. 16, 8p.

Ritchie, J., Spencer, L. et O'Connor, W. (2003). Carrying out qualitative analysis. In Ritchie, J., Lewis, J. (Eds.), *Qualitative research practice: A guide for social science students and researchers*, SAGE. 219–262.

Ryan, G et Bernard, R., (2003). Techniques to Identify Themes, *Field Methods*, 15(1), 85-109.

Scott, M. (2003). The Benefits and Consequences of Police Crackdowns, *Problem-Oriented Guides for Police Response Guide Series*, 1, 80 p.

Seale, C., Charteris-Black, J., MacFarlane, A. et McPherson, A. (2009). Interviews and Internet Forums: A Comparison of Two Sources of Qualitative Data, *Qualitative Health Research*, 20(5), 595-606.

Sherman, L. (1990). Police crackdowns: Initial and Residual Deterrence, *Crime and Justice*, 12, 1-48

Sherman, L., and D. Rogan (1995). Deterrent Effects of Police Raids on Crack Houses: A Randomized, Controlled Experiment. *Justice Quarterly* 12(4), 755–781.

Shortis, P., Aldridge, J. et Barratt, M. J. (2020). Drug Cryptomarket futures : structure, function and evolution in response to law enforcement actions, dans D. R. Bewley-Taylor et K.

Tinasti (dir.) *Research Handbook on International Drug Policy*, (Social and Political Science 2020), Edward Elgar Publishing.

Smith, M., M. Sviridoff, S. Sadd, R. Curtis, and R. Grinc (1992). The Neighborhood Effects of Street-Level Drug Enforcement. Tactical Narcotics Teams in New York: An Evaluation of TNT. New York: Vera Institute of Justice.

Smith, R. (2001). Police-Led Crackdowns and Cleanups: An Evaluation of a Crime Control Initiative in Richmond, Va. *Crime and Delinquency,* 47(1), 60–83.

Smith, R. C. et Frank, R. (2020). Dishing the Deets : How dark-web users teach each other about international drug shipments, *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 4693-4702.

Soska, K., et Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *Paper presented at the USENIX Security '15*.

Spagnoletti, P., Ceci, F. and Bygstad, B., (2018). An investigation on the generative mechanisms of Dark Net markets. *WISP 2018 Proceedings*. 20. Repéré à[https://aisel.aisnet.org/wisp2018/20]

Tewksbury, R (2009). Qualitative versus Quantitative Methods: Understanding Why Qualitative Methods are Superior For Criminaology and Criminal Justice*, Journal of Theoretical and Philosophical Criminology*, 1(1), 38-58.

Thomas D. R., (2006). Q General Inductive Approach for Qualitative Data Analysis, *American Journal of Evaluation*, 27(2), 237-246.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time, *International Journal of Drug Policy*, 56, 176-186.

U.S. Department of Justice (2019, 8 mai). 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*. Repéré à [https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales].

U. S. Department of Justice (2020, 22 septembre). 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*. Repéré à [https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales]

U. S. Department of Justice (2020a, 22 septembre). NDTX Charges Alleged Darkweb drug trafficker in DOJ Operation DisrupTor, *Press Release*. Repéré à [https://www.justice.gov/usao-ndtx/pr/ndtx-charges-alleged-darkweb-drug-trafficker-arrested-doj-operation-disruptor].

U. S. Department of Justice, (2020b, 22 septembre). International Law Enforcement Operation Targeting Opioid Traffickers on the Darknet Results in over 170 Arrests Wolrdwide and the Seizure of Weapons, Drugs and over $6.5 Million, *Press Release*. Repéré à [https://www.justice.gov/opa/pr/international-law-enforcement-operation-targeting-opioid-traffickers-darknet-results-over-170]

United States of America v T. Prihar et M. Phan (2019). 18 U.S.C. § 1956(h), United States District Court for the Western District of Pennsylvania. Repéré à [https://www.justice.gov/opa/press-release/file/1161011/download]

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 Buskirk, J., Roxburgh, A., Farrell, M., et Burns, L. (2014). The closure of the silk road: what has this meant for online drug trading? *Addiction*, 109(4), 517–518.

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. (2015). Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs, *Global Crime*, 16(3), 262-264.

Van Manen, M. (1990). Beyond assumptions : Shifting the limits of action research, *Theory Into Practice*, 29(3), 152-157.

VanNostrand, L. M., et Tewksbury, R. (1999). The motives and mechanics of operating an illegal drug enterprise. *Deviant Behavior*, 20(1), 57-83.

van Wegberg, R., etVerburgh, T. (2018). Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In *Proceedings of the Evolution of the Darknet Workshop,* 1-5.

Villemagne, C. (2006). Des choix méthodologiques favorisant une approche inductive : le cas d'une recherche en éducation relative à l'environnement, *Recherches Qualitatives*, 26(2), 131-144.

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.

Winstock, A.R., Barratt, M.J., Maier, L.J, Aldridge, A., Zhuparris, A., Davies, E., Hughes, C., Johnson, M., Kowalski, M. et Ferris, J. (2019). *Global Drug Survey (GDS) 2019 Key Findings Report*. Repéré à [https://issuu.com/globaldrugsurvey/docs/gds2019_key_findings_report_may_16_]

Woo, S. E., O'Boyle, E et Spector, P. (2016). Best Practices in developing, conducting and evaluating inductive research, *Human Resource Management Review*, 27(2), 255-264.

Wood, E., Spittal, P. M., Small, W., Kerr, T., Li, K., Hogg, R. S., Tyndall, M. W., Montaner, J. S. G. et Schechter, M. T. (2004). Displacement of Canada's largest public illicit drug market in response to a police crackdown. *Cmaj*, 170(10), 1551-1556.

Xiong, L., et Liu, L. (2003). A reputation-based trust model for peer-to-peer eCommerce communities. *IEEE International Conference on E-Commerce*. 275 - 284.

Yin, R. K. (2003). Case study research: Design and methods (3rd ed.). Thousand Oaks, CA: Sage.

Zambiasi, D. (2020) : Drugs on the web, crime in the streets: The impact of Dark Web marketplaces on street crime, *Working Paper Series*, No. WP20/25, University College Dublin, UCD Centre for Economic Research, Dublin, 48p.

Zhang, Y. et Wildemuth, B. M., (2009). Qualitative Analysis of Content, In: B. M. Wildemuth, Ed., Applications of Social Research Methods to Questions in Information and Library Science, Libraries Unlimited, 1-12.

Zimmer, L. (1990). Proactive Policing Against Street-Level Drug Trafficking. *American Journal of Police*, 9(1), 43–74.