Université de Montréal

La collaboration internationale dans les enquêtes sur le darkweb: exploration des types et des motivations selon l'expérience des policiers

par Marie-Pier Villeneuve-Dubuc

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

Mai 2023

Université de Montréal

École de criminologie, Faculté des arts et des sciences

Ce mémoire intitulé

La collaboration internationale dans les enquêtes sur le darkweb: exploration des types et des motivations selon l'expérience des policiers

Présenté par

Marie-Pier Villeneuve-Dubuc

A été évalué par un jury composé des personnes suivantes

Rémi Boivin

Président-rapporteur

David Décary-Hétu

Directeur de recherche

Benoit Dupont

Codirecteur

Valentin Pereda

Membre du jury

Résumé

Mondialement, les organisations policières sont responsables de résoudre les crimes qui sont commis physiquement dans les juridictions qui leur sont attribuées. Cependant, ce fonctionnement n'est pas adapté aux cybercrimes, considérant qu'ils sont commis virtuellement et non physiquement dans l'espace. Depuis les dernières années, des milliers de criminels utilisent le darkweb, la portion cachée de l'Internet, afin de commettre des crimes à l'insu de toutes détections policières. En effet, les forces de l'ordre se retrouvent bien souvent dans l'incapacité d'intervenir face aux cybercrimes à cause du manque de ressources financières et humaines ainsi que du manque de formations adéquates. Une solution proposée face à ce problème est de favoriser les collaborations internationales qui transcendent les juridictions. Cependant, la littérature sur le sujet de la collaboration internationale n'est plus d'actualité et ne prend pas en considération les défis causés par les technologies. Étant la première étude à se pencher sur cette problématique, ce mémoire a pour objectif général de comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb. Précisément, cette étude exploratoire désire (1) décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière et (2) décrire et comprendre les types de collaboration nécessaire à la réalisation d'une enquête policière sur le darkweb. Pour ce faire, nous utilisons une approche internationale et centrée sur les policiers grâce à un corpus de 20 entretiens avec des enquêteurs de cinq pays (Canada, États-Unis, Royaume-Uni, Australie et Suède). Cette recherche s'appuie sur le point de vue des participants afin d'apprécier leurs réalités et leurs expériences. À l'aide d'une analyse thématique classique, nous avons décrit cinq principales motivations et trois types de collaboration expérimentés par les sujets. Ce mémoire permet de mettre en lien des thématiques distinctes dans la littérature, de générer de nouvelles connaissances et d'établir les bases conceptuelles pour de futures recherches. Les résultats illustrent la pertinence et la nécessité de mettre de l'avant les collaborations internationales afin d'accroître le succès des enquêtes policières sur les crimes commis à l'aide du darkweb.

Mots-clés : Enquêtes policières, darkweb, collaboration internationale, motivations, types, coopération.

Summary

Globally, police organizations are responsible for solving crimes committed physically in their assigned jurisdictions. Considering that they are committed virtually and not physically in space, this system is not adequate for tackling cybercrimes. In the last decades, thousands of criminals have been using the darkweb, the hidden part of the Internet, to commit crimes without police detection. Indeed, law enforcement agencies are often unable to intervene in cybercrimes due to a lack of financial, human resources and adequate training. One proposed solution to this problem is to foster international collaborations that transcend jurisdictions. However, the literature about international collaboration is outdated and does not consider the challenges caused by technology. As the first study to address this issue, the overall goal of this master's thesis is to understand international collaborations in police investigations of darkweb crimes. Specifically, this exploratory study seeks to (1) describe and understand the motivations that drive investigators to collaborate outside of their police agency and (2) describe and understand the types of collaboration required to conduct a police investigation on the darkweb. We used an international and police-centric approach through a corpus of 20 interviews with investigators from five countries (Canada, United States, United Kingdom, Australia, and Sweden). This research draws on the participants' perspectives to appreciate their realities and experiences. Using the traditional thematic analysis, we described five main motivations and three types of collaboration experienced by the subjects. This dissertation connects distinct themes in the literature, generates new knowledge, and establishes the conceptual basis for future research. The results illustrate the relevance and necessity of improving international collaborations to increase the success of police investigations of darkweb-related crimes.

Keywords: Police investigations, darkweb, international collaboration, motivations, types, cooperation.

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

ASIO: *Australian Security Intelligence Organisation*

CNC3 : Centre nationale de la coordination des cybercrimes

DEA: *Drug Enforcement Agency*

EC3: *European Cybercrime Center*

FBI: *Federal Bureau of Investigation*

FCB: *First Commercial Bank*

IC3: *Internet Crime Complaint Center*

ICT: *Information and Communications Technology sector*

ILO: *International liaison officers*

IP: *Internet Protocol*

J-CAT: *Joint Cybercrime Action Taskforce*

MLAT: *Mutual Legal Assistance Treaty*

NW3C: *National White Collar Crime Center*

ONU : Organisation des Nations Unies

ONUDC : Office des Nations Unies contre la drogue et le crime

P2P: *Peer-to-peer*

PPP: *Public-Private Partnerships*

SCRS : Service canadien de renseignement de sécurité

VPN: *Virtual private network*

WWW: *World Wide Web*

Remerciements

À la fin de mon baccalauréat, j'ai fait des rencontres qui ont changé la trajectoire de ma carrière. Je tiens à remercier chaleureusement ces personnes pour leur confiance et leur support dès le début de mon parcours.

Tout d'abord, je tiens à remercier mes directeurs de recherche David et Benoit. Ils m'ont offert du support et ont fait part d'une grande disponibilité tout au long de mon parcours. Je tiens spécialement à remercier David et Andréanne, qui m'ont offert mon premier contrat d'auxiliaire de recherche. Cela m'a permis de découvrir le monde académique et m'a encouragé à poursuivre aux études supérieures. De même pour Benoit et Fyscillia, qui m'ont confié la tâche de rédactrice de vulgarisation scientifique alors que j'avais une expérience professionnelle tout autre. En particulier David, qui a eu le courage de confier l'organisation d'un colloque international à une étudiante de première session à la maîtrise, merci. Toutes ces opportunités m'ont permis de grandir énormément. Depuis, j'ai eu l'occasion de travailler sur plusieurs projets, dont j'ai eu l'opportunité de présenter dans de nombreuses conférences internationales.

Après avoir payé chaque sou de mes études de premier cycle en jonglant jusqu'à quatre emplois à la fois, je suis extrêmement honorée d'avoir été récipiendaire des bourses d'excellence du Canada (CRSH) et du Québec (FRQSC) pour mes études supérieures. De plus, j'ai eu l'honneur de recevoir l'aide financière du CRPC, ce qui m'a aussi permis de travailler à temps plein sur des sujets qui m'intéressaient grandement.

Je tiens à remercier mes collègues et amies du laboratoire DARC, vous m'avez offert des souvenirs que je vais chérir toute ma vie. Longue vie aux 4 à 7 et aux *memes* sur le tableau blanc.

Mention spéciale à mes collègues avec qui j'ai eu la chance de créer des initiatives (le Forum Étudiant d'Échange et d'Information en Cybercriminologie et le Journal Universitaire de Criminologie). Nous avons démontré un engagement hors du commun et un fort désir d'aider les autres tout en faisant rayonner notre belle discipline qu'est la criminologie.

Plus personnellement, je tiens à remercier mon copain, qui est le meilleur partenaire et mon plus grand cheerleader. Merci d'être la personne la plus naturellement heureuse et bienveillante. Tu m'encourages constamment à gravir les plus hauts sommets tout en gardant la tête haute.

Je tiens à remercier mes amies de longue date qui, malgré leur incompréhension de ma volonté à poursuivre des études supérieures, m'encouragent à poursuivre mes rêves, et ce, même s'ils apparaissent bien compliqués.

Un dernier merci à ma famille, particulièrement à ma mère, qui m'encourage et m'offre toujours du réconfort lors des moments difficiles. Merci à ma grande sœur. Tu m'as motivée à faire des études universitaires, en me montrant que c'était possible malgré tous les sacrifices.

En bref, les dernières années ont été très enrichissantes et m'ont amené une croissance personnelle et professionnelle impressionnante. Je souhaite à chaque étudiant de saisir les nombreuses opportunités qu'offrent l'École de Criminologie et le CICC ou d'avoir le courage de vous les créer. Ne sous-estimez pas le support qui vous entoure.

Bonne lecture,

Psst. Aux étudiants qui lisent ceci (car soyons honnête, le public cible des mémoires consiste aux étudiants en rédaction ou des parents/amis forcés contre leur gré), ne lâchez pas, ça en vaut la peine!

INTRODUCTION

« […] There is an urgent need to strengthen cooperation to counter the spread of crimes committed using technologies more effectively at the national, regional, and international levels » (Nations Unies, 2023a, 20 avril).

En avril 2023 a eu lieu la plus récente rencontre des Nations Unies sur la potentielle Convention internationale pour la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles (Nations Unies, 2023b) qui a fait preuve d'une grande attention médiatique. Cette réunion se concentrait précisément sur la coopération internationale et la mise en œuvre de ladite convention (Clasen, 2023). Celle-ci a pour objectif d'unir les pays afin de pallier la hausse constante des cybercrimes mondialement. Toutefois, il est particulièrement laborieux d'obtenir l'accord unanime des pays membres sur des sujets aussi sensibles que le transfert de données personnelles, l'extradition judiciaire, les enquêtes policières conjointes, l'accès aux données transfrontalières et l'application de techniques d'enquêtes spéciales (Clasen, 2023). Cette convention évoque la nécessité d'unir les forces policières et judiciaires afin d'avoir un réel impact sur les cybercrimes, étant définis comme des crimes utilisant des technologies de l'information ou de communications (Nations Unies, 2023a). Le comité chargé d'élaborer la convention reconnait explicitement l'urgence de faciliter le partage des preuves digitales, d'assurer que les enquêtes et la poursuite des criminels soient réalisées rapidement, et ce, grâce à la coopération internationale ainsi qu'à l'adoption de lois internationales qui assurent la protection de la société contre ces crimes sans frontières (voir Nations Unies, 2023a).

En effet, l'avènement des crimes impliquant des technologies cause de sérieux tort à la société. Les criminels ont mobilisé les technologies qui assurent leur anonymat sur l'Internet, comme le darkweb, afin de se protéger du système judiciaire. Ainsi, de nombreux criminels échappent au contrôle des forces de l'ordre à cause de l'incapacité de celles-ci à les identifier. Par ailleurs, le grave manque de ressources humaines et financières ainsi que l'insuffisance des formations offertes aux policiers sont des causes importantes de l'incapacité des forces de l'ordre à répondre à leur mandat de protection des citoyens quant aux cybercrimes (Brown, 2015; Harkin, Whelan et Chang, 2018; Faubert et al., 2021). Faisant face à ce grave problème, de nombreux chercheurs ont tenté d'identifier des solutions afin d'améliorer la réponse policière en matière de cybercriminalité. Une solution proposée consiste à inciter internationalement les agences policières à joindre leur renseignement et leur pouvoir juridique en collaborant (Burns et coll., 2004; Sarre et coll., 2018).

Malgré l'avènement de l'intérêt politique et légal qu'amène la nouvelle convention de l'ONUDC (Office des Nations Unies contre la drogue et le crime), la littérature empirique sur le sujet de la collaboration internationale n'est pas adaptée au contexte précis des cybercrimes, ayant été construite dans l'objectif d'améliorer la réponse policière sur les crimes reliés aux actes terroristes, au trafic de drogues et au crime organisé.

Dans l'intention de contrer ce vide empirique, ce mémoire a comme objectif de *comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb* grâce à une méthodologie d'analyse qualitative issue d'entrevues réalisées auprès de 20 enquêteurs policiers qui proviennent de 5 pays développés. Afin d'obtenir une compréhension en profondeur, cette recherche exploratoire est séparée en deux articles scientifiques ayant des fins complémentaires. Spécifiquement, le premier article a pour but de décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière. De son côté, le deuxième article vise à décrire et comprendre les types de collaboration mobilisés dans le cadre d'une enquête policière sur le darkweb. À l'aide des preuves empiriques qui seront présentées, nous espérons mettre en lumière la pertinence des collaborations. En plus, nous souhaitons sensibiliser les praticiens sur l'environnement législatif, politique et structurel complexe qui influence significativement le déroulement des collaborations au sein de la police et de leurs partenaires.

Pour ce faire, ce mémoire est structuré en cinq chapitres. Le premier chapitre comprend une recension des écrits empiriques portant sur la collaboration policière en contexte des crimes commis sur le darkweb afin de détailler les études et les connaissances scientifiques sur les différentes thématiques qui englobent l'objet d'étude. Le second chapitre porte sur la problématique qui est ressortie de la littérature. Le troisième chapitre comprend la méthodologie afin de détailler l'échantillon ainsi que la méthode analytique mobilisée. Le quatrième chapitre contient les deux articles scientifiques qui représentent les résultats empiriques. Par la suite, le cinquième chapitre comprend la discussion qui unifie les résultats des articles tout en tissant des liens avec la littérature existante. Dans ce chapitre, nous répondrons aussi à l'objectif général de la présente étude. Pour terminer, une conclusion détaillée sera présentée afin d'exposer les implications pratiques et empiriques. En plus, les limites méthodologiques seront réitérées tout en suggérant des pistes de solutions pour les futures recherches.

CHAPITRE 1: RECENSION DES ÉCRITS

1. La collaboration internationale en contexte policier

Bien que collaboration et coopération soient des synonymes linguistiques, ces deux concepts sont parfois utilisés différemment dans la littérature scientifique. Selon le dictionnaire, la collaboration est définie comme étant une action de collaborer ou de participer à une œuvre avec d'autres individus (Collaboration, 2022). De son côté, la coopération est définie comme étant une action de coopérer afin de participer à une œuvre commune (Coopération, 2022). Cette légère différence s'explique à l'aide de la littérature sur les institutions commerciales privées. En effet, ces deux concepts impliquent de nombreux acteurs et la présence d'interactions entre différentes institutions publiques et/ou privées (Polenske, 2012). Ils peuvent être tout autant utilisés afin d'améliorer la compétitivité d'une entreprise ou d'une institution et ne peuvent être différenciés par la durée de complétion, car plusieurs facteurs économiques, sociaux et politiques font varier leurs durés (Polenske, 2012). Cependant, les relations de collaborations sont définies comme incluant une participation directe de deux ou plusieurs acteurs à la conception, à la production et/ou à la commercialisation d'un produit (Polenske, 2012). Les relations entre ces acteurs sont la résultante d'arrangements internes qui sont verticaux, parfois au sein de la même entreprise ou dans la même chaîne d'approvisionnement. On y fait alors souvent référence de « *Teamwork* » ou de « *partnership* » (Polenske, 2012). De leur côté, les relations de coopération sont définies comme incluant deux ou plusieurs acteurs qui s'entendent au travers des ententes formelles ou informelles afin de partager de l'information sur des techniques de formation ou sur le marché et à offrir du support ou du capital d'approvisionnement (Polenske, 2012).

De plus, les concepts de coopération, de coordination et de collaboration sont fréquemment utilisés de manière interchangeable dans la communauté de la sécurité (Whelan, 2017). De nombreuses études ont conceptualisé les trois C (coopération, coordination et collaboration) afin de les définir sous un continuum (voir Mandell, 2001 ; Bryson et al., 2006 ; Keast et al., 2007 ; Mattessich et al., 2001 ; Thomson et Perry 2006 ; McNamara, 2012 ; O'Leary et Vij, 2012 ; Whelan, 2017). Ce continuum illustre la coopération d'un côté et la collaboration de l'autre et il se caractérise par la force des liens. La coopération se définit par des liens sporadiques entre acteurs (Keast et al., 2007 ; Whitford et al., 2010), tandis que la coordination désigne des liens plus durables et stables, par exemple lorsque les agences de sécurité ont un employé comme agent de liaison avec d'autres organismes (Whelan, 2012; 2017) ou lorsque des fonds sont investis conjointement pour atteindre

des objectifs (Warren et al., 1974; Mulford et Rogers, 1982; Cigler, 2001). Le nouveau Centre national de coordination en cybercriminalité (CNC3) est un exemple d'institution qui a la charge de coordonner les enquêtes policières sur les cybercrimes au Canada en établissant des liens stables entre les nombreux corps policiers (CNC3, 2023). La collaboration entre les agences de sécurité est considérée comme une interaction de haut niveau et de haute intensité (Cigler, 2001; Keast et al., 2004; Keast et al., 2007), née du désir d'atteindre des objectifs communs en travaillant en équipe (Agranoff, 2006). Cette conceptualisation postule que des liens plus forts conduiront à une plus grande collaboration pour effectuer le travail nécessaire et atteindre des objectifs communs (Whelan, 2017).

Dans le contexte de la littérature sur les organisations policières, étant des institutions publiques et gouvernementales, la collaboration et la coopération sont couramment confondues et utilisées comme des synonymes, plutôt que d'être considérées comme fonctionnant sur un continuum. Étant donné le réseau d'ententes, de relations et de partenariats multiples, la différence entre les deux termes semble avoir peu d'importance.

Toutefois, Thomson et Perry (2006) définissent la collaboration comme un processus dans lequel des acteurs autonomes interagissent à travers des négociations formelles ou informelles, en créant conjointement des règles et des structures qui gouvernent leur relation et leur manière d'agir concernant les problèmes qui les ont réunis; c'est ainsi un processus impliquant le partage de normes et d'interactions mutuellement bénéfiques. Cela dit, la définition la plus récente et disponible dans la littérature est celle de Scott et Boyd (2020). Ces auteurs définissent la collaboration[1] interagence publique comme étant la pratique où les divisions administratives gouvernementales assurent la responsabilité partagée d'atteindre un objectif commun se matérialisant en comportement de partage d'informations, d'élaboration de plans et stratégies afin de travailler ensemble au développement et à la recherche de solutions (Scott et Boyd, 2020).

La police fait généralement référence à une institution publique ayant comme mission l'application de diverses lois civiles, criminelles et pénales dans l'objectif de maintenir l'ordre dans sa société (Lemieux, 2018). Cependant, actuellement, le maintien de l'ordre est réalisé par différents acteurs qui effectuent une panoplie d'actions afin de répondre à la mission qui fut longtemps accordée à

[1] Le terme collaboration sera ainsi utilisé comme synonyme de coopération dans ce mémoire considérant l'utilisation aléatoire de ces deux termes dans la littérature portant sur l'objet d'étude.

la police traditionnelle (Jones et Newburn, 2006; Rogers, 2016). De plus, on retrouve des organisations privées, soit des entreprises, qui offrent des services payants de protection à la population ou des services d'enquête indépendante qui font concurrence aux organisations publiques (Shearing et Stenning, 1983; Johnston, 2005). Ainsi, la police du 21e siècle est amenée à être définie comme un regroupement d'acteurs visant au maintien de l'ordre étatique, et non comme une singulière institution monolithe (Lemieux, 2018). De ce postulat, Jean-Paul Brodeur (1983) a initialement théorisé la police comme étant un regroupement d'organismes étatiques et publics. Parmi ce vaste regroupement, il catégorise les différents organismes en deux classes qui représentent les concepts centraux de sa proposition théorique de la haute et basse police (« *High and Low policing* » en anglais).

Le concept de la haute police fait référence aux activités dans lesquels l'État s'engage à protéger sa population contre des attaques physique ou idéologique. La haute police intervient alors dans un environnement influencé par la politique considérant qu'elle vise davantage à maintenir l'ordre politique que l'ordre public (Lemieux, 2018). Elle a la charge de réguler les actes criminels de type divulgation de secret national, de tromperie ou même des cas de confusion des pouvoirs exécutifs, judiciaires et législatifs (Brodeur, 2010), soit des crimes catégorisés contre « l'État ». Ainsi, la haute police vise à prévenir et à se protéger de menaces potentielles dans une tentative systématique de préserver la répartition du pouvoir dans une société donnée (Brodeur, 1983). Les institutions de haute police deviennent ainsi davantage un médium des activités politiques qu'un outil pour assurer la protection de la société (Radzinowicz, 1956, p.572 dans Brodeur, 1983). À titre d'exemple de l'influence du politique sur la haute police, la *Drug Enforcement Agency* (DEA) fondée en 1973 est une instance policière fédérale qui vise précisément à combattre le trafic de drogues aux États-Unis. La DEA fut un outil du président américain Richard Nixon afin d'appliquer son programme politique du *War on Drugs*[2] (Brodeur, 1983; Epstein, 1990). Bien que le trafic de drogues fasse partie des crimes d'ordre de la basse police selon cette théorie, cette instance policière fédérale servait à répondre aux ordres et intentions du politique qui se positionnait contre les drogues. Afin de répondre à son objectif de protection de l'État, une stratégie développée par la haute police consiste à l'accumulation de renseignements (Brodeur,

[2] Le *War on Drugs* fait référence au mouvement rétributiviste américain amené par le président Richard Nixon en juin 1971. Ce mouvement s'est traduit par une incarcération de masse des individus impliqués dans la consommation, trafic et production de drogues ainsi qu'une augmentation de la durée des sentences pénitentiaires (Bandow, 1991).

1983). Dans les dernières années, plusieurs institutions policières de niveau fédéral ou national se sont spécialisées dans l'accumulation de renseignements criminels ou civils afin d'accumuler le plus d'informations pertinentes à la protection de l'État et de ces préoccupations politiques. Actuellement, ces organisations policières représentent des agences nationales de renseignements de sécurité (Lemieux, 2018). Par exemple, au Canada, on retrouve le Service Canadien de renseignement de sécurité (SCRS) qui « a pour rôle d'enquêter sur les activités qui pourraient constituer une menace pour la sécurité du Canada et d'en faire rapport au gouvernement du Canada » (SCRS, 2023). Similairement, en Australie, on retrouve le *Australian Security Intelligence Organisation* (ASIO) qui collecte, analyse et diffuse les informations pouvant menacer la sécurité publique du pays et prodigue conseils en matière de renseignement afin de répondre aux intérêts et priorités nationale (ASIO, 2023). Au niveau international, le *Five Eyes* agit de regroupement collaboratif de partage de renseignements entre l'Australie, le Canada, le Royaume-Uni, la Nouvelle-Zélande et les États-Unis (Sécurité publique Canada, 2021). À travers ce partenariat, en 2018, on totalisait près de 30 agences nationales de renseignement réparties dans ces cinq pays qui collaboraient principalement à la collecte et au signalement de renseignements pouvant représenter des menaces contre leurs différents États (Lemieux, 2018). Ces organisations sont ainsi qualifiées de hautes polices, considérant leurs objectifs de protection de l'État, sous l'influence quasi directe du politique (Lemieux, 2018).

De son côté, le concept de la basse police fait référence à un modèle policier davantage démocratique qui se préoccupe des crimes plus communs ou des désordres publics (Lemieux, 2018). En effet, selon la théorie de Brodeur (1983), la basse police fait référence à une police criminelle qui a la charge du maintien de l'ordre des États-nations en appliquant les lois pénales et criminelles tout en s'occupant des enquêtes sur les crimes commis à l'intérieur des frontières nationales (Lemieux, 2018). La basse police est particulièrement visée par les défis amenés par le phénomène de mondialisation causé par le capitalisme et l'avènement des technologies. En effet, cela a forcé les agences de basse police à adapter leurs méthodes dans un objectif de conformisation des politiques de gouvernances, ce qui a impliqué l'adoption de normes et pratiques policières qui se devaient d'être internationalement similaires (Finkelstein, 1995). Ce phénomène est souvent référé dans la littérature comme la police mondiale (« *global policing* » en anglais) ou la police transnationale (« *transnational policing* » en anglais) (ex., Andreas et Nadelmann, 2008; Bowling et Sheptycki, 2012; Stenning et Shearing, 2012). Par ailleurs, selon la thèse de Deflem (2000;

2002), la collaboration internationale ne peut se produire que lorsque les agences policières agissent indépendamment du politique. Toutefois, en plus de cette autonomie institutionnelle, il faut que les agences policières partagent le même système de connaissances sur les méthodes de répression et d'application de la loi pour les crimes internationaux (Deflem, 2000).

1.1. Les enjeux de la collaboration internationale policière

La littérature sur la collaboration internationale policière date principalement des années 1990 à 2010 et concerne surtout les crimes du trafic de drogues, le crime organisé et le terrorisme. Rappelons que ces crimes étaient de grandes préoccupations de sécurité publique dans cette période, surtout aux États-Unis après l'évènement tragique du 11 septembre 2001. Selon la typologie de Dupont (2004) reprise par Whelan et Dupont (2017) dans le cadre d'une revue systématique de la littérature, les actions de collaboration au sein des organisations policières peuvent être rapatriées en quatre principales dimensions fonctionnelles :

> 1) *l'échange d'information* : se manifeste grâce à des réseaux de policiers qui partage de l'information à l'extérieur des frontières organisationnelles. Cela peut s'exprimer par l'exploitation de systèmes de police automatisés de collecte de données ou les bases de données de renseignements criminels.
>
> 2) *la génération des savoirs* : consiste à générer de nouvelles connaissances afin de les diffuser au sein des organisations se basant sous le principe de la police fondée sur les preuves ou données probantes (« *evidence-based policy* » traduction libre de l'anglais)[3]. Par exemple, l'évaluation de menaces potentielles d'actes ou d'individus impliqués dans le terrorisme ou le trafic de drogues.
>
> 3) *la résolution des problèmes* : se matérialise en développant des réponses à des problèmes complexes qui ne peuvent être répondus par une seule agence policière. Par exemple, l'initiative de prévention pour réduire la violence des groupes organisés[4] ou les opérations conjointes.

[3] La police fondée sur les preuves fait référence au principe où les actions de la police sont orientées par des données empiriques (Sherman, 1998) (voir aussi Sherman, 1998; Sherman, 2013; Lum et Koper, 2015; Lum et Koper, 2017; Fleming et Rhodes, 2018).
[4] Les auteurs (Whelan et Dupont, 2017) font référence à titre d'exemple à l'opération policière initié à Boston aux États-Unis en 1996 qui visait à réduire la violence armée en établissant un partenariat entre plusieurs États nommée *Boston's Operation Ceasefire* (United States Attorney's Office, 2021).

4) *la coordination* : représente l'action de coordonner des réponses policières conjointes et la prise en charge de services à l'extérieur des frontières organisationnelles, ce qui se manifeste dans le domaine de la gestion d'urgences et de catastrophes.

Cette typologie fut fondée grâce à l'analyse de 117 articles scientifiques identifiés à l'aide de 18 catégories et visait particulièrement à guider les prochaines études sur le sujet (Dupont et al., 2017; Whelan et Dupont, 2017). D'ailleurs, ces auteurs utilisent la terminologie « organisations de sécurités » comme étant un vaste regroupement formant des réseaux d'organisations policières chargées d'assurer la sécurité et de collaborer entre elles (Dupont et al., 2017).

Néanmoins, cette hausse d'intérêt politique, gouvernemental et académique a aussi permis d'apporter différents constats sur les principaux enjeux qui freinent la collaboration internationale entre les différentes agences policières dans la lutte contre ces crimes.

Premièrement, bien que les stratégies internationales utilisées par les agences policières transcendent les limites impliquées par les juridictions, elles ne peuvent les éliminer (Deflem, 2002). Les agences policières sont chargées de répondre aux préoccupations politiques et doivent diriger leurs actions en fonction du politique. Bien que des stratégies internationales soient appliquées, les préoccupations politiques sont bien délimitées dans un certain territoire et guident les actions des organisations policières, ce qui exerce une influence directe sur la liberté des policiers à collaborer à l'international (Deflem, 2002) et sur la manière dont les collaborations prennent forme (Lemieux, 2018).

Deuxièmement, bien que les collaborations aient pour objectif de réduire la compétition entre les agences policières (Lemieux, 2010) et le chevauchement des enquêtes (Wang et al., 2020), la réalité étant qu'elles sont malgré tout influencées par des agendas compétitifs, des ressources limitées et des choix calculés ainsi que discrétionnaires derrière le partage d'informations (Lemieux, 2018). En effet, certains pays vivent plus de difficultés à collaborer, considérant qu'ils possèdent de nombreux corps policiers de différents niveaux ayant ainsi des responsabilités, budgets et préoccupations distincts. Par exemple, le Canada, l'Australie, le Royaume-Uni et les États-Unis sont des pays ayant différentes législations fédérales, provinciales ou étatiques et même locales, impliquant la juxtaposition de plusieurs corps policiers de différents niveaux selon la loi qui les mandatent (Lemieux, 2018). À l'opposé, certains pays ne sont pas autant impactés par cette compétitivité, car ils ne possèdent qu'un ou deux niveaux de police (ex., l'Irlande ou la France)

(Lemieux, 2018). Il est donc amené par les chercheurs que certains pays soient plus enclins à collaborer aisément à l'international considérant que leurs systèmes bureaucratiques facilitent les communications à travers une ou deux organisations policières (Lemieux, 2018), contrairement aux États-Unis par exemple, qui possédaient plus de 18 000 agences policières étatiques et locales en 2016 (Banks et al., 2016).

En outre, deux défis sont aussi recensés dans la littérature à propos de la collaboration locale et nationale, donc à l'intérieur même d'un pays. Le premier défi consiste à la compétition inter-agences. Certaines agences policières sont réfractaires à coopérer entre elles à cause de la forte compétition causée par la distribution des richesses de l'État dans les différentes organisations policières déterminées selon le taux de résolution d'enquêtes, de la productivité générale ou autres (Lemieux, 2018). Ainsi, plus un pays est composé de différents corps policiers devant se battre pour obtenir des ressources financières, moins la collaboration inter-agences sera favorable. Le deuxième défi consiste au manque de communication à l'intérieur même des frontières d'un pays, impliquant qu'il est possible que plusieurs agences policières de différents niveaux enquêtent sur un même crime simultanément (Wang et al., 2020). Par exemple, des agences fédérales policières comme le Federal Bureau of Investigation (FBI), la Drug Enforcement Agency (DEA) et des enquêteurs d'agences locales se rendent fréquemment compte qu'ils enquêtent sur les mêmes trafiquants de drogues, et ce, grâce à des collaborations informelles entre ces agences (Chaiken et al., 1990). Malgré tout, au courant du 21^{e} siècle, de nombreux réseaux d'officiers de liaison internationale (« *international liaison officers* (ILOs) » en anglais) ont été développés afin d'assister les agences de polices nationales et pour exécuter des traités internationaux (Lemieux, 2015). Spécifiquement aux États-Unis, le FBI et la DEA ont récemment développé des réseaux internationaux de centaines d'ILOs (Lemieux, 2018) afin de faciliter différentes tâches reliées à l'échange d'informations, à l'enquête, aux arrestations, à la création de formations sur les crimes internationaux et plus encore (Nadelmann, 1993; Bigo, 2000; Den Boer et Block, 2013).

De plus, la culture au sein des organisations policières est considérée comme un facteur important à la collaboration ou son absence (Cohen, 2018). Certains chercheurs postulent même que c'est le facteur principal, car la culture est ce qui construit les attitudes et détermine les actions des membres d'une organisation face à la collaboration (ex., Kim et Lee, 2006; Zhang et Dawes, 2006; Weare, Lichterman et Esparza, 2014). Bien qu'il ne semble pas avoir de consensus sur la définition

de la culture organisationnelle (Cohen, 2018), il est possible de la décrire comme un système partagé de présupposés, de connaissances, d'attitudes, de valeurs et de normes qui expliquent la façon dont les membres de l'organisation agissent et réfléchissent collectivement (Pettigrew, 1979; Schein, 1992). En effet, de nombreuses études ont conclu que la culture d'une agence policière influence profondément les actions et décisions de celles-ci (ex. O'Reilly et al., 1991; O'Reilly et al., 2014; Denhardt et Catlaw, 2014). Ainsi, le système de croyances instauré au sein du groupe va influencer le choix de collaborer (Mitchell et al., 2015).

Selon Lemieux (2010), la collaboration policière a pour objectif de remédier à la concurrence entre les agences et au chevauchement des enquêtes dans la lutte contre les crimes internationaux. Afin de mieux comprendre les fonctions des différentes agences de collaboration internationale et nationale, Lemieux (2018) a repris les concepts de la haute et basse police de Brodeur (1983) afin de séparer la collaboration internationale au sein des institutions policières en deux types soit la haute et basse collaboration policière (« *High and Low policing cooperation* » en anglais). De plus, la conceptualisation des types de coopération de Lemieux (2018) permet d'identifier les barrières à la collaboration internationale particulièrement au sein de la basse police.

Pour la haute police, la collaboration internationale se matérialise par une dynamique de coopération entre des agences nationales de renseignement de sécurité et de menace contre l'État, comme bien illustré par l'entente des *Five Eyes* (Lemieux, 2018). La collaboration internationale est donc facilitée par la structure hiérarchique élevée et de niveau national dans les agences policières de haut niveau considérant leurs fonctions de protection et d'application de la loi répartie dans l'ensemble d'une nation. De plus, ces agences policières ont été fondées dans un objectif de partages d'informations considérant leurs responsabilités législativement supérieures et de niveau international comparativement aux agences de basse police qui ont été fondés afin de maintenir l'ordre public et d'appliquer les lois dans un certain territoire juridique (Lemieux, 2018).

De son côté, la collaboration internationale dans la basse police est limitée par la structure fondamentale de ces institutions qui est définie par des pouvoirs législatifs et exécutifs distribués par des juridictions géographiquement déterminées (Lemieux, 2014; 2018). En effet, cela est principalement causé par la difficulté d'arrimer les nombreuses lois et les divers systèmes légaux au sein des multiples organisations policières distribuées dans le monde. D'ailleurs, par le passé, les organisations ont essayé, sans succès, d'appliquer leurs lois domestiques ou régionales à un

niveau international (Lemieux, 2018). De plus, dans un contexte de collaboration internationale, les pays développés rapportent davantage de limitations à collaborer avec des pays non développés à cause des différences importantes reliées aux respects et standards des droits humains ainsi qu'à l'application des lois et procédures judiciaires parfois contradictoires (Lemieux, 2018). Néanmoins, pour contrer les problématiques de collaboration, des institutions internationales de coordination de la loi, par exemple Europol (intra-Europe), Interpol (entre différents pays) ou le Federal Bureau of Investigation (FBI)[5] (entre les États aux États-Unis)) ont été instaurées et visent à lutter contre la criminalité transnationale et internationale (Lemieux, 2018). Ces organisations peuvent faciliter les communications entre les collègues policiers de différents pays et institutions, rédiger des mandats d'arrêt (pour Interpol à l'internationale et pour le FBI aux États-Unis uniquement), procéder à l'incrimination de certaines infractions, travailler sur la négociation d'accords de coopération, et plus encore (Fooner, 1989; Bressler, 1992). Ces institutions représentent du *Low Policing Cooperation*, considérant qu'ils se préoccupent des crimes communs et des dérangements publics, comme le trafic de drogues (Lemieux, 2018) ou la lutte contre le terrorisme.

Cependant, malgré les initiatives de collaboration par les institutions de coordination et des ILOs, les deux niveaux de coopération (*High* et *Low*) sont devenus dépendants des institutions privées. En effet, les organisations policières utilisent des outils technologiques qui sont créés et inventés par des institutions privées[6] afin de réaliser leurs enquêtes sur les crimes internationaux. Malgré l'implication et la dépendance des institutions privées dans la réussite de certaines interventions et enquêtes policières portant sur les crimes internationaux, il reste qu'elles ne sont pas considérées comme des organisations de police et ne possèdent pas les droits ni les pouvoirs d'effectuer le travail des organisations officielles policières. Ainsi, celles-ci ne sont pas considérées comme étant des actrices formelles de la collaboration policière (Lemieux, 2018).

[5] On fait davantage référence au *Joint Terrorism Task Force* qui est une équipe spécialisée à l'intérieur du FBI.
[6] Par exemple : « BAE Systems, CSRA, General Dynamics et Northrop Grumman » (Lemieux, 2018, p.16).

1.1.1. Le partage d'information

Lorsqu'il est question de collaboration entre les agences policières, le sujet du partage d'information est omniprésent. L'information peut consister à du renseignement criminel ou des déclarations et elle est essentielle au déroulement efficace de la réponse policière. Le partage d'informations entre les forces de l'ordre a été principalement étudié au niveau national (voir Boba et al., 2009 ; Taylor et Russell, 2012 ; Brewer, 2013 ; Lambert, 2019 ; Pickering et Fox, 2022), mais on en sait peu à ce jour sur la collaboration internationale. Même si plusieurs études ont conclu que le partage d'information est essentiel pour enquêter ou intervenir sur les crimes inter juridictionnels, divers facteurs compliquent les échanges (Pickering et Fox, 2022).

Tout d'abord, il est démontré dans la littérature que les services de police ont fait preuve de résistance à changer leurs méthodes traditionnelles dans le passé (Braga et Weisburd, 2007 ; Schaefer-Morabito, 2010). Comme mentionné précédemment, les structures policières n'ont pas été initialement conçues pour les crimes inter juridictionnels. Cela amène certaines agences à être moins enclines à partager leurs données en raison de la nature de leurs départements, se concentrant uniquement et singulièrement sur un type de crime (Ratcliffe, 2007). De plus, le refus du partage intra pays peut être causé par la concurrence entre les agences pour obtenir du financement. Ce phénomène est particulièrement marqué aux États-Unis, où des milliers d'agences policières se font compétition pour obtenir du financement (Lemieux, 2010; Lemieux, 2018). En plus de la problématique du financement, l'étude de Sheptycki (2004) recense 11 pathologies organisationnelles au sein des agences policières qui freinent le partage de renseignements criminels. À la lumière des résultats présentés, il est possible de comprendre que le choix de partager des informations n'est pas seulement dépendant des individus, mais bien de la culture organisationnelle de l'agence policière (Sheptycki, 2004).

La thésaurisation de l'information (« *information hoarding* » en anglais) (Pickering et Fox, 2022) représente l'action de conserver des informations au sein de son agence policière et constitue aussi un grand obstacle à la collaboration. En effet, comme le mentionnent Sanders et Henderson (2013), certains départements de police semblent être intéressés uniquement à recevoir de l'information sans en fournir réciproquement. Les chercheurs expliquent ce comportement en exposant l'attitude de certains policiers qui pensent que les autres agences ne sont pas équipées, voire incompétentes, pour traiter les informations qu'ils ont collectées (Taylor et Russell, 2012; Cohen, 2017; Lambert,

2019) et que la dispersion des informations les rendra moins incontournables aux yeux du public voire pourrait nuire à leur réputation (Boba et al., 2009). Toutefois, étant donné sa nature, la collaboration nécessite que divers départements s'engagent et partagent réciproquement.

Finalement, même si les agences policières désirent collaborer, ils font souvent face à des difficultés techniques qui sont principalement causées par la constante évolution des outils de collecte de données et le fait qu'il n'existe pas de moyen unique de les collecter. Ainsi, pour transférer des renseignements à un autre service, il est souvent nécessaire de ressaisir les données, de les recoder et de trouver un endroit sécuritaire pour les stocker (Sheptycki, 2004).

1.2. Les deux types de collaboration internationale

Afin de contrer ces enjeux qui nuisent à la fluidité des collaborations internationales, on observe deux types de ressources visant à supporter les agences policières dans la lutte contre les crimes internationaux. Tout d'abord, ces ressources sont décrites comme étant des catégories de collaboration, étant soit qualifiées de formelles ou d'informelles. De son côté, la collaboration internationale formelle fait principalement référence à des organisations de coopération internationale ayant comme mandat légal ou gouvernemental d'aider à la collaboration en facilitant le partage d'informations entre les agences policières et pays membres (ex., Europol et Interpol) (Gerspacher et Dupont, 2007). De l'autre côté, la collaboration internationale informelle fait référence à des échanges d'informations se faisant grâce à une relation spontanée entre deux agents policiers de différents pays qui ont établi une relation de confiance à distance (Lavers et Chu, 1997; Bayer, 2010; Deflem, 2016).

1.2.1. *Les institutions formelles de collaboration internationale*

La hausse des crimes internationaux au début des années 1900 a amené plusieurs chercheurs à démontrer la nécessité de créer un système de gouvernance qui transcende les limites géographiques et législatives afin de pouvoir équilibrer leurs pouvoirs d'agir à ceux des criminels, qui bénéficient de la mondialisation et des nouvelles technologies pour répandre leurs réseaux et commettre des actes criminels partout dans le monde (Gerspacher et Dupont, 2007). Pour répondre à ce besoin croissant, deux organisations policières ayant pour tâche première de faciliter la collaboration internationale ont été fondées : Europol et Interpol.

Interpol fut créé par des agences nationales de police qui étaient confrontées par des problèmes nécessitant la coopération (Gaspacher et Dupont, 2007). Précisément, Interpol fut créé le 7 septembre 1923 à Vienne en Autriche (Deflem, 2002) alors que les crimes internationaux n'étaient pas encore une préoccupation internationale. C'est l'arrivée du Federal Bureau of Investigations (FBI) en 1938 et les évènements des deux Guerre mondiale qui ont amené les organisations policières à faire des pressions gouvernementales et à demander du support face à cette nouvelle problématique (Deflem, 2016). Ainsi Interpol s'est développé durant le 20^{e} siècle en tant qu'organisation intergouvernementale ayant le but de promouvoir la coopération policière internationale principalement en facilitant les communications entre les agences policières membres afin d'éviter les demandes formelles et les limites légales inter-agences (Deflem, 2016; Gerspacher et Dupont, 2007). Contrairement à la croyance populaire, Interpol ne possède pas de pouvoir d'arrestation ni d'investigation, cette organisation sert de services de communication entre les agences policières membres (Deflem, 2016) et de service de formation (Interpol, 2022). À ce jour, Interpol rallie 195 pays membres qui ont accès aux bases de données criminelles, à un système de communication sécurisé, à des groupes de travail composés d'experts et d'agents policiers ainsi qu'à des conférences pour acquérir des connaissances (Interpol, 2022).

De son côté, Europol est l'agence européenne de police criminelle. Elle fut créée en 1992 par le Traité de l'Union européenne (Deflem, 2006) à la suite d'engagements politiques en Europe visant à encourager la collaboration dans la lutte contre la criminalité transnationale (Gerspacher et Dupont, 2007). Europol a comme principal rôle d'aider les agences policières à l'intérieur de l'Europe à lutter contre la criminalité internationale, principalement le crime organisé et le terrorisme, en plus de soutenir des opérations de maintien de l'ordre sur le terrain, d'offrir une plateforme d'informations sur les activités criminelles ainsi que de fournir de l'expertise policière à l'aide de ses nombreux analystes (Union européenne, 2022).

Malgré leurs différences, ces deux organisations ont pour but commun de lutter contre la criminalité internationale et possèdent des similarités dans leurs structures, missions et raisons d'être (Gerspacher et Dupont, 2007). En effet, ces deux agences formelles sont principalement responsables de faciliter les communications entre leurs agences policières ou pays membres ainsi qu'à servir de services-conseils pour la lutte aux crimes internationaux.

1.2.2. *Les regroupements collaboratifs informels*

Malgré les intentions et objectifs des institutions formelles de collaboration, celles-ci ont reçu des critiques importantes concernant leurs méthodes et leurs impacts. En effet, la critique la plus importante expose la lenteur de ces organisations à faire l'échange d'informations entre différentes agences policières (Lavers et Chu, 1997; Bayer, 2010; Deflem, 2016). De plus, les institutions de communication formelles sollicitent de lourdes implications bureaucratiques et politiques nécessitant des demandes formelles d'échanges d'informations qui sont souvent limitées en raison des juridictions empêchant les officiers de police d'agir à l'extérieur de leurs régions légalement attitrées (Lavers et Chu, 1997; Den Boer, 2013). Cela amène certains officiers de police à collaborer de manière informelle avec d'autres officiers dans un autre pays afin d'échanger des informations. Le partage d'informations informelles peut être crucial dans l'avancement des interventions policières et avoir un impact important sur l'identification de suspects (Raustiala, 2002; Slaughter, 2004). Selon Den Boer (2013), les collaborations informelles se font davantage entre des organisations de mêmes niveaux et ayant des pouvoirs législatifs similaires, ce qui se nomme la collaboration horizontale. La collaboration formelle étant davantage décrite comme un service de collaboration policière verticale, impliquant que les organisations policières régionales font appel à ces institutions jugées hiérarchiquement supérieures (Den Boer, 2013). Particulièrement, les avantages de la collaboration informelle sont principalement sa flexibilité, mais aussi son implantation rapide (Lavers et Chu, 1997). L'adoption de collaboration informelle se fait donc sans permission d'une autorité et transperce les barrières bureaucratiques spécifiques à chaque agence de police (Lavers et Chu, 1997).

En plus de sa pertinence pratique pour le succès des tâches policières, certains auteurs ont reconnu que l'accumulation de relations internationales, soit de contacts, fait partie de la culture policière (Ross, 2010; Deflem dans Bayer, 2010). En effet, la culture policière valorise l'accumulation de relations de confiance avec leurs homologues policiers dans d'autres pays (Ross, 2010). Cela se matérialise en échange informel d'information pertinente dans l'avancement de leurs interventions policières ou des enquêtes (Ross, 2010). De plus, selon Bayer (2010), les agents policiers apprécient avoir leur autonomie professionnelle et leur pouvoir d'agir indépendamment de leurs centres décisionnels. Les relations de collaboration informelle se cultivent donc en réalisant du réseautage entre les policiers (Lavers et Chu, 1997; Ross, 2010; Deflem, 2016).

Cependant, la collaboration informelle n'est pas sans limites ni difficulté. En effet, la collaboration informelle n'a pas de statuts juridique, ce qui peut avoir des impacts sur sa légitimité et son implication pratique dans les interventions et enquêtes policières dans certains cas (Lavers et Chu, 1997). Finalement, de nombreux facteurs peuvent influencer les policiers à avoir recours à un type de collaboration au détriment de l'autre, néanmoins la décision d'avoir recours à des organisations formelles ou regroupements informels est généralement prise en fonction de certaines spécificités, dont la langue et la géographie (Tremblay, 2009).

Bien que ces types soient distincts dans la littérature, il est aussi possible qu'elles soient réalisées conjointement à l'aide des ILO. En effet, ces agents de liaison sont des officiers relocalisés afin d'avoir une présence physique dans un autre pays dans l'objectif de faciliter les enquêtes conjointes (Whelan, 2012). Ainsi, bien que ces officiers répondent à des demandes formelles, leur présence au sein de l'autre agence policière favorise la réalisation de collaboration informelle. Au Canada, les ILO répondent aux demandes placées dans le cadre de la Loi sur l'entraide juridique en matière criminelle (voir Gouvernement du Canada, 2023) prend fait parties des ententes internationales d'assistances légales mieux connues sous l'acronyme MLAT (*Mutual Legal Assistance Treaty*).

En résumé, la littérature classique sur la collaboration internationale entre les agences policières porte principalement sur les crimes internationaux qui étaient des préoccupations mondiales importantes après l'événement du 11 septembre 2001 aux États-Unis. Ceci a mené à une juxtaposition d'efforts afin de faciliter les communications portant principalement sur le renseignement criminel afin d'assister les interventions et enquêtes policières portant sur ces crimes, soit principalement le trafic de drogues, le crime organisé et le terrorisme.

2. Les cybercrimes

De 2015 à 2020, l'Internet Crime Complaint Center (IC3) a répertorié plus de 2 millions de plaintes provenant de victimes de cybercrime (IC3, 2020), et ce, seulement aux États-Unis. Au début de l'avènement des cybercrimes, ils étaient définis comme un regroupement complexe de crimes, de délits traditionnels ou innovants, commis par le médium du World Wide Web (WWW) communément appelé l'Internet (Lavoie, Fortin et Tanguay, 2013). Dernièrement, les études sur le sujet sont nuancées en ce qui concerne la définition de ce type de crimes considérant le débat sur la surutilisation du préfix *cyber.* Plusieurs chercheurs critiquent l'utilisation abusive de ce préfixe malgré l'implication presque omniprésente des technologies dans les comportements

humains (Lupton 2015; Marres 2017; Futter 2018; Horst et Miller, 2020; Branch 2021; Gordon et al., 2022). Un argument défendu est que l'utilisation du terme « cybercrime » amènerait une limitation des objets d'études en délaissant tout acte ayant un lien indirect, mais présent, avec les technologies (Verbeek, 2005; Gordon et al., 2022). Et ce, en plus de créer du *digital dualism,* étant une séparation drastique des sphères digitales et physiques (Jurgenson, 2012), alors que celles-ci sont en perpétuelles interactions.

Par ailleurs, l'utilisation du préfixe cyber s'ajoute communément à la notion d'espace dans la littérature en proposant la présence d'un « cyberespace » dans lequel les cybercrimes sont commis. Michael McGuire (2007) dans son ouvrage *Hypercrime : The New Geometry of Harm* postule que cette utilisation du terme cyberespace sous-entend une division entre l'espace traditionnel et virtuel. Cette division amène à la conceptualisation du cyberespace comme un endroit fictif et divergeant de monde manifeste et des interactions sociales dites classiques, soit physiques et concrètes. Toutefois, McGuire (2007) postule que l'utilisation du terme cyberespace ne s'avère pas utile ni véridique, il propose ainsi d'utiliser le concept Hyper en remplacement de Cyber. Le hyper faisant référence au nouvel environnement moderne dans lequel le monde traditionnel, soit physique et manifeste, et le monde fictif englobant la technologie, l'Internet et toutes ses composantes soient un tout. Ainsi, l'Hypercrime et l'Hyperspace sont décrits comme étant des produits qui dérivent de l'espace traditionnel.

Malgré les discours en faveur de l'abolition du préfixe *cyber* ou de l'adoption du préfixe *hyper*, il est notable que la littérature utilise encore à ce jour le concept du cybercrime. La vaste majorité, si ce n'est pas l'ensemble, des articles recensés dans ce mémoire l'ont utilisée à une ou plusieurs reprises. De ce fait, dans le cadre de ce mémoire, nous utiliserons les termes cybercrimes, cyberespace et cybercriminalité, toutefois, nous adoptons une approche globale qui tient compte des limites et soulignons les critiques de la conceptualisation fictive de ce préfixe.

Ainsi, malgré l'absence de définition unique de ce qu'est un cybercrime (Toure et Mef, 2011; Phillips et al., 2022), ce terme est généralement utilisé afin de décrire une grande variété d'actes illégaux ou illicites commis par un individu ou un groupe contre un ou plusieurs ordinateurs, réseaux informatiques ou technologies (Donalds et Osei-Bryson, 2019). Il peut aussi être utilisé pour faire référence à des crimes traditionnels ou des actions illicites qui ciblent autrui à l'aide de

l'utilisation d'Internet ou de technologie(s) (Donalds et Osei-Bryson, 2019). En bref, la terminologie « cybercrime » est encore utilisée dans la littérature afin de différencier l'ensemble des actes répréhensibles par un Code criminel des actes répréhensibles impliquant l'utilisation d'une technologie ou prenant entièrement place sur le cyberespace. On fait alors référence aux cybercrimes dans lequel la technologie est la cible, par exemple les attaques de déni de service ou les logiciels malveillants, en plus des infractions où la technologie est l'instrument, par exemple la fraude, le vol d'identité, l'exploitation sexuelle d'enfants, le trafic de drogues et plus encore (Gendarmerie Royale du Canada, 2015; NW3C[7] dans Macdonald, 2020). De plus, une caractéristique importante des actes qualifiés de cybercrimes est qu'ils sont considérés comme des crimes internationaux grâce à leur capacité de transcender les limites géographiques, car ceux-ci peuvent être commis de n'importe où dans le monde et viser n'importe quelles victimes ou technologies (Donalds et Osei-Bryson, 2019).

Les cybercrimes peuvent être mis en œuvre à l'aide des trois parties du World Wide Web (WWW) : le clearweb (ou Surface Web), le deepweb ou le darkweb. Ils ne prennent donc pas place physiquement dans l'espace, mais uniquement virtuellement sur le cyberespace (Cross, 2020). Le clearweb représente tout ce qui est visible, accessible et indexé à l'aide des moteurs de recherche (Kaur et Randhawa, 2020) par exemple Google ou Bing. Malgré son accessibilité, le clearweb ne représente qu'une infime partie de l'Internet comparativement aux deux autres parties cachées qui représentent 96% de l'ensemble du contenu (Mirea et al., 2019). En effet, le deepweb n'est pas accessible à l'ensemble de la population, car il est protégé par des demandes d'accès comme des droits d'utilisation payants ou des mots de passe (ex., les courriels, les services financiers en ligne, les banques de données, les services de divertissements comme Netflix et plus encore) (Mirea et al., 2019). Le darkweb quant à lui réfère aux réseaux qui rendent plus difficile l'identification des utilisateurs en obfusquant leurs adresses IP (« *Internet Protocol* » en anglais). L'adresse IP fait référence à un numéro qui permet l'identification d'un appareil connecté à un réseau local ou Internet (Kaspersky, 2023). Bien que le réseau le plus utilisé soit Tor (Kaur et Randhawa, 2020), il existe d'autres réseaux comme FreeNet, l'Invisible Internet Project (12P) et Whonix (Mirea, et

[7] Le National White Collar Crime Center (NW3C), fondé en 1978, est une organisation mondiale qui offre du support aux enquêtes policières sur les crimes économiques et technologiques aux professionnels (https://www.nw3c.org/).

al., 2019). Nous nous concentrerons cela dit sur le réseau Tor qui compte pour plus de 95% des utilisateurs du darkweb.

2.1. Crimes commis à l'aide du darkweb

Le réseau Tor fut développé par la marine américaine qui désirait communiquer des renseignements secrets à ses agents postés partout dans le monde, sans que ces derniers soient détectés (Mirea et al., 2019). Il a été construit et fonctionne aujourd'hui grâce à l'utilisation de divers protocoles de communication ainsi que le chiffrement et les algorithmes aléatoires de routage (Çaliskan et al., 2015). Le réseau Tor est bâti sur une infrastructure pair à pair (P2P ou *peer-to-peer* en anglais) décentralisée où trois relais (ou *proxy* en anglais) séparent un utilisateur de l'internet pour protéger son identité (Kaur et Randwara, 2020). Ceci rend plus difficile l'identification des acteurs qui l'utilise. Par sa fonction anonymisante, le darkweb est un canal de communication utilisé afin de commettre des activités illégales ou illicites (Naseem et al., 2016; Mirea et al., 2019; Kaur et Randhawa, 2020). Il est aussi possible d'y trouver des pages *.onions* qui peuvent prendre différentes formes comme des marchés virtuels ou de forums de discussions (Moore et Rid, 2016). À titre d'illustration, les chercheurs Moore et Rid (2016) ont observé que sur un total de 5 615 pages (*.onion)* sur Tor, 57% d'entre elles facilitaient des activités illégales, comme la vente de drogues, des produits financiers illégaux ou de la pornographie impliquant soit de la violence, des enfants ou des animaux. Les principaux crimes observés et recensés dans la littérature sont des actes reliés à la pornographie juvénile, à la fraude, au piratage informatique, à l'arnaque de cryptomonnaie (Mirea et al., 2019; Kaur et Randhawa, 2020) ainsi qu'au trafic de drogues (Van Hout et Bingham, 2013; Aldridge et Décary-Hétu, 2014; Tzanetakis et al., 2015; Soska et Christin, 2015; Barratt et Aldridge, 2016; Rhumorbarbe et al., 2016; Broséus et al., 2017; Tzanetakis, 2018), de cigarettes (Munksgaard et al., 2021) et d'armes à feu sur les cryptomarchés[8] (Holt et Lee, 2022). Les crimes aussi commis à l'aide du darkweb, mais avec moins de preuves empiriques, consistent en trafic humain, la vengeance pornographique (« *revenge porn* » en anglais) et le recours à des services payants de tueurs à gages (Kaur et Randhawa, 2020). En ce qui concerne le langage le plus courant sur le darkweb, Faizan et Khan (2019) ont observé que,

[8] Cryptomarchés: les marchés de reventes de drogues sur le darkweb portent le nom de cryptomarchés et ils opèrent similairement aux plateformes de commerces en ligne comme eBay (Aldridge et Décary-Hétu, 2014) ou même Amazon. Les cryptomarchés sont ainsi des services anonymisant sur Internet invitant les trafiquants de drogue indépendants et les consommateurs à commercer sur leurs plateformes qui sont régulées par des administrateurs.

dans un total de 6 227 services cachés et disponibles sur Tor, le langage le plus utilisé après l'anglais consistait en ordre décroissant : le russe, l'allemand, le français et l'espagnol.

2.2. Les difficultés d'enquêtes causées par l'avènement des technologies

Selon Dodge et Burrus (2020), il est possible d'identifier quatre principaux aspects qui posent des problèmes considérables à la réponse policière en matière d'enquête de crimes impliquant l'utilisation de technologies : 1) l'anonymat, 2) les juridictions, 3) l'asynchronicité et 4) les preuves numériques.

Premièrement, les cybercriminels cachent leurs crimes grâce à des interactions anonymes, et ce, souvent par le biais de connexions réseau falsifiées ou anonymisées (« Virtual Private Networks » (VPN) en anglais) (Dodge et Burruss, 2020) ou par l'utilisation de technologies anonymisantes comme le darkweb (Naseem et al., 2016; Mirea et al., 2019; Kaur et Randhawa, 2020). Cela a un impact sur la capacité d'identification du ou des suspects par les policiers impliquant l'impossibilité de mener l'enquête, l'arrestation, ni la poursuite des cybercriminels (Dodge et Burruss, 2020). Par exemple, les acheteurs et les vendeurs sur les cryptomarchés communiquent grâce à des messages cryptés et transportent les commandes par colis postaux. De plus, les transactions sont payées à l'aide des cryptomonnaies[9] afin de protéger leur identité (Van Hout et Bingham, 2013 ; Van Slobbe, 2016). Deuxièmement, même lorsqu'un suspect est identifié, la capacité d'intervention pour les policiers est limitée par les juridictions établies dans chaque pays, et ce, malgré le fait que les cybercrimes sont internationaux (Dodge et Burruss, 2020). En effet, les crimes informatiques peuvent se faire à tout moment, n'importe où dans le monde et viser n'importe quel pays. Cependant, les Codes criminels interdisant certains actes, eux, sont définis et appliqués en fonction de chaque nation (Wall, 2007a). Dans ce type de criminalité, la victime et le criminel font fréquemment partie de deux à plusieurs régions juridiques différentes, tous dépendamment de l'acte commis. Cela ajoute une complexité supplémentaire importante à l'identification et à l'arrestation des criminels comparativement à un crime commis sous un même territoire géographiquement rapproché. D'autre part, le même acte peut être déclaré illégal dans un pays, mais faire l'objet d'un vide juridique ou être déclaré comme légal dans un autre (Brenner

[9] La cryptomonnaie consiste à une monnaie numérique, uniquement disponible sur Internet, produit par un processus de pair-à-pair ou de blockchain, sans régulation d'une banque centrale ou d'un gouvernement.

et Schwerha, 2004), ce qui entrave le succès des opérations de police. Par ailleurs, il a même été démontré empiriquement que plus la dispersion géographique des crimes est grande, plus la probabilité pour les criminels de se faire prendre est faible (Lammers et Bernasco, 2013). Troisièmement, la nature asynchrone des cybercrimes implique que l'infraction peut avoir été commise des mois avant qu'une victime ne s'aperçoive de la cyberattaque, ce qui amène des difficultés supplémentaires qui sont considérables à l'enquête (Dodge et Burruss, 2020). Par exemple, dans le cas d'un vol d'identité sur Internet, le temps entre le vol de données et le moment où la victime réalise le préjudice peut être très variable, allant de minutes à des années. Quatrièmement, il est peu probable pour les agents policiers de première ligne de posséder l'expertise nécessaire à la collecte, le stockage, ni le traitement de la chaîne de possession des preuves numériques (Dodge et Burruss, 2020), considérant la complexité et la constante évolution des technologies.

De plus, les défis des départements de criminalistique numérique (« *digital forensics* » en anglais) (DF) sont exposés dans la littérature (voir Horsman, 2017 ; Casey, 2019 ; Wilson-Kovacs, 2021). Les preuves numériques nécessaires pour chaque cas comportant une composante technologique, y compris les crimes liés au darkweb, doivent être extraites, traitées et analysées par les unités DF pour être utilisées comme renseignements pour les enquêtes ou les procédures pénales (Casey, 2011). À titre d'exemple, dans 90% des cas judiciaires au Royaume-Uni, au moins une preuve digitale est présentée (NPCC, 2020). Cela démontre de l'importance de la criminalistique numérique de nos jours. Même si davantage d'outils sont à la disposition des équipes DF, l'identification des suspects devient de plus en plus complexe (Horsman, 2017).

Au début des données 2010, il y avait un consensus généralisé au sein de la communauté que la police n'était simplement apte à intervenir légalement sur le darkweb à cause de ses caractéristiques aléatoires, anonymes et à cause de l'encryption des données (Armerding, 2015 dans Davis, 2020). Toutefois, il est à noter que les forces policières ont développé des stratégies puissantes pour identifier les criminels dans les dernières années (Davies, 2020). Par souci de confidentialité, ces stratégies ne sont pas publiques à l'exception des stratégies de collecte de données en sources ouvertes ou l'infiltration des réseaux criminels en ligne (voir Davies, 2020).

2.3. Les interventions policières sur le darkweb

Malgré les limitations géographiques et les difficultés qu'amènent les cybercrimes aux enquêtes policières, plusieurs interventions ont été réalisées sur le darkweb afin d'identifier des suspects, de désorganiser des activités criminelles ou de démanteler des réseaux organisés en ligne dans l'objectif de réduire la criminalité et/ou d'aider aux enquêtes afin d'amener en justice les délinquants. Dans la littérature, on retrouve deux grandes catégories d'interventions policières. Celles-ci sont soient qualifiés de réactives ou de proactives (Zimmer, 1990; Mazerolle et al., 2007). Les interventions réactives surviennent à la suite d'un évènement criminel, généralement causé par l'interception d'un suspect par un policier sur la scène du crime ou à la suite d'une plainte d'une victime. On y retrouve des interventions qui visent à résoudre un problème ciblé dans le temps et l'espace, par exemple des *raids* (opérations de recherche localisée), du *policing* intensif (augmentation de la présence policière dans un milieu donné) ou du « *search and seizure* » (la quête et saisie de produits illégaux comme la drogue) (Mazerolle et al., 2007). Les interventions proactives consistent davantage à des stratégies organisationnelles développées et mises sur pied dans l'objectif de contrer un phénomène criminel plus complexe ou impliquant de nombreux acteurs, par exemple le trafic de drogues (Mazerolle et al., 2007). Ce sont particulièrement ces interventions qui sont mobilisées par la création de partenariats entre différentes agences de police, car elles nécessitent l'amassement de preuves, d'informations et de ressources de différents endroits géographiquement distingués (Mazerolle et al., 2007).

Dans le cas des crimes impliquant l'utilisation des technologies et un nombre restreint de victimes, par exemple le vol d'identité ou la cyberintimidation, les interventions policières sont davantage réalisées en réaction à l'évènement, donc à la suite d'une plainte de la victime (Moore, 2015). Contrairement aux crimes plus complexes qui sont davantage la priorité des agences policières, comme les crimes relatifs à la pornographie juvénile sur Internet, on observe plus d'interventions policières proactives qui sont réalisées par un amalgame de techniques, d'enquêtes et d'investissement dans des outils afin d'intercepter les suspects concernés (Moore, 2015). En ce qui concerne les crimes commis sur le darkweb, la littérature aborde principalement les nombreuses interventions menées proactivement afin de déstabiliser des cryptomarchés (Van Slobbe, 2016; Aldridge et Askew, 2017). Ces interventions sont des opérations de perturbation et elles visent principalement à rendre non accessible la plateforme (ex., la fermeture de *Silk Road*

1.0[10]). Cependant, on observe aussi des interventions réactives, comme des opérations d'infiltration, des saisies de colis postaux ou des arrestations de masse, comme il fut le cas avec l'opération *Onymous* (Décary-Hétu et Giommoni, 2017). L'Opération *Onymous* est une perturbation policière orchestrée par 16 pays européens et les États-Unis afin d'arrêter 17 personnes, dont l'administrateur de *Silk Road* 2.0 en plus de saisir plus de 1,3 million d'USD $ en Bitcoins, argents comptants, métaux précieux et drogues (Décary-Hétu et Giommoni, 2017).

Néanmoins, les interventions policières de grande envergure sont orchestrées par des institutions formelles de collaboration. Par exemple, en mai 2023, un communiqué de presse de Europol informe la réussite de l'opération SpecTor contre le trafic de drogues sur le darkweb (Europol, 2023, 2 mai). Cette opération, coordonné par Europol, a permis d'arrêter 288 vendeurs, de saisir des cryptomonnaies représentant 50 millions d'Euros, de saisir 850 kg de drogues et un total de 117 armes à feu. Grâce à la saisie du cryptomarché *Monopoly Market* par les autorités en Allemagne, Europol a cumulé, analysé et comparé les données avec les informations partagées par leurs partenaires lors d'une rencontre du *Joint Cybercrime Action Taskforce* (J-CAT). Au total de 9 pays ont été impliqués dans l'accumulation de renseignements, l'enquête sur les suspects et l'arrestation physique de ces individus dans leurs pays respectifs (Autriche, France, Allemagne, Pays-Bas, Pologne, Brésil, Royaume-Uni, États-Unis et la Suisse) (Europol, 2023, 2 mai).

De plus, dans l'étude de Jardine (2021), on observe quatre principales stratégies adoptées par les agences policières afin d'intervenir en fonction des différentes étapes de la création et de l'expansion d'un cryptomarché sur le darkweb : 1) l'accumulation d'informations sur les individus concernés, 2) la formation de compte afin d'infiltrer la plateforme, 3) l'échange de marché afin d'identifier les serveurs et 4) l'interception de livraison/réception de colis. Ces stratégies ont toutes pour objectif de dissuader les utilisateurs, que ce soient les vendeurs, les acheteurs ou les administrateurs de ces plateformes. En effet, les interventions policières sur le darkweb visent principalement à dissuader les utilisateurs de poursuivre leurs activités criminelles (Martin, 2014; Gupta et al., 2018).

[10] La fermeture de *Silk Road* 1.0 fut réalisée le 2 octobre 2013 par une agence policière des États-Unis (Décary-Hétu et Giommoni, 2017).

2.3.1. *Les résultats des interventions policières*

Malgré la hausse du nombre d'interventions policières sur le darkweb dans les dernières années, les utilisateurs du darkweb ont démontré être très résilients et résistants (Décary-Hétu et Giommoni, 2017; Van Buskirk et al., 2017; ElBahrawy et al., 2020). En effet, des études sur les interventions policières sur les cryptomarchés ont démontré un impact limité (Aldridge and Décary-Hétu, 2016; Van Buskirk et al., 2017; Décary-Hétu and Giommoni, 2017). Précisément, dans le cas où le marché est saisi et fermé, les chercheurs ont remarqué un important déplacement des activités des utilisateurs vers un autre marché encore actif (Barratt et al., 2016; van Buskirk et al., 2017; van Wegberg et Verburgh, 2018; Ladegaard, 2019; Miller, 2019). Par exemple, dans le cas de l'opération *Onymous,* celle-ci n'a causé qu'un déplacement des utilisateurs vers d'autres plateformes sans les dissuader (Tsuchiya et Hiramoto, 2021). De plus, les études ont démontré que ces interventions policières n'ont qu'un effet à court terme et temporaire sur les marchés illicites (Soska et Christin, 2015; Décary-Hétu et Giommoni, 2017; van Buskirk et al., 2017; Bhaskar et al., 2019; Ladegaard, 2019; Norbutas et al., 2020) et ont même contribué à augmenter le nombre de marchés actifs (Bhaskar et al., 2019). En effet, il semblerait que la médiatisation des accomplissements policiers sur les marchés illicites a amené des impacts pervers, dont la popularisation de ce type de services en ligne (Bhaskar et al., 2019). De plus, ces opérations auraient comme effet d'encourager la communauté des marchés illicites à s'adapter en réponse aux faiblesses d'anonymat exposées par les forces policières en améliorant le système qui était en place, comme il fut le cas avec *Silk Road* 2.0. (Ladegaard, 2019). Ainsi, cela amène les utilisateurs à devenir plus vigilants des faiblesses technologiques qui existent sur ces plateformes et à agir plus sécuritairement (Soska et Christin, 2015; Barratt et al., 2016).

Par ailleurs, de nombreux chercheurs proposent d'utiliser des méthodes alternatives afin d'adapter les interventions policières à ce nouveau phénomène (DiPiero, 2017; Lane et al., 2018). Par exemple, certains chercheurs proposent de cibler davantage les acteurs des marchés illicites plutôt que la plateforme (Broséus et al., 2016; DiPiero, 2017). Ce type d'intervention amène les agences policières à concentrer leurs efforts sur l'identification des utilisateurs (DiPiero, 2017) en faisant par exemple de l'infiltration dans les marchés afin de créer des relations de confiance auprès des vendeurs les plus prolifiques (Martin, 2014). Malgré cela, l'étude de Holt et al., (2015), affirme grâce à l'observation de 10 forums et marchés illicites de piratage informatique que les utilisateurs

ne sont pas dissuadés par une menace ou l'arrestation d'un membre du forum, ceux-ci continuent simplement leurs activités en contrôlant leurs propres interactions. Cependant, les utilisateurs des forums se basent énormément sur la réputation de leurs pairs afin d'échanger ou de commercer avec ceux-ci (Turgeman-Goldschmidt, 2005; Dupont et al., 2016). Plusieurs vendeurs mettent beaucoup d'efforts dans un forum afin d'augmenter leur réputation, cependant, si ce forum est fermé, tous leurs efforts sont perdus (Turgeman-Goldschmidt, 2005; Frank et al., 2018; Zambiasi, 2020). Cela motive d'ailleurs les utilisateurs des plateformes sur le darkweb à être actifs sur plusieurs forums ou marchés simultanément, dans l'objectif d'acquérir à la fois davantage de connaissances (Motoyama et al., 2011; Haslebacher et al., 2017; Biswas et al., 2018), mais aussi pour se prémunir des perturbations qui peuvent nuire drastiquement à leur réputation (Frank et al., 2018). En supplément, les utilisateurs des cryptomarchés se sont récemment tournés vers la vente directe (« *direct dealing* » en anglais), impliquant l'utilisation de courriels ou de messageries cryptés afin d'effectuer des achats directement avec leur vendeur pour éviter une possible interception de preuves digitales par une tierce personne sur un forum ou marché illicite (Barratt et al., 2016; Childs et al., 2020). Ces situations amènent des difficultés supplémentaires aux policiers.

En résumé, en plus des difficultés que les cybercrimes causent, le darkweb ajoute des difficultés supplémentaires à la réponse policière à cause de l'anonymat qu'il procure à ses utilisateurs, des technologies poussées de cryptage, l'utilisation de cryptomonnaies afin de masquer les transactions et la résilience de ces utilisateurs.

3. La collaboration internationale en contexte de cybercrimes

3.1. Le manque de ressources et de formations

Les agences policières se retrouvent bien souvent dans l'incapacité d'intervenir face aux crimes impliquant l'utilisation de technologies anonymisantes, principalement à cause du manque de ressources et de formations (Brown, 2015; Harkin et al., 2018; Faubert et al., 2021). En effet, le nombre croissant de cybercrimes dépassent les capacités d'intervention des agences policières, laissant ainsi un nombre important de crimes et criminels passer sous le radar. Les agences policières doivent alors prioriser certains types de crimes, car elles ne peuvent simplement pas tous

les prendre en charge. Malheureusement, les cybercrimes sont souvent ceux laissés de côté (Leukfeldt et al., 2013; Boes et Leukfeldt, 2017), et ce, pour de nombreuses raisons selon la littérature. Il est possible de les rapatrier en trois principales catégories 1) le manque de compétences et d'expériences, 2) la sous-estimation de l'importance de ce type de criminalité et 3) le manque de main-d'œuvre.

Premièrement, les officiers de police manquent souvent de connaissances, de formations et d'expériences sur les technologies et les nouvelles méthodes criminelles, ce qui les amène à se tenir loin de celles-ci (Calderoni, 2010; Leukfeldt et al., 2013; Boes et Leukfeldt, 2017; Dolliver, 2019). Effectivement, de nombreuses études ont affirmé que les policiers ne se sentent pas assez préparés pour faire face aux crimes impliquant des technologies et que les formations qu'ils reçoivent sont trop brèves et de surface (Bossler et Holt, 2013; Burns et al., 2004; Hadlington et al., 2018; Harkin et al., 2018; Burruss et al., 2019). Précisément, dans le cadre de l'étude qualitative de Harkin et al. (2018) réalisé en Australie, ils ont observé que le manque de formation policière se fait ressentir à différents niveaux. En effet, les besoins de formations ne sont pas les mêmes pour les agents de première ligne, les enquêteurs généralistes, les enquêteurs spécialisés ou les civils travaillant dans les unités de cybercrimes (Harkin et al., 2018). Chaque rôle, bien qu'ils soient tous issus d'une même agence policière, a des besoins particuliers et spécifiques en termes de formations pour assurer une réponse efficace et adaptée aux crimes technologiques. Bien qu'ils reconnaissent un manque important de formation au sein de la police, ils postulent qu'il existe quatre raisons supplémentaires à l'insuffisance policière : 1) les compétences techniques et l'expérience approfondie nécessaires pour qu'une unité spécialisée en cybercriminalité soit efficace est difficile à acquérir, 2) la constante évolution des technologies mène à une courte durée de l'expertise en cybercriminalité, et ainsi, à un constant besoin d'acquérir de nouvelles connaissances, 3) le phénomène de la fuite de cerveau (« *brain drain* » en anglais) où les policiers développant une expertise sont souvent incités à basculer du côté des organisations privées, afin d'obtenir un salaire nettement plus élevé et 4) les limitations imposées sur le cheminement de carrière des civils spécialistes au sein des unités cyber (Harkin et al., 2018).

Deuxièmement, les cybercrimes sont encore perçus comme des crimes à haut volume, considérant leur fréquence et le nombre de cas répertoriés, mais avec peu d'impacts sur la société, selon l'échelle de gravité de la police (Wall, 2007b; Dupont, 2017). En effet, tout comme le recense

l'étude de Button et al. (2022), de nombreuses études supportent le postulat que la police perçoit les cybercrimes comme étant non-sérieux en termes de gravité et donc de faible priorité (Wall, 2007, 2008; Bossler et Holt, 2012; Holt et Bossler, 2012a, 2012b; Cross, 2015, 2018, 2020; Hadlington et al., 2018; Correia, 2019; Bossler et al., 2020; Leukfeldt et al., 2020; Cross et al., 2021; Notté et al., 2021; Paek et al., 2021). Cela amène les organisations policières à ne pas concentrer leurs ressources dans les interventions et enquêtes sur les cybercrimes, lorsque celles-ci ne sont pas dans les principales préoccupations du politique. En effet, bien que certaines agences policières aient investi dans l'expertise et les technologies, il reste que leurs ressources sont davantage déployées dans les cas de haute gravité ou ceux qui impliquent les crimes contre les enfants sur Internet, et non les nombreux appels de cas de fraudes ou de cartes de crédit volées (Dodge et Burruss, 2020).

Troisièmement, le manque de personnel qualifiés et spécialisés pour répondre aux besoins spécifiques des cybercrimes est une problématique importante (Chang, 2012; Hadlington et al., 2018; Harkin et al., 2018). Comme mentionné précédemment, les individus policiers ou civils qui se développent une expertise peuvent être enclins à quitter la police pour un meilleur salaire dans une compagnie privée (Harkin et al., 2018), ce qui cause une instabilité au sein des équipes et nuit à la rétention de personnels adéquatement qualifiés. De plus, le nombre de policiers pour répondre aux crimes technologiques est tout simplement insuffisant comparativement aux nombres de cas et cela s'applique particulièrement aux enquêteurs (Chang, 2012). Cela peut s'expliquer par le manque de ressources financières octroyées aux unités pour engager de la main-d'œuvre, par le roulement important de personnels qualifiés ou par le manque d'intérêt des enquêteurs (Chang, 2012). Tout comme l'illustre l'étude de Chang (2012) réalisé auprès d'enquêteurs taiwanais et chinois, certaines agences policières dans le monde utilisent un système de pointage afin d'évaluer la performance des enquêteurs. Toutefois, à cause des nombreuses difficultés qu'apportent les cybercrimes aux enquêtes (Li, 2018) de nombreux cas ne seront pas résolues et seront ainsi jamais considéré comme « complété ». Cela nuit considérablement à la productivité des enquêteurs, n'accumulant pas de points pour leur évaluation, causant ainsi un manque, voir l'absence, d'intérêt à joindre une unité cyber alors qu'ils peuvent travailler dans d'autres unités rapportant davantage de « succès » (Chang, 2012).

3.2. La nécessité de collaboration

Comme mentionné précédemment, les agences policières se retrouvent bien souvent dans l'incapacité d'intervenir à cause du manque de ressources et de formations sur les crimes impliquant des technologies (Brown, 2015; Harkin et al., 2018; Faubert et al., 2021). Une des solutions proposées à ce problème est de favoriser les collaborations internationales qui transcendent les juridictions (Burns et al., 2004; Sarre et al., 2018; Wang et al., 2020). Cependant, la riche littérature sur le sujet de la collaboration internationale date des années 1990-2010 (Nadelmann, 1993; Aromaa et Viljanen, 2005; Andreas et Nadelmann, 2008; Roberson et al., 2010; Lemieux, 2010; Mandel, 2011) et se concentre uniquement sur la résolution de crimes reliés au trafic de drogues, au crime organisé et à la lutte contre le terrorisme. Cela implique que cette littérature classique ne prend pas en considération l'ensemble des difficultés supplémentaires qu'ajoutent les cybercrimes et encore moins les difficultés reliées aux technologies anonymisantes comme le darkweb. À ce jour, deux études se sont concentrées sur la collaboration internationale en matière de réponse policière à des cybercrimes. Néanmoins, aucune étude recensée ne s'est concentrée sur la collaboration policière en contexte de crimes commis à l'aide d'outils technologiques complexes qui masquent l'identité des suspects, comme le darkweb.

Premièrement, dans l'étude de Dupont (2017) portant sur la régulation policière des Botnets[11], trois approches de régulation et de contrôle de la criminalité sont décrites afin d'illustrer leurs défis et leurs efficacités. Précisément, les stratégies observées sont 1) l'incarcération de pirates informatiques par les agences policières afin d'avoir un effet dissuasif, 2) la perturbation des réseaux de Botnets par la compagnie privée Microsoft et 3) la réduction des méfaits à l'aide d'une initiative d'entente entre des organisations publiques et privées dans cinq pays. Les résultats de l'étude démontrent que le modèle traditionnel d'application de la loi locale par les agences policières est inadéquat pour faire face à des problématiques internationales. Ce sont davantage les stratégies innovantes menées par une juxtaposition d'acteurs privés en collaboration avec différentes agences policières qui ont conduit des résultats encourageants. Cependant, Dupont (2017) précise que l'évaluation de l'efficacité et de l'acceptabilité de ces stratégies n'est pas décrite dans la littérature. Il existe peu de preuves empiriques sur la pertinence des stratégies

[11] Les Botnets consistent à des réseaux de robots informatiques. Ils sont souvent définis comme étant des réseaux de machines (ordinateurs) infectées par des logiciels malveillants qui permettent aux criminels ou aux maîtres des bots (« botmasters » en anglais), de contrôler des milliers voire millions de machines à distance (Rajab et al., 2006).

d'intervention de régulation policière qui incluent des collaborations en contexte de crimes technologiques, malgré sa pertinence pratique (Dupont, 2017).

Deuxièmement, l'étude de Wang et al. (2020) s'est penchée sur le cas médiatisé du piratage informatique de la *First Commercial Bank* (FCB), une institution financière renommée à Taiwan. En 2016, un regroupement d'individus malveillants avait programmé des guichets automatiques à différents endroits sur l'île afin de sortir tout l'argent qu'ils contenaient, pour un total de 2,6 millions d'USD. De plus, ce même regroupement d'individus avait commis plus d'une centaine de piratages similaires de guichets automatiques dans plus d'une dizaine d'institutions financières en Europe auparavant. Les chercheurs ont recueilli un nombre inconnu d'entrevues au sein d'agents policiers impliqués dans l'enquête qui a suivi. Les résultats ont démontré que la collaboration entre les agences policières nationales taiwanaises, certaines agences fédérales des États-Unis et les nombreuses agences locales sur l'île ont permis d'identifier des suspects et d'amener en justice les pirates informatiques (Wang et al., 2020). De plus, cette étude démontre la pertinence pratique de la collaboration internationale en général, mais aussi de la collaboration entre les agences policières nationales avec les agences policières locales qui possèdent moins de ressources et connaissances pour intervenir dans ce type de criminalité transnationale.

En somme, ces deux études sont arrivées à la conclusion que les collaborations internationales entre les agences policières sont nécessaires à la réussite des interventions et enquêtes policières sur les crimes technologiques qui transcendent les juridictions. Néanmoins, aucune étude recensée ne s'est concentrée sur la collaboration policière en contexte de crimes commis sur le darkweb.

3.3. Initiatives de collaboration internationale en matière de cybercriminalité

Dans les dernières années, certains auteurs ont proposé de développer une agence policière internationale strictement dédiée à l'enquête des cybercrimes afin de répondre à ce besoin de collaboration (Moore, 2015). Néanmoins, considérant la grande variété de lois, chartes et systèmes pénaux dans le monde, aucune agence policière internationale n'est dédiée à la lutte contre les cybercrimes à ce jour. Ainsi, les multiples agences policières de partout dans le monde doivent collaborer entre-elles afin de contourner les limites imposées par les juridictions, le fonctionnement traditionnel de la police et les caractéristiques anonymes des cybercrimes en général. Considérant les difficultés supplémentaires que le darkweb apporte aux interventions

policières, il est adéquat de suggérer que la collaboration internationale est aussi pertinente et s'avère efficace dans la résolution des crimes commis sur le clearweb.

Malgré le manque d'études sur le sujet, il est possible de trouver certaines ressources mises à disposition par des institutions de collaboration formelles afin de faciliter l'échange d'informations à propos des cybercrimes ou afin de faciliter l'avancement des enquêtes (Pickering et Fox, 2022). Par exemple, Interpol a développé dans les dernières années un centre de coordination pour les crimes technologiques (*« Cyber Fusion Centre* » en anglais) afin de recueillir des experts dans les crimes technologiques et d'aider les organisations membres dans l'avancement de leurs enquêtes (Interpol, 2017). De plus, ils ont développé des partenariats privés afin d'être à la fine pointe des technologies et de former les officiers de police qui en font la demande (Interpol, 2017). Dernièrement, ils offrent un laboratoire d'informatique légale, afin d'aider la détection de preuve chez les officiers de première ligne (Interpol, 2017). Ces ressources viennent répondre à un grand besoin de nombreuses organisations policières.

En supplément, Europol a développé le *European Cybercrime Center* (EC3) en 2013 afin d'apporter de l'assistance technique à la suite de l'avènement des nombreux cybercrimes au sein de ces pays membres (Europol, 2022). Un an plus tard, le EC3 a fait naître l'unité opérationnelle J-CAT (Europol, 2022; Europol, 2023) qui s'avère grandement utile pour coordonner les opérations policières et pour accumuler du renseignement criminel comme l'opération SpecTor le démontre (voir Europol, 2023, 2 mai). J-CAT ne se limite pas aux pays 12 pays membres de l'Union européenne, mais inclut aussi l'Australie, le Canada, la Colombie, la Norvège, la Suisse, le Royaume-Uni et les États-Unis (Europol, 2023). De plus, un traité international a été fondé au début des années 2000 afin de faciliter le partage d'informations à l'international. Nommée la Convention de Budapest, cette entente formelle visait à faciliter le partage d'information sur les cybercrimes, que ce soit pour la détection, l'investigation ou la poursuite des cybercriminels en établissant des cadres juridiques communs (Calderoni, 2010; Pool et Custers, 2017) au sein des 65 pays membres qui proviennent de l'Europe, l'Asie, les Amériques et le Pacifique (Gouvernement de la Nouvelle-Zélande, 2020). Ainsi, ces initiatives de collaboration internationale formelle ont pour objectif commun de venir en aide aux agences policières dans la lutte contre les cybercrimes. Néanmoins, selon les études de Dupont (2017) et Wang et al. (2020), les collaborations informelles semblent être davantage celles qui sont priorisées afin de mener à terme les enquêtes ou pour avoir

un réel impact sur la régulation des cybercrimes. Il serait alors possible d'hypothétiser que les enjeux répertoriés dans les études sur les crimes internationaux du début du 21e siècle soient encore d'actualité, faisant en sorte que les agences policières préfèrent avoir recours à des collaborations informelles qu'aux services offerts par Interpol ou la Convention de Budapest.

3.3.1. Avènement de la collaboration entre le secteur public et privé

Les institutions privées sont décrites comme des infrastructures dans lesquelles les décisions sont prises à l'intérieur d'un modèle d'affaire qui se base sur le profit, l'expérience des clients et l'intérêt des actionnaires ou de ces dirigeants (Carr, 2016). Comme le recense Pomerleau (2019) dans son ouvrage, de nombreuses initiatives visant à améliorer la collaboration entre les secteurs public et privé ont été fondées mondialement dans les dernières années. Malgré l'avènement des initiatives de partenariats publics-privées (« Public-Private Partnerships » (PPPs)), l'accès aux données, qui représentent des preuves digitales pour les enquêtes, témoigne d'une grande complexité encore à ce jour. En effet, il n'est pas évident d'obtenir légalement des preuves judiciaires sans compromettre la confidentialité numérique des citoyens et clients (Tun et al., 2016; Vincze, 2016). De plus, les PPP sont composés d'interactions alambiquées entre des parties ayant des objectifs distincts (Dodge et Burruss, 2019). En ce sens, la police a pour but de protéger la société en maintenant l'ordre public (Lemieux, 2018) et les compagnies privées de technologies de l'information et communication (« *Information and Communications Technology sector* (ICT) » traduction libre de l'anglais) visent la capitalisation de profits (Carr, 2016). Cette disparité engendre des doutes quant aux intentions de chacun et cela nuit à la confiance qui est fondamentale à la collaboration (Dodge et Burrus, 2019). Étant donné la complexité des collaborations entre ces deux acteurs, de nombreux chercheurs ont signalé la nécessité d'examiner plus en profondeur cette interaction (Hinduja, 2007; Wexler, 2014; Vincze, 2016; Dodge et Burruss, 2019).

Par ailleurs, en plus de devoir collaborer avec les compagnies privées afin d'acquérir des preuves digitales, la police se voit dépendante des produits offerts par le secteur privé. De nombreuses compagnies vendent des produits et services qui sont essentiels à l'enquête policière sur les crimes technologiques, par exemple Chainanalysis[12] offre des produits dispendieux qui aide au traçage et à l'enquête des transactions de cryptomonnaies.

[12] https://www.chainalysis.com/

CHAPITRE 2: PROBLÉMATIQUE

1. Résumé des connaissances

Mondialement, les organisations policières sont responsables de résoudre les crimes qui sont commis physiquement dans les juridictions qui leur sont attribuées. Cependant, ce fonctionnement n'est pas adéquat dans le cas des cybercrimes, considérant qu'ils sont commis virtuellement et non physiquement dans l'espace (Cross, 2020). De 2015 à 2020, l'Internet Crime Complaint Center (IC3) a répertorié plus de 2 millions de plaintes provenant de victimes de cybercrime (IC3, 2020), et ce, seulement aux États-Unis. Cela implique autant les cybercrimes dans lesquels la technologie est la cible (ex., les attaques de déni de service ou les logiciels malveillants) que les infractions où la technologie est l'instrument (ex., la fraude, le vol d'identité, l'exploitation sexuelle d'enfants, le trafic de drogues, etc.) (Gendarmerie Royale du Canada, 2015). Dans les dernières années, des milliers de criminels utilisent le darkweb, la portion cachée de l'Internet, afin de commettre des cybercrimes (Moore et Rid, 2016). En effet, le darkweb devient un endroit très intéressant pour les criminels étant donné ses technologies qui cachent l'identité des utilisateurs (Naseem et al., 2016; Mirea et al., 2019; Kaur et Randhawa, 2020).

Cependant, face à cette hausse grandissante de nouvelles méthodes de commettre des crimes, les agences policières se retrouvent bien souvent dans l'incapacité d'intervenir face aux cybercrimes à cause du manque de ressources ou de formations (Brown, 2015; Harkin, Whelan et Chang, 2018; Faubert et coll., 2021). Une des solutions proposées à ce problème est de favoriser les collaborations internationales qui transcendent les juridictions (Burns et coll., 2004; Sanders et Henderson, 2013, Sarre et al., 2018). Cependant, la littérature sur le sujet de la collaboration internationale date des années 1990-2000 (Nadelmann, 1993; Aromaa et Viljanen, 2005; Andreas et Nadelmann, 2008; Roberson, Das, Singer, 2010; Lemieux, 2010; Mandel, 2011) et se concentrent sur la résolution de crimes reliés au trafic de drogues, au crime organisé et au terrorisme. Quelques études ont tenté d'illustrer la pertinence des innovations stratégiques de collaboration en matière de réponse policière sur les cybercrimes (ex., Dupont, 2017; Wang et al., 2020). Malgré cela, il existe peu de preuves empiriques sur la pertinence des stratégies d'intervention de régulation policière en contexte de crimes technologiques, malgré sa pertinence pratique (Dupont, 2017). Par ailleurs, Dupont (2017) évoque que sa démonstration empirique pourrait permettre d'adopter une approche plus durable.

Notamment, on retrouve deux types de collaboration internationale dans la littérature. Le premier type consiste aux collaborations formelles impliquant des organisations officielles (ex., Interpol ou Europol) (Lavers et Chu, 1997; Rothe et Friedrichs, 2015; Lemieux, 2018). Cependant, en raison de la lenteur de ces organisations (Lavers et Chu, 1997), plusieurs corps policiers vont avoir recours à un type de collaboration qualifié d'informel. Dans ce cas, les collaborations sont faites entre des agents policiers, enquêteurs ou agents spécialisés qui communiquent avec un ou plusieurs autres policiers d'une agence externe à la leur sans entreprendre des procédures administratives ni hiérarchiques (Inyang et Abraham, 2013). Afin d'accomplir ce type de collaboration, les agences doivent réaliser du réseautage pour créer des alliances informelles (Kreiner et Schultz,1993; Lavers et Chu, 1997; White, 2011; Inyang et Abraham, 2013; Kim et al., 2013).

Pour faciliter les collaborations inter agence de basse police, des initiatives comme le traité Convention de Budapest sur les cybercrimes au début des années 2000, le département des cybercrimes de Interpol et le EC3 facilitent le partage d'information à l'international, que ce soit pour la détection, l'investigation ou la poursuite des cybercriminels (Calderoni, 2010; Interpol, 2017; Pool et Custers, 2017; Europol, 2022). Cependant, bien que de nombreux pays aient signé la convention et que ces deux institutions investissent beaucoup dans les ressources qu'ils offrent, la pertinence et l'utilité de ces initiatives et des collaborations internationales en général n'est pas reconnue ni mesurée dans la littérature à ce jour (Dodge et Burruss, 2019). De plus, les études de Dupont (2017) et Wang et al. (2020) ont démontré grâce à des études de cas que les agences policières ont recours à des collaborations informelles pour intervenir ou faciliter leurs enquêtes, et ne font pas appel aux institutions formelles.

1.1. Limite soulevée par la littérature

À la suite de cette revue de la littérature, nous avons observé qu'à ce jour, aucune étude ne combine les thématiques de la collaboration internationale et les crimes commis à l'aide du darkweb. Les études classiques abordent principalement la collaboration en lien avec les crimes reliés au trafic international de drogues ainsi qu'au terrorisme (ex., Nadelmann, 1993; Aromaa et Viljanen, 2005; Andreas et Nadelmann, 2008; Robserson et al., 2010; Lemieux, 2010; Mandel, 2011). Bien que les études récentes sur les interventions policières en contexte de cybercriminalité abordent la pertinence, et même la nécessité des collaborations entre les agences (Burns et al., 2004; Brown,

2015; Sarre et al., 2018; Harkin et al., 2018; Faubert et al., 2021), aucune d'entre elles ne permet de comprendre ce qu'apporte les collaborations aux enquêteurs et comment celles-ci prennent forme dans le contexte précis des crimes commis à l'aide du darkweb. Comme la recension des écrits a exposé, le darkweb apporte des difficultés supplémentaires et spécifiques aux enquêtes (ex., l'identification des utilisateurs, le recours aux technologies de messages cryptés, la constante fermeture et l'ouverture de nouvelles plateformes afin de commettre des actes illégaux sans laisser de traces, etc.). À la lueur de ce postulat, duquel nous comprenons que les enquêtes policières sur les crimes commis à l'aide du darkweb demandent des techniques d'enquêtes particulières, il n'est pas possible d'appliquer les concepts de la collaboration policière sans valider empiriquement sa convenance. Entre autres, il serait pertinent d'observer si les problématiques des collaborations internationales qui ont été identifiées dans les contextes du trafic de drogues et du terrorisme (ex., le réseautage, la compétition, le délai des communications, etc.) s'appliquent aussi aux crimes commis à l'aide du darkweb. Ainsi, il y a donc un vide dans la littérature sur les raisons qui poussent les enquêteurs à collaborer ainsi que comment les collaborations prennent forme. Nous voulons donc comprendre l'impact des difficultés générées par le darkweb sur la forme que les collaborations prennent ainsi que sur les motivations des enquêteurs à collaborer.

D'ailleurs, les études classiques sur la collaboration internationale ont été réalisées sur un niveau d'analyse macroscopique, impliquant l'analyse des lois et des politiques mises en place (Dupont et al., 2017) en délaissant l'analyse mésoscopique et microscopique des organisations et de leurs structures relationnelles. Considérant la hausse des cas de crimes commis en utilisant le darkweb et son impact sur la police, il est essentiel d'adopter et de développer de nouvelles perspectives, théories et pratiques (Dupont et al., 2017).

1.2.Stratégie pour surmonter la limite

Afin de contrer les limites de la littérature, ce projet de recherche s'intéresse exclusivement aux collaborations policières sur l'enquête de crimes commis à l'aide du darkweb au sein d'institutions de différents niveaux : local, régional et national. En effet, grâce à un corpus de 20 entrevues réalisées auprès d'enquêteurs ayant travaillé sur des crimes commis à l'aide du darkweb réparti dans 5 pays en Amérique, Océanie et Europe, ce mémoire a ainsi comme objectif de comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du

darkweb. Dans le cadre de ces entrevues semi-directives, les participants racontent une intervention ou une enquête policière dans laquelle ils ont participée et comment celle-ci s'est déroulée. Précisément, les participants décrivent une enquête ou une intervention policière impliquant un cybercrime commis à l'aide du darkweb et précisent les résultats de l'intervention, incluant l'atteinte des objectifs initiaux, ainsi que la présence et le rôle de collaboration internationale.

1.2.1. *Objectifs de recherche*

La méthode d'analyse thématique classique permettra de répondre à l'objectif général de ce projet qui consiste à comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb. Précisément, cette étude possède deux objectifs spécifiques. Premièrement, elle vise à décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière. Ce sous-objectif vise donc à comprendre les raisons derrière les collaborations qu'on entreprit les enquêteurs à l'étude afin de saisir la pertinence de celles-ci dans le cadre de leur emploi. Deuxièmement, elle vise à décrire et comprendre les types de collaboration mobilisés dans le cadre d'une enquête policière sur le darkweb. La complétion de ce sous-objectif permettra d'observer la présence ou l'absence des types de collaboration recensée dans la littérature au sein des entretiens des participants et comment celles-ci prennent forme dans le contexte précis des crimes commis à l'aide du darkweb.

En somme, l'identification des motivations et des types de collaboration permettra de comprendre pourquoi et comment les enquêteurs collaborent dans le cadre de leur emploi. De plus, les résultats pourront démontrer empiriquement la valeur ajoutée de la collaboration en produisant des connaissances spécifiques aux crimes commis sur le darkweb. Cela viendra ajouter aux connaissances théoriques ou conceptuelles recensées dans la section précédente tout en actualisant la littérature grâce à l'objet d'étude.

CHAPITRE 3 : MÉTHODOLOGIE

Dans ce chapitre, le choix méthodologique adopté afin de répondre à l'objectif de recherche sera dévoilé. Suivant cet ordre, nous justifierons le choix méthodologique, l'échantillon, la méthode de collecte de données, la méthode d'analyse thématique utilisée ainsi que les limites.

1. Méthodologie qualitative

1.1. Justification de la méthodologie qualitative

Le choix d'avoir recours à une méthodologie qualitative se justifie par la nature descriptive et exploratoire de ce mémoire. À titre de rappel, l'objectif de ce projet est de *comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb.* Les objectifs spécifiques de cette étude visent à :

1) Décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière;
2) Décrire et comprendre les types de collaboration nécessaire à la réalisation d'une enquête policière sur le darkweb.

Comme le mentionne Holloway et Hubbard (2001), inclure l'expérience des humains permet de soutirer une image beaucoup plus riche des connaissances à obtenir. En d'autres mots, l'ajout de l'expérience des participants sur un sujet d'étude permet d'obtenir des résultats beaucoup plus complets. De ce fait, Graham (1997) précise que les études portant sur les humains se doivent d'observer celui-ci comme un être émotif, et non comme un numéro ou une statistique. La méthodologie qualitative permet d'observer l'humain comme un sujet rempli d'émotions, dans son propre contexte et avoir accès à ses attitudes et opinions. Celle-ci ne cherche pas à observer la fréquence d'apparition d'un phénomène (Anadòn et Guillemette, 2007), car elle vise à comprendre la nature et la force des interactions des variables qui entourent une réalité sociale (Zhang et Wildemuth, 2009).

Dans le contexte des études sur la police en général, selon l'analyse de la littérature publiée dans les années 2000 à 2007 par Mazeika, Bartholomew, Distler et al. (2010), il fut courant de réaliser des études exploratoires qui visent à observer l'unité narrative de participants. Récemment, des études sur les unités de police spécialisées en cybercrime ont aussi eu recours à des méthodologies qualitatives, particulièrement l'utilisation d'entretiens afin de réaliser leurs objectifs de recherche

à tendance exploratoire ou descriptive (ex., Hadlington et al., 2018; Harkin et al., 2018; Nouh et al., 2019; Whelan et Harkin, 2021; Harkin et Whelan, 2022; Cheurprakobkit et Lerwongrat, 2023).

Bien qu'il existe différentes formes de données et d'analyses qualitatives, nous avons opté pour les entretiens auprès de participants. Dans l'objectif d'avoir accès au vécu et expériences des enquêteurs, l'entretien auprès des sujets s'avère être la meilleure méthode afin d'obtenir leurs points de vue et perceptions.

Selon Tewksbury (2009), une des façons les plus productives d'apprendre à propos d'un répondant, d'un endroit ou des activités est de questionner les individus à propos de ce sujet par le biais d'une entrevue. Quand un intervieweur questionne un répondant, il vise à le comprendre, comprendre ses expériences ou ses perceptions sur un sujet (Tewksbury, 2009). Les entretiens permettent aux sujets de révéler beaucoup plus d'informations en profondeur que s'ils avaient été observés dans une situation et qu'on en déduisait le sens (Simons, 2009). C'est pourquoi la méthode d'entrevue réalisée auprès des participants consistait à l'entrevue à tendance semi-directive, car ce type d'entrevue aborde généralement un thème principal auquel le participant développe et répond comme il le désire. Les interventions de l'interviewer se limitent à des relances ou des encouragements, pour démontrer une écoute active et un intérêt empathique, sans apporter de nouvelles informations ou diriger la conversation vers une autre direction (Ghiglione et Matalon, 1978). Cette méthode permet donc d'enrichir le matériel et de favoriser l'émergence d'un savoir en laissant la liberté au participant de discuter de ce qui lui vient à l'esprit tout en s'assurant de répondre aux objectifs visés par les entrevues. Les participants dans les entrevues semi-directives du projet de recherche connaissaient à l'avance les thèmes auxquels ils devaient réagir. En revanche, il n'y avait pas d'ordre établi pour aborder les thématiques. Le seul élément qui fut déterminé à l'avance était la consigne de départ (Ghiglione et Matalon, 1978). Dans ce cas-ci, l'intervieweur utilisait la consigne de départ : « Pouvez-vous nous raconter une intervention policière sur le darkweb dans lequel vous avez participé, et nous exprimer son déroulement? ». Toutefois, les entrevues étaient principalement réalisées en anglais. La question de départ fut la suivante : « *Can you tell us about a police intervention on the darkweb in which you participated and tell us how it unfolded*? ».

Les questions de relance s'étalaient sur trois sections ou dimensions (voir Guide d'entretien à l'Annexe 2). Étant donné la nature de l'entrevue semi-directive, les questions de relance étaient

flexibles, elles guidaient l'interviewer afin de couvrir le sujet en profondeur. Toutefois, si le participant divaguait et sortait du « cadre » des questions, l'interviewer suivait la nouvelle direction afin de s'adapter à celui-ci. Nonobstant, les trois principales questions des thématiques de la grille d'entrevues étaient réparties ainsi : 1) la première section portait sur l'intervention ou l'enquête menée 2) la deuxième section portait sur l'impact de cette intervention/enquête 3) la troisième section portait sur leurs perceptions face à l'avenir des futures interventions. Comme il sera discuté dans la section méthode d'analyse, ce mémoire porte notamment sur une sous-question issue de la première section des entrevues:

« *The roles and responsibilities of those involved in the planning of the intervention, including those of people from outside your organization:*

- *collaborations with outside partners: other police forces, parapublic and private organisations and businesses.* »

Toutefois, la totalité des verbatims ont été analysés afin de prendre en considération l'ensemble des informations relatives aux collaborations réalisées par les participants. L'ordre des sections et questions de relance n'étant pas fixe ni ordonné, il fut nécessaire de couvrir l'ensemble des verbatims afin d'identifier les passages pertinents aux sous-objectifs de cette recherche.

1.2. Collecte de données

Les données utilisées dans cette recherche proviennent d'un projet de recherche conduit par un groupe de chercheurs, donc les directeurs de ce mémoire. Précisément, le groupe de chercheurs en question fut composé de David Décary-Hétu (Université de Montréal), Benoit Dupont (Université de Montréal), Aili Malm (University of California), Jerry Ratcliffe (Temple University) ainsi que la coordonnatrice de projet Camille Faubert (initialement étudiante à Université de Montréal et actuellement chercheure pour l'École Nationale de Police).[13] Ce projet initial fut subventionné par PMI Impact[14]. Les informations relatives aux détails méthodologiques de la collecte de données initiales proviennent de la demande éthique ainsi que des discussions auprès des chercheurs impliqués dans le projet.

[13] Le projet fut approuvé par la Comité d'éthique de la recherche – Société et culture de l'Université de Montréal (#CERSC-2019-111-D).
[14] Philip Morris International Inc (PMI) Impact est un organisme subventionnaire privée qui supporte les initiatives contre les trafics illégaux et les conséquences négatives pour les individus et la communauté (PMI Impact, 2023).

Les entretiens ont été conduits principalement par Camille Faubert qui fut accompagnée par un chercheur du groupe pour certaines entrevues. Une fois les entretiens réalisés, ceux-ci ont été transcrits afin de créer des verbatims anonymisés[15]. La transcription des verbatims fut réalisée par des auxiliaires de recherche dont j'ai fait partie. Les entretiens enregistrés par Zoom ont été partagés temporairement et sécuritairement afin que les verbatims soient écrits. La transcription automatique de Zoom fut utile afin de réduire la tâche de transcription des auxiliaires. Une fois les verbatims complétés, les enregistrements des entretiens ont été détruits. Ainsi, les entretiens comportent des numéros afin d'identifier les participants, et seulement la coordonnatrice a connaissance de l'identité de ceux-ci. Les participants ont consenti soit par écrit ou verbalement à l'enregistrement et à la transcription des entretiens.

Recrutement

Le recrutement des participants fut réalisé entre le 5 mars 2020 et le 2 septembre 2021. Il a été réalisé par le groupe de chercheurs initial du projet portant sur les interventions et enquêtes policières sur le darkweb. Les chercheurs ont eu recours à des auxiliaires de recherche, dont j'ai fait partie. Initialement, les chercheurs à l'étude ont contacté des policiers grâce à leurs réseaux de contacts qu'ils ont rejoints par courriel ou téléphone. Par la suite, grâce à l'effet boule-de-neige issue de références des participants, ils ont pu obtenir quelques participants supplémentaires. Cependant, la pandémie de la COVID-19 avait drastiquement ralenti le recrutement après quelques mois d'effort pour trouver des participants. Ainsi, les chercheurs ont eu recours au recrutement par le réseau social professionnel LinkedIn afin de contacter des enquêteurs, sergents et agents spéciaux s'affichant publiquement comme travaillant dans une unité de cybercriminalité. De cette façon, 51 participants ont répondu à l'appel. De plus, étant donné les restrictions de transports et de contacts physiques, les entretiens ont été réalisés virtuellement sur la plateforme Zoom[16].

Les critères d'inclusion et d'exclusion initiaux

Dans l'intention d'obtenir une perspective internationale des collaborations, les chercheurs visaient à collecter des données auprès de cinq pays : l'Australie, le Canada, les États-Unis, les Pays-Bas et le Royaume-Uni. Toutefois, ils ont inclus dans la recherche tout participant répondant

[15] Les entretiens ont été identifiés d'un numéro de 1 à 51. L'identité des participants n'est uniquement connue des interviewers présents lors des entretiens ou des membres de l'équipe de recherche initiale qui ont recruté ses participants. Les verbatims sont donc anonymisés et toutes informations subjectives pouvant menant à l'identification de ceux-ci ou de leur organisation ont été enlevées.
[16] Zoom est une plateforme de vidéoconférence californienne (https://www.zoom.us/).

aux critères provenant d'un pays issu des continents nord-américain, européen et océanique. En ce qui concerne les critères d'inclusion, les participants devaient être d'âge majeur, employé comme policiers dans un pays visé par la recherche et s'exprimer en anglais ou en français, étant les deux langues parlées des interviewers. Précisément, ils devaient avoir une connaissance des interventions ou des enquêtes policières sur les crimes commis à l'aide du darkweb. Il n'y avait pas de critères précis quant à l'âge, le sexe, l'origine ethnique, l'orientation sexuelle, le nombre d'années d'ancienneté ni leur grade au sein de leur organisation policière. Ainsi, les participants qui ne répondaient pas à ces critères ont été exclus de la recherche.

1.3. Échantillonnage

L'échantillon primaire de l'étude contient 51 entretiens auprès de policiers provenant d'agences policières issus de huit pays : le Canada (39%), les États-Unis (29%), le Royaume-Uni (18%); l'Australie (6%); la France (2%); l'Italie (2%); les Pays-Bas (2%) et la Suisse (2%)). Cela représente un total de 46 heures de contenu, avec un temps moyen par entretien de 55 minutes [intervalle : 29- 96 minutes]. Les participants ont consenti par écrit (46/51) ou verbalement (5/51) à l'étude. Les entrevues ont été enregistrées et retranscrites afin de créer des verbatims (46/51) à l'exception de cinq entretiens dans lesquels des notes ont été prises.

Précisément, l'échantillon est composé de 80% d'hommes et 20% de femmes. L'âge moyen des participants est de 45 ans [intervalle : 25-60] et 75% d'entre eux possédaient un diplôme d'étude de niveau collégial ou supérieur. En moyenne, ils avaient 20 ans d'expérience dans la police [intervalle : 3-37].

L'échantillon comporte une grande variété de titres de policiers comme il est possible d'observer au Tableau 1. Un total de 10% des participants n'ont pas divulgué leur titre. Il est à prendre en considération que chaque agence policière possède sa propre structure hiérarchique et sa description de rôle. Ainsi, deux titres similaires ou différents peuvent avoir les mêmes responsabilités selon le pays et le niveau de police de celles-ci. Toutefois, malgré la diversité de rôle policier dans l'échantillon, les participants ont tous en commun une connaissance des interventions policières sur le darkweb réalisées par leur agence. En ce qui concerne les niveaux de police des participants, ils sont principalement répartis sur trois niveaux : Nationale/Fédéral (39%), régional/État/provincial (29%) ou local/municipal (22%). Deux participants étaient

officiellement des officiers d'État prêtés à la police fédérale et deux autres occupent un rôle exerçant des responsabilités issues des trois niveaux de police (locale, régionale et nationale). Un seul participant était issu d'une agence policière internationale. En somme, 71% des participants étaient encore en fonction, 22% étaient retraités et 7% avaient quitté les forces policières.

Tableau 1. Description de l'échantillon initial

Caractéristiques descriptives	**Statistiques**
Identité de genre :	
Homme	41 (80 %)
Femme	10 (20 %)
Âge (moyen) :	45 ans [intervalle : 25-60]
Manquant	6 (12%)
Éducation :	
Diplôme d'études supérieures	9 (18%)
Baccalauréat/Certificat universitaire	24 (47%)
Collégial	5 (10%)
Secondaire	6 (12%)
Manquant	7 (14%)
Années d'expérience dans la police (moyenne) :	20 ans [intervalle : 3-37]
Manquant	6 (12 %)
Pays :	
Canada	20 (39%)
États-Unis	15 (29%)
Royaume-Uni	9 (18%)
Australie	3 (6%)
France	1 (2 %)
Italie	1 (2 %)
Pays-Bas	1 (2 %)
Suède	1 (2 %)

Rang/Fonction :	
Enquêteur/détective	14 (27%)
Sergent/Chef d'équipe	9 (17%)
Enquêteur en chef/Sergent enquêteur	7 (14 %)
Agent spécial	5 (10%)
Sergent agent spécial	3 (6%)
Analyste civil	2 (4%)
Assistant Caporal	1 (2%)
Constable	1 (2%)
Procureur adjoint	1 (2%)
Directeur adjoint	1 (2%)
Directeur adjoint exécutif	1 (2%)
Sergent d'État-Major	1 (2%)
Manquant	5 (10%)
Niveau d'agence :	
Nationale/Fédérale	20 (39%)
Régionale/État/Provinciale	15 (29%)
Locale/Municipale	11 (22%)
Responsabilités partagées	3 (6%)
Internationale	1 (2%)
Autre	2 (4%)
Statut de travail :	
À l'emploi au sein de la police	36 (71%)
À la retraite	11 (22%)
A quitté la police	4 (7 %)

La vaste majorité des entrevues ont été conduites en anglais, à l'exception de quelques entretiens auprès de la communauté francophone du Canada. Pour des raisons de respects des conditions du consentement, le nombre exact de francophones ayant participé à l'étude ne sera pas divulgué.

1.3.1. *Sous-échantillon : enquêteurs*

Dans le but d'homogénéiser l'échantillon, uniquement les entretiens avec des participants occupant un rôle d'enquêteur, de sergent enquêteur ou d'inspecteur[17] ont été inclus. Un chef d'équipe et enquêteur fut retiré de l'échantillon, car le participant ne réalisait pas d'enquêtes dans

[17] Le terme inspecteur fut surtout utilisé en anglais, à titre de synonyme. Il est à noter que les agences policières dans le monde n'utilisent pas tous les mêmes titres pour des postes similaires.

le cadre de ces fonctions. Il occupait davantage des fonctions de gestion et de supervision, l'entretien ne permettait pas d'observer l'objet d'étude de ce mémoire. Un sous-échantillon fut ainsi créé représentant un total de 20 entretiens[18].

Précisément, les participants sélectionnés proviennent de cinq pays : le Canada (45 %), la Suède (5 %), le Royaume-Uni (25 %), les États-Unis (10 %) et l'Australie (15 %) (voir Annexe A). L'échantillon comprenait 30 % de femmes et 70 % d'hommes. Plus de la moitié des participants ont un diplôme universitaire (70%) et une moyenne de 20 ans d'expérience dans la police [écart : 12-37]. À l'exception de deux participants qui avaient pris leur retraite ou ont quitté leur emploi au sein de leur agence policière, ils travaillaient activement au moment des entrevues (90 %). Le temps moyen des entretiens était de 52 minutes [intervalle de 29 – 72 minutes]. À l'exception de deux participants ayant des responsabilités partagées dans différents niveaux de police. Les policiers provenaient de différents niveaux d'agences policières : 35% d'agences provincial/régionale/État (35%), d'agences municipales (35%), d'agence de niveau fédéral (10%). Finalement, deux participants étaient formellement des policiers d'état, mais prêtés à la police fédérale (10%).

Pour la gestion des données secondaires, chaque entretien a été identifié aléatoirement d'un numéro de 1 à 20 afin de créer la nouvelle base de données.

2. Méthode d'analyse

Dans ce mémoire, la méthode d'analyse adoptée consiste à l'analyse thématique d'entretiens sous une approche inductive et itérative. Les entretiens auprès d'enquêteurs policiers ont été codifiés et nous avons procédé à l'identification de thèmes et sous-thèmes afin de répondre à l'objectif et aux sous-objectifs de la recherche. Uniquement l'auteur de ce mémoire a complété la codification et l'analyse des données. Toutefois, les chercheurs impliqués dans la recherche ont validé la pertinence et la justesse des thèmes identifiés en lien avec l'objet d'étude afin d'obtenir un accord interjuge.

[18] Ce projet de mémoire fut approuvé par le Comité d'éthique de la recherche – Société et culture de l'Université de Montréal (#CERSC-2022-109-D).

Inductive

L'approche inductive consiste à développer des thèmes à partir des éléments présents dans les données collectées (Fereday et Muir-Cochrane, 2006; Zhang et Wildemuth, 2009; Hadlington et al., 2018). Ainsi contrairement à l'approche déductive (voir Hyde, 2000; Elo et Kyngäs, 2008; Azungah, 2018), les thèmes ne ressortent pas des intérêts ni des objectifs préétablis par les chercheurs afin de tester des théories ou hypothèses (Martineau et Blais, 2006; Thomas, 2006). Dans la recherche déductive, l'analyse est opérationnalisée à l'aide de connaissances et concepts qui sont basés sur les connaissances préexistantes (Elo et Kyngäs, 2008; Hsieh et Shannon, 2005; Mayring, 2014; Armat et al., 2018). De ce fait, l'approche inductive s'avère la mieux adaptée à l'objet d'étude, étant construit sur des connaissances partielles sur le sujet et un manque de preuve empirique. Ainsi, cette méthode est recommandée lorsque le but de l'analyse est de créer des connaissances à l'aide d'expériences partagées par les participants sans se baser sur une théorie ou des résultats préexistants (Elo et Kyngäs, 2008; Hsieh et Shannon, 2005; Thomas, 2006). Rappelons que ce projet se base sur des données secondaires, ce devis ne fut créé pour répondre à des hypothèses prédéterminées, mais bien explicitement dans un objectif d'exploration des points de vue des enquêteurs. Concrètement, l'exploration de données qualitatives sous l'approche inductive implique une lecture en profondeur des données afin de faire ressortir naturellement les thématiques qui s'y trouvent (Hsieh et Shannon, 2005; Fereday et Muir-Cochrane, 2006; Elo et Kyngäs, 2008; Zhang et Wildemuth, 2009; Hadlington et al., 2018). Le chercheur lit ainsi chaque phrase des entretiens afin d'y assigner des codes à chaque paragraphe ou passage textuel qui est pertinent au sujet d'étude (Azungah, 2018). Les questions de recherche deviennent ainsi les lunettes avec lequel les chercheurs observent les données (Azungah, 2018).

Subjectivité et unité narrative

La méthodologie qualitative se fait régulièrement reprocher de comporter des biais importants nuisant à la validité des résultats qui manquent d'objectivité. En effet, la méthode qualitative est teintée d'une subjectivité quasi omniprésente. Elle se manifeste, entre autres, du côté du chercheur qui mène l'entretien (Beck, 1998; Ratner, 2002; Anadòn et Guillemette, 2007), considérant qu'il est presque impossible d'éliminer leurs connaissances et perceptions préexistantes (Roulston et Shelton, 2015). Toutefois, il est ainsi nécessaire de faire valider les résultats par plusieurs chercheurs afin d'acquérir une validité interne. Par ailleurs, la subjectivité est aussi présente au

sein des participants. En basant l'analyse sur l'unité narrative des participants, représentant leurs mots transcrits dans les verbatims, nous appuyons notre recherche sur le point de vue des enquêteurs sur les collaborations réalisées et vécues. Nous n'observons pas le phénomène, nous observons comment les sujets impliqués s'expriment face à celui-ci. Toutefois, dans ce projet, nous tirons profit de ce biais subjectif afin d'observer les perceptions des policiers face à la collaboration. Les entretiens semi-directifs permettent d'avoir accès au langage des participants, ce qui permet d'accroître notre compréhension de leur réalité lorsqu'ils abordent les thématiques de la recherche tout en reflétant comment ils les conçoivent (Legard, Keegan et kit., 2003). L'entretien se concentre directement sur l'individu dans son contexte, ce qui permet d'obtenir des détails personnels sur leurs opinions, motivations, expériences et rôles identitaires (Legard et al., 2003). Précisément, l'utilisation des unités narratives des professionnels au sein d'une organisation permet d'avoir une vue exclusive du milieu. En effet, cela permet d'identifier les points de vue des participants sur les caractéristiques d'une pratique professionnelle propre à ce milieu (Duchesne, 2000). En somme, nous nous appuyons sur le vécu et les opinions des répondants afin de répondre à nos objectifs de recherche et d'explorer l'objet d'étude grâce à cette subjectivité unique.

2.1. Codification des données

En plus d'avoir opté pour l'approche d'analyse inductive, les données ont été codifiées à l'aide d'un processus itératif, signifiant que les thématiques ont été construites à l'aide d'un retour constant entre les entrevues afin de raffiner et adapter les thématiques tout au long de la codification de ceux-ci. Nous avons commencé par effectuer une première relecture des transcriptions des entretiens afin de construire une liste de thématiques potentielles en lien avec nos deux objectifs spécifiques. Nous sommes passés par un processus itératif et inductif pour relire de nombreuses fois les transcriptions et sélectionner les thèmes finaux qui ont été codés dans QDA Miner (Ritchie et al., 2003).

La méthode d'analyse des données qui est utilisée dans ce projet mémoire consiste à l'analyse thématique classique. Cette méthode implique l'utilisation d'un arbre thématique qui sert à regrouper les thèmes visés initialement et qui sont par la suite retrouvés à l'intérieur des verbatims (Paillé et Mucchielli, 2012). Afin d'analyser le contenu des 20 entrevues, le logiciel QDA Miner, un outil spécialement conçu pour faire de l'analyse qualitative de la gamme de *Provalis*

Research[19], fut utilisé. Ce logiciel permet la codification des entrevues et permet d'en faire ressortir les passages importants ainsi que pertinents pour faciliter l'interprétation des résultats.

2.2. Analyse thématique

Nous avons adopté un cadre d'analyse thématique qui consiste à identifier les éléments et concepts à partir de l'unité narrative des participants et de les transformer en thèmes et sous-thèmes des entretiens (Michelat, 1975 ; Ryan et Bernard, 2003 ; Braun et Clarke, 2006 ; Gavin, 2008 ; Braun et Clarke, 2013 ; Miles, Huberman et Saldana, 2014). Étant donné l'approche inductive et itérative, les thématiques ressortent fluidement et instinctivement à la lecture des entretiens (Fereday et Muir-Cochrane, 2006 ; Zhang et Wildemuth, 2009 ; Hadlington et al., 2018). Un thème représente des patrons récurrents de réponses codifiées à l'intérieur des unités narratives qui sont en lien et ont du sens avec les questions de recherche (Braun et Clarke, 2006).

2.2.1. *Description des thématiques*

À la suite de nombreuses lectures, la codification des entrevues a mené à l'identification de nombreuses thématiques très variées. De par la nature exploratoire de cette étude, nous avons choisie d'analyser en profondeur deux principales thématiques : les motivations à collaborer exprimées par les enquêteurs et les types de collaborations expérimentés par ceux-ci. Les thématiques ressortent des unités narratives des participants lorsqu'ils racontaient le déroulement d'enquêtes qu'ils ont menés qui impliquaient une collaboration, soit inter-agences ou intra-agences.

Le premier thème porte sur les motivations des enquêteurs à collaborer. La motivation fait couramment référence à l'intérêt, le désir, à la volonté ou à l'envie qui pousse un individu à réaliser ou maintenir un but. Elle est ainsi définie comme étant la direction et la persistance d'une action qui est soutenue par une force au sein de l'être dans le but de satisfaire un besoin ou des attentes (Rudolph et Kleiner, 1989). L'étude de la motivation se concentre donc sur les raisons, voire pourquoi les humains agissent d'une certaine façon. Par ailleurs, selon la théorie dynamique des collaborations (voir Emerson et Nabatchi, 2015), le fait de partager des motivations communes représentent le fondement d'une collaboration fonctionnelle et performante (Heikkila et Gerlak,

[19] https://provalisresearch.com/

2015). Ainsi, dans ce mémoire, nous observerons ce qui a motivé les enquêteurs à collaborer dans le cadre de leur emploi afin de comprendre pourquoi ils agissent ainsi. Un total de cinq sous-thèmes/motivations fut identifié : le partage d'information (1), l'efficacité des enquêtes, (2), l'identification des suspects (3), l'identification des victimes (4) et l'arrestation des criminels (5).

Le deuxième thème consiste aux types de collaboration expérimentée par les enquêteurs. Un type représente l'ensemble des caractéristiques communes d'une manière d'agir. Au total trois sous-thèmes/types ont été identifiés : les collaborations formelles (1), informelles (2) et privées (3). Ces thématiques nous permettent de comprendre comment les collaborations prennent forme grâce aux témoignages des sujets.

Les deux thématiques qui sont explorées dans ce mémoire s'avèrent à la fois complémentaires et distinctes. À notre connaissance, aucune étude ne s'est concentrée sur les motivations et les types conjointement. Ainsi, nous avons divisé ce mémoire en deux articles scientifiques traitant individuellement d'un des sous-objectifs de cette recherche par souci de couvrir en profondeur ces thèmes et leur sous-thèmes. Cela nous permet de les contextualiser adéquatement et de mobiliser la littérature existante et appropriée à chacun. Dans la section résultat, nous présenterons en détail les sous-thèmes qui ont émergé à la suite de l'analyse des données.

3. Limites méthodologiques

Grâce à l'utilisation d'entretiens auprès de policiers responsables d'enquêter sur des crimes commis à l'aide du darkweb, nous avons accès à des preuves empiriques riches et originales. Néanmoins, il est essentiel de déclarer les deux principales limites méthodologiques de l'échantillon.

La première limite porte sur l'utilisation de données secondaires. En effet, l'utilisation de données ayant été construites sous un autre objectif de recherche cause des limites importantes à la généralisation des résultats. Bien que les entretiens semi-directifs n'ont pas été limités aux thématiques initiales, la portée de la représentation des résultats à l'ensemble des enquêteurs ou corps policiers des pays ciblés est restreinte. En effet, il est fort probable que les participants aient omis des informations en lien avec les collaborations par la simple raison que la discussion s'est réorientée sur d'autres sujets. Nous reconnaissons la pertinence de reproduire cette étude à l'aide

d'un devis de recherche strictement orientée vers les collaborations. Les résultats exploratoires obtenus dans ce mémoire peuvent servir de point de départ afin d'apporter une meilleure compréhension du chercheur et d'approfondir les connaissances.

La deuxième limite porte sur la composition de l'échantillon secondaire. Celui-ci fut construit dans le but d'homogénéiser le rôle des policiers en n'incluant que les participants occupant un titre d'enquêteurs. Toutefois, aucune distinction n'a été portée lors des analyses quant aux trois niveaux d'agences policières (locale, régionale/étatique ou nationale/fédérale. La répartition inégale des participants dans chacun des niveaux a empêché l'atteinte de validité interne entre les thématiques obtenues. Ainsi, nous avons observé les entretiens uniquement en nous basant sur le rôle professionnel des participants et non en fonction des caractéristiques de leur agence policière. Cela pose des limites quant à la généralisation de résultats. Par ailleurs, nous reconnaissons la pertinence de reproduire l'étude en considérant les niveaux de police afin de produire des recommandations pratiques adaptées à la réalité du milieu spécifique des enquêteurs. Ce mémoire ne peut qu'humblement proposer des recommandations générales à l'aide des résultats obtenus en complément des connaissances préexistantes sur la collaboration internationale.

Par ailleurs, l'échantillon de l'étude est uniquement composé de pays développés qui font partie de la Convention de Budapest et du Five Eyes Partnership. Il serait possible d'émettre l'hypothèse que les pays observés dans cette étude sont sujets à bénéficier d'une facilité supplémentaire à collaborer à l'internationale comparativement à d'autres pays qui ne sont pas membres de ses ententes légales et politiques. Nous soulignons la pertinence de reproduire cette étude à l'aide d'un échantillon composé de participants provenant de pays non développés.

En bref, bien que ce projet de recherche exploratoire possède des limites, il permet de guider les prochaines études sur le sujet des collaborations policières en contexte d'enquêtes sur des cas de crimes commis à l'aide du darkweb.

CHAPITRE 4: RÉSULTATS

Article 1: What Motivates Law Enforcement Officers to Collaborate: Experiences and Perceptions of International Cybercrime Investigators

L'article a été soumis tel quel à la revue *Public Administration Review* lors du dépôt de ce mémoire. Il est rédigé en conformité avec les exigences de la revue.[20][21]

[20] Villeneuve-Dubuc, M-P., Décary-Hétu, D. et Dupont, B. (2023). What Motivates Law Enforcement Officers to Collaborate: Experiences and Perceptions of International Cybercrime Investigators.

[21] Déclaration de l'étudiante : Je suis l'auteure principale de cet article. De ce fait, j'ai réalisé la codification des entrevues, les analyses et la rédaction de l'article. Après la rédaction du premier brouillon comprenant toutes les sections de l'article, David Décary-Hétu, professeur et directeur principal du mémoire, a apporté des commentaires afin d'améliorer l'article et assurer de la pertinence de celui-ci. J'ai par la suite effectué les corrections. David Décary-Hétu effectuera des relectures avant la soumission de l'article à la revue ainsi que du dépôt officiel du mémoire. Benoit Dupont, co-directeur du mémoire, a lu l'article afin d'ajouter conseils et suggestions étant un expert sur le sujet. Le cœur du travail de l'article et les corrections sont effectués par moi.

Abstract

This study identifies what motivates law enforcement investigators to collaborate on darkweb related cases. Due to a corpus of 20 interviews with investigators from five countries (Canada, United-States, United Kingdom, Australia, and Sweden), we used a thematic analysis to understand their motives to collaborate internationally. This research is based on participant's point-of-view to appreciate their realities and experiences. We found that investigators are motivated to collaborate police-to-police because this allows them to share helpful information, to increase investigation efficiency, to identify offenders as well as to identify victims, and to be able to arrest, put charges or prosecute delinquent people on the darkweb. Since not all law enforcement agencies collaborate, understanding investigator's motivations and willingness to do so enable us to model how future collaborations could likely be fostered based on empirical data, and help leaders in police organizations craft their messages to enhance collaboration.

Evidence for practice

- International collaborations empower investigators and are needed to work on darkweb related cases.
- Collaboration allows investigators to share helpful information, increase investigation efficiency, identify offenders, as well as victims, and arrest, put charges or prosecute delinquent people on the darkweb.
- Police-to-police collaborations help to overcome the main investigatory challenges associated with cybercrimes: the anonymity of suspects, the lack of legal power caused by jurisdictions, and the lack of training and human/financial resources.
- International collaborations contribute to de-anonymizing the darkweb and enable police investigations to move forward effectively.

Keywords: *Law Enforcement, Darkweb, Investigations, International Collaboration, Motivations, Policing, Cybercrime.*

Introduction

> "And I think if we had an international approach to dealing with that. It would make life easier for all nations across the world. It might alleviate some of that frustration that is experienced and sort of encourage and underpin the value of why we're sending this information to those international partners." (Interview 9, Australia).

Studies on police collaboration have yet to rigorously research how police agencies interact with each other in the specific context of cybercrime. As a result, several questions remain unanswered concerning the organization's effectiveness and context of the collaborations between investigators specializing in cybercrime and darkweb investigations. In light of this gap in extant research, this study examines international collaborations in darkweb police investigations by drawing upon the experiences of investigators themselves. The current literature implies that the police can choose how they collaborate (i.e., formally or informally), although there is a distinct lack of empirical data on the subject. However, it is well established that crimes involving technologies are international and are not restricted to the territories determined by police jurisdictions. Law enforcement agencies must therefore collaborate to tackle those crimes. Although, international collaborations between agencies seem random, subjective to each police agency, and difficult to accomplish in some cases. This article identifies investigators' motivations for collaborating with one another during police investigations into the darkweb. This research is positioned in the point of view of the investigators in order to understand why they wish to collaborate within the framework of their functions.

To achieve this, the paper first establishes the state of extant literature on international collaboration in the police context, then defines the problems associated with investigating crimes committed on the darkweb. Thereafter, the problem, research questions, and qualitative methodology are delineated. Finally, the results of the analyses are presented and discussed. The article concludes by elucidating investigators' motivations for collaboration, highlighting limitations of the study, and proposing avenues for future research.

Literature review

International collaboration in a policing context

The concepts of cooperation, coordination and collaboration are frequently used interchangeably in the security community (Whelan, 2017). Many studies have conceptualised the three C's (cooperation, coordination and collaboration) as a continuum (see Mandell, 2001; Bryson et al., 2006; Keast et al., 2007; Mattessich et al., 2001; Thomson and Perry 2006; McNamara, 2012; O'Leary and Vij, 2012; Whelan, 2017). This continuum depicts cooperation on one end, and collaboration on the other. This continuum is characterised by the strength of the ties. Specifically, cooperation is defined by sporadic ties between actors (Keast et al., 2007; Whitford et al., 2010), whereas coordination designates more durable and stable connections, such as, for example, when security agencies have an employee serve as a liaison officer with other agencies (Whelan, 2012; 2017) or when funds are jointly invested to achieve objectives (Warren et al., 1974; Mulford and Rogers, 1982; Cigler, 2001). Collaboration between security agencies is regarded as a high-level and high-intensity interaction (Cigler, 2001; Keast et al., 2004; Keast et al., 2007), one which is borne out of the desire to achieve common goals by working as a team (Agranoff, 2006). This conceptualization posits that stronger ties will lead to greater collaboration to carry out the necessary work and achieve common goals (Whelan, 2017).

In the context of literature on police organisations, collaboration and cooperation are routinely confused and used as synonyms, rather than being viewed as operating on a continuum. Given the web of multiple agreements, relationships and partnerships, the difference between the two terms would appear to be of little significance. That said, the most frequently cited definition in extant literature is from Scott and Boyd (2020), who define public interagency collaboration as a practice through which governmental administrative divisions ensure shared responsibility for achieving a common goal. The latter can refer to either the sharing of information or the development of plans and strategies to work together to both develop and find solutions. This rather general definition of collaboration between public agencies was initially refined by Dupont (2004), before then being taken up again by Dupont, Manning and Whelan (2017), who identified four main functional dimensions to collaboration within police organisations: 1) information exchange, 2) knowledge generation, 3) problem solving and 4) coordination (Dupont, 2004; Dupont et al., 2017). According to the literature, international collaborations between police agencies can take two forms. First,

formal collaboration refers to international cooperation involving organisations with a legal or governmental mandate to support collaboration by facilitating the sharing of information between police agencies and member countries (e.g., Europol and Interpol) (Gerspacher and Dupont, 2007). Second, informal collaboration refers to the exchange of information that takes place via an informal interaction between two or more police officers from different countries who have established a relationship of trust (Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016).

Sharing information between law enforcement agencies has been mainly studied at a national level (see Boba et *al.*, 2009; Taylor and Russell, 2012; Brewer, 2013; Cohen, 2018; Lambert, 2019; Pickering and Fox, 2022), but little is known about international collaboration. Even if multiple studies concluded that sharing information is essential for cross-jurisdictional crimes, various factors complicate intelligence sharing (Pickering and Fox, 2022). Foremost, it is acknowledged in the literature that police departments have shown resistance to changing their traditional ways in the past (Braga and Weisburd, 2007; Schaefer-Morabito, 2010), and the policing structures were not initially built for cross-jurisdiction crimes. By its nature, collaboration requires various departments to engage and share reciprocally. However, some agencies are less inclined to share data because of the nature of their departments, focusing only and singularly on one type of crime (Ratcliffe, 2007) as well as the competition between agencies for funding (i.e., in the United States). The fact that they keep intelligence to themselves causes what is known as "*information hoarding*" and is a barrier to collaboration (Pickering and Fox, 2022). As Sanders and Henderson (2013) exposed, some agencies prefer to receive information than give some to partners. Some scholars explain this behavior based on the reasons that some police officers believe that other agencies are not equipped to handle the information that they have collected (Taylor and Russell, 2012; Cohen, 2018; Lambert, 2019) and that the dispersion of information will make them less essential to the public eyes or even damage their reputation (Boba *et al.*, 2009). In addition, there is the technical difficulty of the newest data-gathering tools and the fact that there is no single way to collect data worldwide. To be able to transfer intelligence to another department, there is often a need to re-enter data, re-code, and find a secure place to store it (Sheptycki, 2004).

Offenses facilitated by the darkweb

The literature on international police collaboration primarily encompasses the period 1990 to 2010 and pertains to drug trafficking, organized crime and terrorism (Nadelmann, 1993; Aromaa and

Viljanen, 2005; Andreas and Nadelmann, 2008; Roberson et al., 2010; Lemieux, 2010; Mandel, 2011). More recently, there has been an emergent interest in other types of crimes, particularly those facilitated by the darkweb. The darkweb is a communication channel that ensures both the confidentiality and anonymity of its participants. Although there are several darkwebs, the best known is the Tor network, which was developed by the US Navy to communicate with its agents on missions abroad, in hostile countries (Mirea et al., 2019). To enhance the confidentiality of exchanges, the Tor network can be used by anyone, anywhere, both for legitimate and illegitimate purposes. Internet traffic from ordinary users makes it possible to better camouflage common military communications that take place via the Tor network. The Tor network operates on the model of peer-to-peer (P2P) networks and is therefore not centralized (Kaur and Randwara, 2020). This makes it almost impossible to shut down. By its very nature, the darkweb is a popular communication tool for offenders (Naseem et al., 2016; Mirea et al., 2019; Kaur and Randhawa, 2020). Moore and Rid (2016) observed that out of a total of 5,615 websites that were accessible only through the Tor network, 57% of these facilitated illegal activities, such as, for example, sale of drugs, illegal financial products or pornography involving either violence, children, or animals. These findings have subsequently been confirmed by other studies linking the darkweb with child pornography, fraud, hacking, cryptocurrency scamming (Mirea et al., 2019; Kaur and Randhawa, 2020) as well as drug trafficking (Van Hout and Bingham, 2013; Aldridge and Décary-Hétu, 2014; Tzanetakis et al., 2015; Soska and Christin, 2015; Barratt and Aldridge, 2016; Rhumorbarbe et al., 2016; Broséus et al., 2017; Tzanetakis, 2018), cigarettes (Munksgaard et al., 2021) and firearms trafficking (Holt and Lee, 2022). Other crimes such as human trafficking, revenge porn and the use of paid hitmen services (Kaur and Randhawa, 2020) are also accessible through the Tor network, albeit in smaller quantities.

Investigating the darkweb

The darkweb complicates police investigations for four main reasons (Dodge and Burruss, 2019). First, offenders can camouflage their activities and make their detection more difficult through the use of anonymizing technology (Naseem et al., 2016; Mirea et al., 2019; Kaur and Randhawa, 2020). It therefore becomes more difficult to identify one or more suspects, and to carry out investigations (Dodge and Burruss, 2019). For example, buyers and sellers of illicit drugs who contact each other via illicit markets accessible through the darkweb generally leave little or no

trace of their interactions, and only use computers which are in practice very difficult to retrace. Second, even if a suspect is identified, the ability of police to intervene is hindered by the different jurisdictions in which a crime has been committed (Dodge and Burruss, 2019; Cross, 2020). Dark web-facilitated crimes can originate in any country, and target a victim in any other country, by using resources in a third country. Given that criminal codes differ across jurisdictions (Wall, 2007a), manifold rules and procedures add significant additional complexity to both the identification and apprehension of offenders. Alternatively, the same act may be declared illegal in one country but be subject to a legal vacuum or declared legal in another (Brenner and Schwerha, 2004), which, in turn, hampers the success of police operations. It even has been demonstrated that broader the geographical dispersion of the crimes is, lower are the probability of the criminals to get caught (Lammers and Bernasco, 2013). Third, particularly in the case of darkweb facilitated crimes, a crime may have been committed months before a victim is even aware of it, which raises additional considerable difficulties (Dodge and Burruss, 2019). For example, in the case of internet identity theft, the time between the theft of identity data and the moment at which the victim realizes the harm can vary widely, ranging from only a few minutes to years even. Fourth, frontline police officers are unlikely to possess the expertise needed to collect, store, and process the chain of custody of digital evidence (Dodge and Burruss, 2019), given the complexity and constant evolution of technologies. Precisely, challenges for digital forensics (DF) departments are exposed in the literature (see Horsman, 2017; Casey, 2019; Wilson-Kovacs, 2021). Digital evidence needed for every case with a technological component, including darkweb related crimes, must be extracted, processed, and analyzed by the DF units to be used as intelligence for criminal investigations or proceedings (Casey, 2011). Even if more tools are available to DF teams, identifying suspects is becoming increasingly complex (Horsman, 2017).

Current study

In recent years, many offenders have used the darkweb to both facilitate their offences and increase their impunity (Moore and Rid, 2016) as a result of the anonymity it provides (Naseem et al., 2016; Mirea et al., 2019; Kaur and Randhawa, 2020). However, police agencies often find themselves unable to respond to cybercrimes due to a lack of resources or training (Brown, 2015; Harkin, Whelan and Chang, 2018; Faubert et al., 2021). Moreover, one of the chief concerns of cybercrime investigators is the lack of laws making certain new types of crimes unpunishable (De Paoli et al.,

2021). This results in some offenders either simply continuing with their activities without any repercussions or being charged for other misdemeanors that are unrelated to their offences, which often lead to minor sentences or acquittal (De Paoli et al., 2021). Although changing laws appears to be necessary, statutory laws take considerable time to change (Dodge and Burruss, 2019). This also applies to the management of digital evidence, insofar as the current procedural laws in some countries have not been adapted to open-source technologies or data collection (Koops, 2013). One of the proposed solutions for these problems is to promote international collaborations that transcend legal jurisdictions (Burns et al., 2004; Sarre et al., 2018). However, few studies have attempted to illustrate the relevance of collaborative strategic innovations in police intervention and cybercrime investigation (e.g., Dupont, 2017; Wang et al., 2020). Whelan (2017) conducted interviews with agencies in order to gain insight into their perceptions of collaboration driven by a performance agenda (Whelan, 2017). Although, these studies did not specifically address the cyber context nor the darkweb. Resultantly, there is scarce empirical evidence on the relevance of collaborative strategies in the context of technological crimes, despite its practical relevance (Dupont, 2017). Its empirical demonstration could thus make it possible to adopt a more sustainable approach (Dupont, 2017).

This study explores the experiences of police officers responsible for investigating crimes committed on the darkweb who carry out international collaborations as part of their employment. The general objective is to understand international collaborations in police investigations on the darkweb through the experiences of investigators. To this end, the study aims to identify and understand the motivations that drive investigators to collaborate internationally. Due to the fact that not all investigators collaborate, understanding their motivations for doing so will enable us to both model how future collaborations could likely be fostered and help leaders in police organizations craft their messages to enhance collaboration. Given that this is the first study to examine the subject, we attempt to understand international collaborations through the experiences of the actors who both participate in and benefit from them. Through this, we can better identify ways to maximize the impact of police collaborations.

Data and method

The data comes from interviews initially collected for a larger research project on the disruption of darkweb offenders' activities. As part of this project, 14 police investigators and 6 sergeant investigators were interviewed. The participants come from five countries: Canada (45%), Sweden (5%), the United Kingdom (25%), the United States (10%) and Australia (15%) (see Exhibit A). They were recruited using professional and personal contacts from the research team as well as through LinkedIn, a social network specializing in professional connections. Although, admittedly, using a convenience sample limits the generalization of our findings, given the limited number of investigators with experience in darkweb investigations, it would have been difficult to employ a different sampling strategy. The interviews took place between March 2020 and July 2021, both in person and via Zoom, and were then transcribed anonymously. Although some of the participants had the title of investigator sergeant, it should be noted that they carried out daily tasks similar to the other investigators interviewed. Both job titles themselves and the meaning of professional titles vary across policy levels as well as by country. With the exception of two participants who had retired or left law enforcement, they were all actively working at the time of the interviews (90%). The initial data collection was approved by the Research Ethics Committee – Society and Culture of University of Montreal (CERSC) (#CERSC-2019-111-D). This specific project was also approved by the CERSC (#CERSC-2022-109-D).[22]

We adopted a thematic analysis framework to identify the main themes in the interviews (Gavin, 2008). We began by carrying out an initial read-through of the transcriptions of the interviews and building a list of potential themes connected to our objective. We went through an iterative and inductive process to reread the transcriptions and select the final themes that would be coded in QDA Miner Software tool (Ritchie et al., 2003). A single author conducted the analysis. The themes were present in all of the interviews that we conducted. Overall, we identified five themes connected to motivations.

[22] The initial data collection was founded by PMI Impact.

Motivations driving investigators to collaborate

We identified five main motivations for collaborating internationally within the framework of police investigations: information sharing, investigation efficiency, offenders' identification, victim's identification, and arrestation/prosecution.

Information sharing

To respond to and investigate cybercrimes, which are often international in nature, police agencies benefit from *sharing information* with their colleagues in the same country, but also internationally. This is critical for maximizing the impact of criminal intelligence collection and, as such, this practice is encouraged – if not mandatory - in many organizations.

> "*It is encouraged at a national level for us all to share, so, yes. And the fact that cybercrime is international. There needs to be that sharing of information and that assistance*." (Interview 19, Regional Agency, United-Kindgom).

> "*We need to collaborate; we need to go police-to-police. […] In cybercrime, because it's my field that I see, we share information. We have no choice*." (Interview 2, Provincial Agency, Canada).

In these two excerpts, the participants emphasize the need to share information, framing it as being obligatory for successful investigations. Specifically, the passage from interview 2 illustrates this participant's perception of the exchange of information. From his perspective, it is not a choice to exchange information with colleagues; rather, they must do it in order to successfully complete their investigations. These extracts also underscore that this exchange of information takes place police-to-police at a national and international level. Although most of the participants perceived information sharing as accessible and effective, some countries appear to be less inclined to share information.

> "*…you're sending [requests] to 35 different countries, you're going to have to wait for the answers. So, we're sending to China to Hong Kong, to Panama, to the US, to Canada, you know, everywhere around the world, and some of those countries are responding quite fast and some are responding really*

> *slow. […] In one case, we had to wait over a year to get an answer for our legal request in that country.*" (Interview 14, National Agency, Sweden).

In the above excerpt, the investigator from Sweden discusses that in his experience, some police organizations respond quickly but that he had to wait a year before receiving an answer from another organization. His experience demonstrates that the response time to information sharing requests can differ significantly depending on the country.

> "*I think the only time we were ever really unsuccessful is where we located people who were in Russia or China, where we knew that we weren't going to get any cooperation from local law enforcement, and we really effectively had to give up. Yeah, which is always frustrating when you have quite good evidence about who's involved.*" (Interview 18, Regional Agency, United Kingdom).

Many interviewees stated that the lack of cooperation by certain countries influences the choice of investigations carried out by the police organization in order to ensure success in terms of arrest and cooperation. There appears to be a lack of consistency in the delay for information sharing amongst police agencies, which, in turn, means that some countries place little value on sharing information.

Thus, the interviewees believed that an international approach to cybercrime investigation would help to demonstrate the relevance of sharing information.

> "*And I think if we had an international approach to dealing with that it would make life easier for all nations across the world. It might alleviate some of the frustration that is experienced and sort of encourage and underline the value of why we're sending this information to those international partners*." (Interview 9, Federal Agency, Australia).

Here, participant #9 from Australia outlines how an international law enforcement response to cybercrime would encourage and demonstrate the value of information sharing, while, simultaneously, alleviating some of the frustrations caused by the lack of collaboration. Unfortunately, the participant did not elaborate on what was meant by an international approach. The sharing of information goes above and beyond criminal intelligence. Police agencies also need

to share technical information to support each other. This compensates for the lack of training of certain units responsible for investigating cybercrimes.

> "*On the one hand, but also, in cybercrime, there's really a lot of information sharing because it's a very specific field. You know when you're a policeman and you start looking at cybercrime, we're not computer technicians. We're not… uh… hackers. We're not… We need to help each other to learn, and also, we need to collaborate because it's all intertwined*." (Interview 2, Provincial Agency, Canada).

In this excerpt, participant #2 expresses how investigators tasked with solving complex technological crimes are not hackers or computer technicians. As such, they must share their knowledge in order to learn from the experiences of their peers.

Investigation efficiency

The second motivation is *efficiency*. Cybercrime investigations are long and complex, and collaborations can help speed up investigators' rate of discovery.

> "*We set up this [collaboration]… Because of the hindrance with law enforcement and the bureaucracy and the paperwork and production orders, it was all too slow to actually go after the money with a production order […]. It was way too slow, once you brought that intelligence, or actually, I should call it information, into law enforcement, we were bound by law enforcement rules and regulations and paperwork, and we needed to move faster than that. So, I looked, and I call it my goldfish bowl. So, if I had a goldfish bowl sat outside of law enforcement, that the banks could put their intelligence in*." (Interview 15, Multiple level agency, United Kingdom).

In this excerpt, it is possible to discern the intersection between the motivation to share information and the desire to save time to act quickly. These motivations are interrelated in certain instances, but they can also be independent of one another. Participant #15 from United-Kingdom shared an experience in which he and his team needed to act fast to trace the provenance of the money used in their investigation. The bureaucracy and production orders simply required too much time, so instead they worked with the financial institutions to use the information they shared. The

participant used the analogy of a goldfish bowl outside the police to refer to the way in which the bank shared information with them as part of their collaboration.

In this particular case, the investigators opted for an informal collaboration, which was cultivated through contacts and agreements, to cut through the official processes and requests in order to save time. Thus, it appears that informal collaborations are more likely to increase efficiency than formal collaborations (Lavers and Chu, 1997). Despite the existence of formal collaborative institutions, these institutions have received significant criticism regarding their methods and impact, chief amongst which is the slowness with which these organizations exchange information between different police agencies (Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016). In addition, formal communication institutions carry notable bureaucratic and political implications, requiring formal requests for information exchanges that are often limited due to jurisdictions preventing police officers from operating outside their legally appointed regions (Lavers and Chu, 1997; Den Boer, 2013). This leads some police officers to collaborate informally with their counterparts in another country to exchange information. Even if little is known in the literature about effective investigation according to a literature review from Prince *et al*. (2021), this except exposes the willingness of our participants to gather effective investigation.

With respect to investigations of cybercrimes involving child abuse, the notion of time and efficiency is considerably more important. Informal collaborations are seen as more spontaneous partnerships that enable effective and efficient collaborations in a context in which every minute, day or week spent on an unresolved case means that the child victim may be suffering serious abuse.

> "*It's from a partnership perspective. Definitely. It's really integral. To be able to collaborate effectively and efficiently because we're talking about minutes, hours, days, weeks longer. That is a particular child victim might be suffering or being injured or abuse*." (Interview 9, Federal Agency, Australia).

Offender's identification

The third motivation for collaboration observed in the interviews is the *identification of suspects*. The results suggest that the sharing of informal information can be crucial to the identification of suspects (Raustiala, 2002; Slaughter, 2004). As aforementioned, the darkweb raises additional

challenges for investigations, specifically with respect to identifying suspects. Consequently, collaboration, primarily in the form of sharing intelligence, becomes a crucial way of identifying suspects via the accumulation of evidence. In the specific case of cybercrimes involving the use of cryptocurrencies, the identification of suspects becomes considerably more difficult due to the pseudo-anonymity of users.

> "*It's really difficult to deconflict or engage… We have global law enforcement partners to establish what it is they are working on and then cross-jurisdiction coordination as I said is protracted… Umm… Especially when it comes to servers or the use of cryptocurrencies, mixed services significantly complicate our investigations, especially if it is a customer wallet or an output as an exchange outside the [country]*." (Interview 12, Multiple level agency, United Kingdom).

Here, participant #2 expresses that cryptocurrencies and mixed services makes their investigations more complex and that they have used international collaborators in the past to obtain information or even to achieve cross-jurisdiction coordination, which involves transferring the file to a police unit that has the legal powers to pursue the investigation if the suspect or the wallet comes from another country.

Victims' identification

Police investigators also explained that above and beyond arresting offenders, they have a *desire to identify and support victims*. In the case of sexual offences especially, identifying victims – when suspects remained unknown – could stop the victimization from going on. The participants suggested that the identification of victims, when they are unknown, constitutes a tremendous motivation for collaboration in order to respond to the mandate of the police to ensure the safety of the population.

> "*It all comes back to victim and victim, victim reduction and harm reduction, in my opinion. So, I mean, I know I spoke about kind of, like, charging and prosecution always being the end goal. I mean, in law enforcement, our goal,*

> *our overarching goal is public safety*." (Interview 13, Municipal Agency, Canada).

In the above excerpt, participant #13 expresses that the ultimate objective of his work is public protection. He also notes that everything law enforcement does, according to him, refers back to the victims, specifically their protection. Thus, the identification of victims makes it possible to ensure their protection. In the following excerpt, participant #17 stresses that investigators go to the victims as well as the suspects, sharing their own experiences of when they had to request physical assistance in another country in order to complete their mandate. In this specific case, it is possible to acknowledge that law enforcement collaboration represents a wide range of actions that change depending on the underlying motive.

> "*You go with where the victims are and suspects are. And, you know, in order to conduct the operation, yes, they did need presence in there [other country] as well*." (Interview 17, Federal Agency, United Kingdom).

Arrest and prosecute

The fifth motivation for collaboration is the *desire to arrest, charge or prosecute* identified suspects on the darkweb. This is often done through transferring a case, with all the information and intelligence compiled, to another police organization that has both a responsibility to take action and the legal power to do so. This is mainly justified by the limits of jurisdictions, which serve to constrain the powers of police agencies to their own country. Here, collaboration becomes a method of securing legal action, physical arrests, or criminal sentences like fines against cybercriminals.

> "*If we want to arrest someone like a drug dealer on the darkweb, we will have done our part… Recover the evidence, identify the suspect, and the file will be transferred to another agency for arrest*." (Interview 1, Provincial Agency, Canada).

In our interview, participant #1 expressed that from his experience, cases of crimes committed on the darkweb are transferred to another agency that has the capacity to arrest the suspect(s). Thus, this is done after they have collected the evidence and identified the suspect.

> "*Like I said earlier on, like… you can't just catch these guys without… international collaboration [...]. Yeah, and then people can go hundred years without, like in another country in Russia, without any fear of being caught*." (Interview 8, Federal Agency, Australia).

This excerpt from the Australian investigator (Interview #8) testifies to the need for international collaboration in order to identify suspects and possibly intercept them. From their perspective, some countries that are more resistant to collaboration, such as Russia, do not benefit from this service, and, in turn, help criminals to flee the justice system.

Discussion and conclusion

Overall, this study demonstrates that investigators want to collaborate for multiple reasons which aims to empower investigators in their investigations on the dark web. Indeed, according to the experiences of the investigators we interviewed, international collaborations make it possible to effectively share information, make investigations more efficient, help to identify suspects and victims, and ensure the continuation of criminal investigations that lead to arrests in multiple jurisdictions. Simply put, then, collaborations empower police investigators. Collaborations also help to overcome the main investigatory challenges associated with the darkweb: the anonymity of suspects, the geographically assigned jurisdictions, the time it takes to detect offences and the lack of police training (Dodge and Burruss, 2019). Indeed, our results suggest that three of the motivations for collaboration, namely the sharing of information, the identification of suspects and the identification of victims contribute to the de-anonymization of the darkweb and enable police investigations to move forward. Moreover, the sharing of information makes it possible to counter the limitations imposed by jurisdictions, by exchanging information or even by transferring the file to a police agency that has the legal capacity to undertake legal proceedings against one or more identified suspects. Further, police collaborations are particularly expedient for acting quickly and countering the delays imposed by the occasionally slow detection of victimization. Finally, collaborations help to compensate for the lack of training police officers receive, by allowing exchange of advice or even tools.

It is possible to observe that the motivations for collaboration expressed by our participants closely correspond to one of Dupont et al.'s (2017) collaborative dimensions, namely the exchange of information. The other two motivations could be correlated with other dimensions; for example, the identification of suspects could potentially represent the generation of knowledge. The motivation to save time and speed up investigations could correspond with problem solving, considering that the slowness of formal institutions has been extensively documented in extant literature (see Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016). Consequently, more details concerning those dimensions are required in order to ensure with certainty that our results are consistent.

Moreover, the results of the study illustrate that collaborations can take different forms depending on their underlying motive. Between police organizations, they can be formal, thus referring to the use of inter-agency communication procedures or via an official collaborative body. They can also be informal and, as such, be characterized by the exchange of information or mutual assistance between contacts accumulated through networking (Kreiner and Schultz, 1993; Lavers and Chu, 1997; White, 2011; Inyang and Abraham, 2013; Kim et al., 2013). This latter form of collaboration is often faster and does not require procedures, which explains why it is often employed during urgent requests or investigations involving the abuse of children according to the testimonies in this study. Indeed, the most important criticism of official organizations pertains to the slowness with which these organizations exchange information between different police agencies (Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016). Moreover, formal communication institutions create cumbersome bureaucratic steps that require formal requests for information exchange (Lavers and Chu, 1997; Den Boer, 2013). These constraints lead some police officers to collaborate informally with others in order to exchange information. As noted by both Raustiala (2002) and Slaughter (2004), the informal sharing of information can prove crucial to the progress of police investigations and significantly impact upon the identification of suspects.

However, the results of the study suggest that collaborations, whether formal or informal, are generally effective and that police organizations around the world are open to collaboration, with the exception of certain countries, such as, for example, Russia or China. Indeed, following Scott and Boyd’s (2020) definition of public interagency collaboration, sharing information informally thus becomes crucial in the advancement of police interventions and has a significant impact on

the identification of suspects (Raustiala, 2002; Slaughter, 2004). Nevertheless, although our results suggest that collaboration represents one of the main ways to combat this issue, important limits to international collaborations must be addressed. Indeed, although international collaborations between police agencies transcend jurisdictions, the latter remain strongly influenced by national policies (Deflem, 2004). Police agencies both respond to the concerns of their political leaders and direct their actions in accordance with the political climate. This directly restricts the freedom of police agencies to collaborate internationally (Deflem, 2002), as demonstrated in this study with respect to the lack of collaboration with Russia and China. Also, the lack of collaboration from some agencies can transform onto conflictual relationships (Crawford, 1997), precisely when agencies are inconsistent or withhold information from others (Sedgwick and Hawdon, 2019).

Nonetheless, this study has limitations pertaining to its sampling and scope. The verbatims used in the research did not focus entirely on the collaboration, as the initial interviews were oriented towards the types of police interventions or investigations carried out on the darkweb. During the interviews, the participants discussed whether or not they engaged in collaborations in their activities and how these took place. Future studies could thus reproduce this methodology by emphasizing the role of international collaborations in addition to expanding the sample size to allow for a greater representation of countries. A further limitation is that although we used the broader definition of public interagency collaboration as the practice through which governmental administrative divisions ensure shared responsibility for achieving a common goal (Scott and Boyd, 2020), which in our study mainly concerns information sharing in order to investigate cybercrimes. Future studies could analyze the types of collaboration along a continuum between cooperation, coordination and collaboration (see Mandell, 2001, Bryson et al., 2006 ; Keast et al., 2007; Mattessich et al., 2001; Thomson and Perry 2006; McNamara, 2012; O'Leary and Vij, 2012; Whelan, 2017). Doing so would enable researchers to delve more deeply into the nature of the different actions involved in collaboration. Finally, our data does not allow us to classify acts of collaboration due to a lack of details, and thus future studies should encourage participants to provide more element into their interactions in order to better differentiate the relationships between the agencies with respect to the different types of collaboration on the continuum.

Article 2: How Law Enforcement Investigators Collaborate Within and Beyond their Jurisdictions on Darkweb-Related Crimes

L'article a été soumis tel quel à la revue *Police Practice and Research* lors du dépôt de ce mémoire. Il est rédigé en conformité avec les exigences de la revue.[23][24]

[23] Villeneuve-Dubuc, M-P., Décary-Hétu, D., Dupont, B. (2023). How Lar Enforcement Investigators Collaborate Within and Without their Jurisdictions on Darkweb-Related Crimes.

[24] Déclaration de l'étudiante: Je suis l'auteure principale de cet article. Tout comme le premier article, j'ai réalisé la codification des entrevues, les analyses et la rédaction de l'article. Après la rédaction du premier brouillon, dans lequel j'ai écrit chacune des sections de l'article, David Décary-Hétu, apportera des commentaires afin d'améliorer l'article et assurer de la pertinence de celui-ci. Une fois les corrections effectuées et l'article prêt à soumettre, celui-ci sera envoyé à Benoit Dupont, co-directeur du mémoire, afin d'obtenir ses commentaires et son opinion sur la justesse de l'article considérant son expertise sur le sujet. Une fois les modifications complétées par moi, l'article sera soumis à la revue conjointement au dépôt officiel du mémoire. Ainsi, tout comme le premier article, le cœur du travail de l'article et les corrections sont effectués par moi.

Abstract

Investigating crimes committed with anonymising technologies, such as the darkweb, is a massive problem for law enforcement. These communication technologies make it challenging to identify suspects or victims online. In addition, crimes committed remotely transgress legal jurisdictions and force policing agencies to collaborate. However, little is known about law enforcement collaboration on cybercrimes, and even less knowledge is available about crimes committed with the darkweb. Studies on law enforcement international collaboration have used empirical data from drug trafficking, terrorism, or organised crime. Thus, this study explores the experience of police officers responsible for investigating crimes committed on the darkweb who carry out international collaborations as part of their employment. This research aims to describe and understand the types of collaboration the investigators in this study have experienced. Through this, we can better identify opportunities to maximise the impact of police collaborations with empirical data from interviews with 20 investigators from five countries (Canada, United States, Australia, United Kingdom, and Sweden). Our results expose that our participants primarily use three types of collaboration: (1) formal, (2) informal, and (3) private. Darkweb-related investigations equally depend on the three types of collaboration to obtain digital evidence and intelligence.

Keywords: Policing, Formal Collaboration, Informal Collaboration, Public and Private Partnership, International Investigations, Darkweb.

"…international collaboration between police authorities is key for combatting crime on the Dark Web" (Europol, 2023, May 2).

Introduction

Numerous networks of international liaison officers (ILO) have been developed in order to assist national police agencies in achieving their responsibilities in line with international treaties (Lemieux, 2015). Specifically in the United States, the FBI and the DEA have developed networks (Lemieux, 2018) that facilitate information exchange, investigation, arrests, training and more (Nadelmann, 1993; Bigo, 2000; Den Boer and Block, 2013). To date, studies on police collaboration are not adapted to the specific context of computer crimes. Several questions remain unknown as to how investigators in specialised cybercrime units, particularly those committed using the Darkweb, collaborate and how exactly these collaborations use them. This study, therefore, examines international collaborations in darkweb police investigations through the experiences of investigators. Specifically, it is by illustrating empirical proof of the types of collaboration used by investigators from different countries that we can provide a better understanding of those collaborations. To do this, this article establishes the state of the literature surrounding international collaboration in a police context in addition to defining the problems of investigation that engender crimes committed on the darkweb. Thereafter, the problem under study, the research questions and the qualitative methodology are detailed. Finally, the results are presented and discussed. The article concludes on the limits and future avenues of this research.

Literature review

Collaboration, cooperation, and coordination

The concepts of cooperation, coordination and collaboration are frequently used interchangeably in the security community (Whelan, 2017). Many studies have conceptualised the three C's (cooperation, coordination and collaboration) as a continuum (see Mandell, 2001; Bryson et al., 2006; Keast et al., 2007; Mattessich et al., 2001; Thomson and Perry 2006; McNamara, 2012; O'Leary and Vij, 2012; Whelan, 2017). This continuum depicts cooperation on one end, and collaboration on the other. This continuum is characterised by the strength of the ties. Specifically, cooperation is defined by sporadic ties between actors (Keast et al., 2007; Whitford et al., 2010),

whereas coordination designates more durable and stable connections, such as, for example, when security agencies have an employee serve as a liaison officer with other agencies (Whelan, 2012; 2017) or when funds are jointly invested to achieve objectives (Warren et al., 1974; Mulford and Rogers, 1982; Cigler, 2001). Collaboration between security agencies is regarded as a high-level and high-intensity interaction (Cigler, 2001; Keast et al., 2004; Keast et al., 2007), one which is borne out of the desire to achieve common goals by working as a team (Agranoff, 2006). This conceptualisation posits that stronger ties will lead to greater collaboration to carry out the necessary work and achieve common goals (Whelan, 2017).

In the context of literature on police organisations, collaboration and cooperation are routinely confused and used as synonyms rather than being viewed as operating on a continuum. Given the web of multiple agreements, relationships and partnerships, the difference between the two terms would appear to be of little significance. That said, the most frequently cited definition in the extant literature is that put forward by Scott and Boyd (2020), who define public interagency collaboration as a practice through which governmental administrative divisions ensure shared responsibility for achieving a common goal. The latter can refer to either the sharing of information or the development of plans and strategies to work together to both develop and find solutions. This rather general definition of collaboration between public agencies was initially refined by Dupont (2004) before then being taken up again by Whelan and Dupont (2017), who identified four main functional dimensions to collaboration within police organisations: 1) information exchange, 2) knowledge generation, 3) problem-solving and 4) coordination (Dupont, 2004; Dupont et al., 2017).

Formal police collaboration

The rise in international crimes in the early 1900s demonstrated the pressing need to establish a system of governance that transcends geographical and legislative boundaries in order to counteract the power of offenders who took advantage of globalisation and new technologies to spread their networks and offend all over the world (Gerspacher and Dupont, 2007). To meet this growing need, two police organisations with the principal task of facilitating international collaboration were founded: Interpol and Europol. Interpol was created by national police agencies that were encountering issues with collaborating (Gaspacher and Dupont, 2007). It was the creation

of the Federal Bureau of Investigation (FBI) in 1938 and the events of the two World Wars that led police organisations to put pressure on governments and ask for support to build up the organisation (Deflem, 2016). Interpol developed across the course of the twentieth century as an intergovernmental organisation whose aim was to promote international police cooperation, primarily by facilitating communications between member police agencies in order to avoid formal requests and inter-agency legal constraints (Deflem, 2016; Gerspacher and Dupont, 2007). Interpol does not have the power to arrest or investigate but rather functions as both a communications service between member police agencies (Deflem, 2016) and a training service (Interpol, 2022). To date, Interpol has brought together 195 member countries that have access to criminal databases, a secure communications system, working groups comprising experts and police officers as well as conferences to share knowledge (Interpol, 2022). Europol is the European criminal police agency. It was established in 1992 by the Treaty of the European Union (Deflem, 2006) in the wake of political commitments in Europe aimed towards encouraging greater collaboration in the fight against transnational crime (Gerspacher and Dupont, 2007). Europol's principal role is to help police agencies inside Europe combat international crimes, mainly organised crime and terrorism, in addition to supporting law enforcement operations on the ground by offering a platform for information on criminal activities and providing police with expertise from many analysts (European Union, 2022). In 2013, Europol created the European Cybercrime Center (EC3) which led to the creation of the J-CAT operational unit in 2014 (Europol, 2022; Europol, 2023). This taskforce facilitate collaboration between its member for tackling cybercrimes internationaly. Per exemple, the operation SpecTor led by EC3 and J-Cat, brought together 9 countries to arrests 288 sellers and buyers on the darkweb (Europol, 2023, May 2st). Despite their differences, these two organisations share the common goal of fighting international crime as well as having similar structures, missions, and purposes (Gerspacher and Dupont, 2007). Indeed, these two formal agencies are mainly responsible for facilitating communications between police agencies or member countries as well as providing advisory services in the fight against international crimes.

Collaboration is far from a simple process, and two factors in particular can hinder its actualisation within the police and international context. First, although international collaborations between police agencies transcend jurisdictions, the latter nevertheless remain strongly influenced by national policies (Deflem, 2002). Hence, police agencies both respond to the concerns of their

political leaders and direct their actions in accordance with the political climate. This directly impinges upon the freedom of police agencies to collaborate internationally (Deflem, 2002) as well as the way in which these collaborations ultimately take shape (Lemieux, 2018). Second, although collaborations aim to reduce both competition between police agencies (Lemieux, 2010) and duplicate investigations being conducted (Wang et al., 2020), these goals are rarely achieved in practice (Lemieux, 2018). Indeed, some countries such as Canada, Australia, the United Kingdom, and the United States are made up of states, provinces, and cities that each have their own police department (Lemieux, 2018). The United States, for example, has more than 18,000 state and local police agencies that one would have to navigate to establish international collaboration (Banks et al., 2016). Other countries like Ireland and France have only one or two levels of police, which facilitates the establishment of collaborative links (Lemieux, 2018). Bureaucratic systems thus make communication slower and more difficult (Lemieux, 2018).

There are also forces operating at the local and national level that serve to constrain collaboration between police agencies. First, some police agencies are resistant to collaboration because of the strong competition between them, due to the fact that states reward law enforcement agencies based on their investigation resolution rates and overall productivity (Lemieux, 2018). The more police forces operating in a given country, the more they must fight for financial resources. This, in turn, makes them less inclined to collaborate. Second, the low level of communication even within the borders of a country leads several police agencies to investigate the same crime (Wang et al., 2020). For example, federal law enforcement agencies such as the FBI, the Drug Enforcement Agency (DEA), and investigators from local agencies frequently find out that they are investigating the same drug dealers, thanks to informal collaborations between these agencies (Chaiken et al., 1990). Given the limited police capacity to respond to the increase in cybercrime cases, the duplication of investigations represents a significant waste of police resources.

Informal police collaboration

Despite the good intentions and objectives of formal collaborative institutions, they have received criticism concerning their choice of methods and limited impact. Indeed, the most important of these criticisms pertains to the slowness with which these organisations exchange information between the different police agencies (Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016).

Moreover, formal communication institutions create cumbersome bureaucracies that require formal requests for information exchange (Lavers and Chu, 1997; Den Boer, 2013). These constraints, in turn, lead some police officers to collaborate informally with one another to exchange information. The sharing of informal information can be critical for advancing police investigations, particularly with respect to the identification of suspects (Raustiala, 2002; Slaughter, 2004). According to Den Boer (2013), informal collaborations take place more between organisations at the same levels and with similar legislative powers, which is called horizontal collaboration. Formal collaboration is described more as a form of vertical police collaboration, which involves regional police organisations appealing to institutions deemed hierarchically superior to them (Den Boer, 2013). The advantages of informal collaboration primarily pertain to its flexibility as well as its rapid implementation (Lavers and Chu, 1997). The adoption of informal collaboration is therefore done without prior permission from an authority, and, as such, pierces the bureaucratic barriers specific to each police agency (Lavers and Chu, 1997).

Informal collaboration does more than ensure the success of police investigations, however. The creation of informal collaborative ties is also part of police culture (Ross, 2010; Deflem, 2016 in Bayer, 2010). Indeed, police culture values the accumulation of trusting relationships with counterparts in other countries (Ross, 2010). This manifests in the informal exchange of relevant information that helps to advance police investigations (Ross, 2010). According to Bayer (2010), police officers value their professional autonomy and independence from decision-making centres. Informal collaborative relationships are thus cultivated by networking between police officers (Lavers and Chu, 1997; Ross, 2010; Deflem, 2016). Although undoubtedly important, informal collaboration is not without its limitation or difficulties. Informal collaboration has no legal status, which may impact upon both its legitimacy and practical involvement in police investigations in certain cases (Lavers and Chu, 1997). Finally, many factors can influence the establishment of collaborative ties, such as language and geography (Tremblay, 2009). This restricts the pool of potential links that can be created.

Public and private collaboration

According to many researchers (Hinduja, 2007; Wexler, 2014; Vincze, 2016; Dodge and Burruss, 2019), there is a significant need to improve our knowledge of the complex relationships between law enforcement and the private sector. Private institutions are described as infrastructures in

which decisions are made within a business model based on the customer's experience, the interests of shareholders and managers, and, mostly, on profit (Carr, 2016). As listed in Pomerleau's (2019) manuscript, many initiatives to improve collaboration between the public and private sectors have been founded worldwide in recent years. However, despite the advent of Public-Private Partnerships (PPPs) initiatives, access to data representing digital evidence for investigations remains highly complex. Indeed, it is not easy to legally obtain judicial evidence without compromising the digital privacy of citizens and customers (Tun et al., 2016; Vincze, 2016).

Moreover, PPPs comprise complex interactions between parties with distinct objectives (Dodge and Burruss, 2019). In this sense, the police aim to protect society by maintaining public order (Lemieux, 2018), and ICT companies aim for profit capitalisation (Carr, 2016). This disparity raises doubts about everyone's intentions and undermines the fundamental trust needed to collaborate (Dodge & Burrus, 2019).

International collaboration in the context of cybercrime

Police agencies often find themselves unable to intervene due to a lack of resources and training on crimes involving technologies (Brown, 2015; Harkin et al., 2018; Faubert et al., 2021). One of the proposed solutions for this problem is to foster international collaborations that transcend jurisdictions (Burns et al., 2004; Sarre et al., 2018; Wang et al., 2020). To date, only two studies have focused on international collaboration in police responses to cybercrime (Dupont, 2017; Wang et al., 2020). However, no study has yet focused on police collaboration in the context of crimes committed on the darkweb. The study by Wang et al. (2020) examined the high-profile hacking case of *First Commercial Bank* (FCB), a renowned financial institution in Taiwan. In 2016, a group of malicious individuals programmed ATMs in different places on the island to withdraw all the money they contained, which amounted to a total of 2.6 million US dollars. This same group of individuals had previously committed more than a hundred similar ATM hacks on more than a dozen financial institutions across Europe. Researchers collected interviews from police officers involved in the ensuing investigation. The results demonstrated that collaboration between Taiwanese national law enforcement agencies, some U.S. federal agencies, and the many local agencies on the island ultimately helped to identify the suspects and bring the hackers to justice (Wang et al., 2020). Moreover, this study also demonstrates the practical relevance of international collaboration in general, but also of collaboration between national police agencies

and local police agencies that have less resources and knowledge to intervene in this type of transnational crime. In Dupont's (2017) study of police regulation of Botnets, three approaches to crime regulation and control were described to illustrate their respective challenges and efficiencies: first, the incarceration of hackers by law enforcement agencies to produce a deterrent effect; second, the disruption of botnet networks by the private company Microsoft; and finally, harm reduction using an agreement initiative between public and private organisations in five countries. The results of the study demonstrate that the traditional model of local law enforcement employed by police agencies is inadequate for dealing with international issues. Rather, it is more the innovative strategies carried out by a combination of private actors in collaboration with different police agencies that have generated encouraging results. However, Dupont (2017) specified that evaluations of the effectiveness and acceptability of these strategies is not described in extant literature. There is scarce empirical evidence on the relevance of police regulation intervention strategies that include collaborations in the context of technological crimes, despite its practical relevance (Dupont, 2017).

In recent years, some authors have proposed developing an international police agency strictly dedicated to the investigation of cybercrimes in order to address this need for collaboration (Moore, 2015). However, considering the wide variety of laws, charters, and penal systems across the globe, there remains no international police agency singularly dedicated to combatting cybercrimes. Consequently, multiple law enforcement agencies around the world must collaborate with each other in order to circumvent the limitations imposed by jurisdictions, traditional policing, and the anonymous characteristics of cybercrimes in general. Despite the relative dearth of studies on this issue, some resources have been made available by formal collaborative institutions to both facilitate the exchange of information on cybercrimes and help further progress investigations (Pickering and Fox, 2022). For example, Interpol in recent years developed a coordination centre for technological crimes (*Cyber Fusion Center*) in order to both bring together experts in technological crimes and help member organisations make progress in their investigations (Interpol, 2017). In addition, Interpol has developed private partnerships in order to be at the cutting edge of technology and provide training to police officers who request it (Interpol, 2017). Recently, Interpol started offering a forensic computer laboratory, designed to help the detection of evidence amongst frontline officers (Interpol, 2017). These resources serve a great need from many police organisations. In addition, an international initiative was founded in the early 2000s

to facilitate international information sharing. This formal agreement, known as the Budapest Convention, facilitates the sharing of information on cybercrimes, whether for the detection, investigation, or prosecution of cybercriminals (Calderoni, 2010; Pool and Custers, 2017) within the 65 member countries from Europe, Asia, the Americas, and the Pacific (New Zealand Government, 2020). These formal international collaborative initiatives share the common goal of assisting law enforcement agencies in the fight against cybercrime. Nevertheless, according to studies by Dupont (2017) and Wang et al. (2020), informal collaborations appear to be prioritised more in order to either complete investigations or have a real impact upon the regulation of cybercrimes.

Policing challenges while investigating on the darkweb

In short, police agencies often encounter significant challenges in their investigations involving crimes facilitated by the darkweb. Lack of resources and training are perhaps the two most significant issues in this respect (Brown, 2015; Harkin et al., 2018; Faubert et al., 2021). Indeed, the growing number of cybercrimes exceeds the response capabilities of law enforcement agencies, leaving a significant number of offences and offenders to simply fly under the radar. Law enforcement agencies need to prioritise certain types of offences because they simply cannot handle them all. Cybercrimes often bear the brunt of this offloading (Leukfeldt et al., 2013; Boes and Leukfeldt, 2017), for two main reasons (Faubert et al., 2021). First, police officers often lack knowledge, training and experience with technologies and new criminal methods, which, in turn, leads them to postpone taking over the investigation of these crimes (Calderoni, 2010; Leukfeldt et al., 2013; Boes and Leukfeldt, 2017; Dolliver, 2019). Numerous studies have demonstrated that police officers do not feel sufficiently prepared to deal with crimes involving technologies and that the training they receive is too brief and superficial (Bossler and Holt, 2013; Burns et al., 2004; Hadlington et al., 2018; Harkin et al., 2018; Burruss et al., 2019). Second, cybercrimes continue to be viewed as high-volume crimes, based on both their frequency and the number of recorded cases, which have little impact on society, according to the severity scale of the police (Wall, 2007b; Dupont, 2017). This leads police organisations to not focus their resources on cybercrime interventions and investigations, particularly when these are not the chief concerns of politicians in their country. Indeed, although some police agencies have invested in expertise and technology, the fact is that their resources are still deployed more in serious cases or those that threaten the

integrity of children, rather than being dedicated to the numerous appeals of cases of fraud or stolen credit cards, for example (Dodge and Burruss, 2019).

Study aim

This study explores the experience of police officers responsible for investigating crimes committed on the darkweb who carry out international collaborations as part of their employment. The objective of this research is to describe and understand the types of collaboration the investigators in this study has experienced. We seek here to understand if investigators use formal and/or informal collaborations, and the shape that these collaborations take in practice. Through this, we can better identify opportunities to maximise the impact of police collaborations.

Methodology

Data used in this paper come from interviews with police officers who were initially part of a larger project on darkweb offenders law enforcement disruptions strategies. That project was funded by PMI Impact. As part of this project, 14 investigators and 6 chef investigators were interviewed. Participants (n=20) came from five countries: Canada (45%), Sweden (5%), the United Kingdom (25%), the United States (10%), and Australia (15%) (see Table 1, Appendix A). They were recruited via the research team's professional and personal contacts and LinkedIn. While admittedly using a convenience sample limits the generalizability of our results, given the limited number of interviewers experienced in darkweb surveys, it would have been difficult to employ a different sampling strategy. Interviews took place between March 2020 and July 2021, both in person and via Zoom, and were then transcribed anonymously. Although some of the participants held the title of investigative sergeant, it should be noted that they performed similar day-to-day duties as the other investigators interviewed. In addition, the job titles and the meaning of professional titles varied between political levels and countries. The sample was 30% female and 70% male. More than half of the participants had a university degree (70%) and an average of 20 years of policing experience. The vast majority were actively working at the time of the interviews (90%), except for two who had either retired or left law enforcement. The project was initially approved by the Research Ethics Committee – Society and Culture of the University of

Montreal (CERSC) (#CERSC-2019-111-D), and the use of secondary data was also authorised by CERSC (#CERSC-2022-109-D).

The interviews were coded using the QDA Miner software tool. We adopted a thematic analysis framework to identify significant themes in the interviews (Gavin, 2008). We began by reviewing the interview transcripts and building a list of potential themes related to our purpose. Then, we went through an iterative and inductive process to reread the transcripts and select the final themes coded in QDA Miner (Ritchie et al., 2003). Only one author conducted the analysis. As a result, themes were present in all interviews we analysed.

Results

We identified three types of collaborations accomplished and experienced by our participants. The following sections present the content of these themes.

Formal collaborations

Formal collaboration involves an explicit, established and rigid process structuring agreements for collaboration between police agencies. These formal collaborations also include official international collaboration agencies such as Europol or Interpol. In our sample, the investigators did collaborate a lot internationally, by having official partnerships or agreement between agencies. Also, many shares that they used on a frequent basis the assistance of Interpol in order to accomplish international collaboration with agencies they did not already have a formal direct agreement with.

Formal collaboration can be formed at various level of police agencies and can be both within their jurisdictions and country as well as outside their legal barriers and internationally. In this except below, investigator #16 from a local law enforcement agency mentions that even if they had federal partners, he shares that he did collaborate with the sheriff from the city were the suspect they were looking for lived in order for them to provide assistance. He also adds that, according to him, partnerships make most investigations successful.

> "*We did have federal partners. The suspect lived up in the center of the state, in a different city, and so then, we partnered with the sheriff's office from that jurisdiction*

as well to assist so… It was a lot of partnerships which… is how most successful investigations have to work." (Interview 16, Municipal agency, United States).

Formal collaboration can also be initiate from the needs to accomplish a dual investigation, meaning that both agencies are interested in the same things, since they both want to find a suspect so they can put charges on the crimes that was committed in both jurisdictions and caused harms to victims located in more than one place.

In the following passage, the investigator from Canada shares his experiences with dual investigation explaining in what context they occur. He also mentions that when they share intelligence, they need an affidavit in order to get sworn written evidence that can be accepted to court.

"*And the other thing is, do you have a corresponding investigation? Are you investigating a crime, here right? On that person. So, it can lead into an investigation, but then it would be our investigation and then that source. And absolutely, if they [the FBI] source that information, say, yes, we can provide an affidavit, a statement saying this is what we did, and this is how we got the information right and provided it to us. That would be part of it. But it's usually sometimes a dual… it usually happens to be a dual investigation because they're interested because in an offense there. But the person's here and they're also conducting offenses here in Canada. The victims may be in Canada, the victims may be in the States, most likely both places*." (Interview 20, Provincial agency, Canada).

Thus, collaborations are often justified by the presence of victims or suspects in another jurisdiction. Moreover, collaborations seem to be facilitated when both police agencies have an interest in the investigation. Investigators are therefore led to collaborate internationally, as is the case between Canada and the United States in this case shared by participant #9. According to our investigators, official partnerships seem not to be limited by the police level. Regional agencies collaborate with national agencies. Although collaboration between different level of agencies is possible, it seems that official process implies smaller law enforcement agencies to contact federal agencies prior to regional or local levels. Also, as mentioned in the following except, every agency has they own process in order to collaborate and share information.

"*There are certain protocols that you have to adhere to. It's like from a state agency trying to communicate to another International Agency. Generally speaking, all of our communication should go through our federal partners and*

> *trying with federal police and then obviously they have their due process as well."* (Interview 9, Federal agency, Australia).

Informal collaborations

The second type identified is *informal collaborations*. This specific type does not involve any formal process. Many participants mentioned that they used both formal and informal collaborations through their investigations. Although, informal collaboration was often discussed and presented as being more efficient and an adequate tool to meet the needs of cybercrime and particularly darkweb related investigations.

> "It's *more at an informal level. I made contacts that I've made through my research on the darknet. I've just put people that are my points of contact. So, it's nothing formal between state police. I've worked with [investigator from another country] now. Him and I just keep in touch. Yeah, it's set at a very light level*." (Interview 10, Regional agency, Australia).

In the previous citation, the investigators share his experiences with informal collaboration. Sharing that he did create relationships with other police officers that he accumulated by researching on the darknet while working on those cases. According to our participants, informal collaborations seem to be created through the accumulation of contacts outside their agency as well as contacts exchanges within the organisation.

> "*I have colleagues that... uh, who have contacts, let's say Europol or, you know, we were talking about the Netherlands earlier, Switzerland, Australia, anywhere … If I have a need in another country, I'll find myself a colleague who has a contact there. So, there are contacts*." (Interview 2, Provincial Agency, Canada).

Additionally, interviewees mention the option of contacting a Europol employee directly through a colleague's contact, meaning they can avoid Europol's official collaboration request process. As mentioned previously, formal collaborations are defined as taking a considerable amount of time and informal collaborations are therefore interesting in order to speed up the time it takes to establish a collaboration.

Private collaborations

The third type involve *collaborations with private companies*. These are especially useful and necessary to obtain legal and digital evidence in the context of cybercrimes that can be legally brought to court. This type of partnership can take place within local, regional or multinational companies. In our sample, they essentially represented banks or large corporations like Facebook, Google and Microsoft. Although private-public collaborations are not always easy nor in the interest of private companies, participants' experiences suggest that the success of them seem to vary on a case-by-case basis.

Although in general, our participants expressed having made requests for cooperation with private companies in order to obtain information on suspects, victims or on events. It turns out that the relations between the two parties can become collaborations, in the sense that private companies can also benefit from police support. Participant #17 presents his experience with a specific example where the police had initiated the partnership with several banks in the United-Kingdom, because they needed intelligence for their new cybercrime units. Finally, after being the victim of a cyber-attack, the banks benefited from the help of this cyber team. Thus, although the relationship between private companies generally seems to be one-way, sometimes it turns into a two-way relationship where both parties benefit.

> "*It was a partnership with the banks. So, what happened is the [a public law enforcement] created a cyber unit to tackle… Basically it was going to be one of the UK's response to tackling cybercrime. And in order to do that, we needed intelligence from banks because they were the ones who were seeing a majority of it. And we worked with the banks through a partnership approach. They then came to us and identified that they were suffering from a new strain of malware that was impacting about six, seven banks in the UK, actually six or seven banking customers in the UK and they were probably losing out of a couple hundred thousand pounds a day*." (Interview 17, Federal agency, United Kingdom).

In general, participants expressed having to undertake legal procedures, with lawyers and judges' permissions to obtain cooperation from private companies. However, some participants also experimented collaborations with companies that did not have the same approach to protecting

their customers' data. They were thus able to obtain the necessary information without official documentation.

> "*It wasn't me that called up, but it was another that called-up… a Taiwanese company and asked for: "Hey we've got this account. It's gotta be bad guys account… Can you just tell us something about it? ". And they just gave them all the details [...] without a production order, warrant or anything because they don't care.*" (Interview 5, Municipal agency, Canada).

These collaborations do not seem to be experienced by all investigators. Indeed, although some organisations have established effective collaborations, others hit walls and must take legal steps.

One principal reason that private companies refuse to cooperate seems to be the desire to protect their customers' data. However, according to the experience of investigators in this study, some companies take a stand against the police, and adopt a refractory attitude towards all requests from law enforcement.

> "*Uh… Just honestly, just more cooperation and understanding like we know that everyone has the right to privacy and communicate to whom they want and what they want to communicate with but sometimes these companies are either 100% anti law enforcement or they are just no equipped to handle a lot of requests. Some companies are very good but the one a lot of these types communication app services are not even located in the United States so getting someone to actually work with you overseas is very difficult*." (Interview 11, Municipal agency, United States).

However, another reason that seems to be the cause of denial to collaborate is the fear that the collaboration with the police will be public, and thus will damage the company reputation. As participant #20 explains, publicly traded companies are fearful of public opinion and thus can be hesitant to cooperate with the police, either because they fear to demonstrate a cybersecurity vulnerability or offending customers.

> "*Another huge thing about our investigations is cooperation. The businesses just don't… once they get a lawyer involved and their cyber coach, there's just no cooperation and it's incredibly frustrating. And the reasons behind it, you try to… we try to understand, but it doesn't make sense. They're being provided advice at some point that slows any kind of communication with us. I don't know what that advice is, but we're not getting the information after the cyber coaches*

> *and counsel talk to them. And it could be a risk-based thing, too, right? If there's they don't want to share data that's on their server, they're afraid of something that might be maybe illicit financing or something like that. But we're not looking for that. We're not interested in that. We're interested in the logs and kind of more higher-level data. And we try to explain that. But again, and some people don't even want to report it because of obviously optics and the stock trade. Right. On how much how much their company's worth*." (Interview 20, Provincial agency, Canada).

Although, it is important to acknowledge that the participants expressed great understanding for private companies being reluctant to collaborate, specifically to share information about their customers. As participant #18 mentioned, he himself would not want anyone to have access to his data without a valid reason. However, he adds that for them, being law enforcement, they need to obtain information on an identified suspect and want to cooperate with that private company for a specific case.

> "That's *why we are understanding. I wouldn't want someone to just go through my personal data and messages just because the hell of it. But what we have is an identified target and we know that we're looking for cooperation that is essentially it*." (Interview 18, State Agency, United Kingdom).

Even if there is a reluctance to collaborate among some companies, our participants seemed optimistic about the future of relationships between the police and private companies, particularly in cyber cases. Specifically, in many instances, a factor that greatly helps collaboration is communication. Precisely when the police agency justifies their requests by explaining their intentions and motivations, the companies are more open and wish to demonstrate that they are in good faith.

> "It's *getting better. Umm… cause those companies want to show that they are working in good faith, so it is getting better. A lot more companies are providing information to law enforcement either via, you know, search warrant, sopinas, officially dragged letter head indicating why you need all these indications for it. It all depends on the company*." (Interview 11, Municipal agency, United States).

However, even if the companies wish to collaborate, it is noted that legal procedures must be undertaken to achieve collaboration with private companies and especially in order to be able to bring this evidence to court. Each of these steps requires time and resources.

Conclusion

Moreover, the results of the study illustrate that collaborations can take different forms. Between police organisations, they can be formal, thus referring to the use of inter-agency communication procedures or through an official collaborative body. They can also be informal, therefore, characterised by the exchange of information or mutual assistance between contacts accumulated through networking (Kreiner and Schultz, 1993; Lavers and Chu, 1997; White, 2011; Inyang and Abraham, 2013; Kim et al., 2013). This last form of collaboration being often faster, not requiring procedures, is often used during urgent requests or investigations involving the abuse of children according to the testimonies analysed. Indeed, the most important criticism of official organisations exposes the slowness of these organisations to exchange information between different police agencies (Lavers and Chu, 1997; Bayer, 2010; Deflem, 2016). Moreover, formal communication institutions create cumbersome bureaucratic steps that require formal requests for information exchange (Lavers and Chu, 1997; Den Boer, 2013). These constraints lead some police officers to collaborate informally with others in order to exchange information. As mentioned by Raustiala (2002) and Slaughter (2004), the sharing of informal information can be crucial in the progress of police investigations and have a significant impact on the identification of suspects. The interest of informal collaboration is therefore to speed up investigations by being more efficient and to avoid bureaucracy. Although, those informal interactions are usually not accepted in court, meaning they can be useful for intelligence purposes or for interventions on the darkweb for example, but can't be used to prosecute nor be considered as digital evidence. However, the results of the study suggest that collaborations, whether formal or informal, are generally effective and that police organisations around the world are open to collaboration, with the exception of certain countries, for example Russia or China.

Nevertheless, although our results suggest that collaboration is one of the ways to fight against this scourge, important limits to international collaborations must be addressed. Indeed, although international collaborations between police agencies transcend jurisdictions, the latter remain strongly influenced by national policies (Deflem, 2002). Police agencies respond to the concerns of their political leaders, who direct their actions according to politics. This directly restricts the freedom of police agencies to collaborate internationally (Deflem, 2002), as suggested by our results when it comes to collaboration with Russia or China.

Outside of police organisations, collaborations can also take place within private companies. Nevertheless, these collaborations are brought as being sometimes very effective and sometimes absent. Indeed, our results suggest that some private companies simply refuse to cooperate for multiple reasons, for example, by general refusal to cooperate with the police or by lack of response to requests for information. Some studies have also emphasised the need to improve information exchange relations between police organisations and private companies (see Hinduja, 2007; Wexler, 2014; Vincze, 2016; Dodge and Burruss, 2019). It should be noted that more and more private organisations, i.e. businesses, offer paid protection services to the population or independent investigation services that compete with public organisations[25] (Shearing and Stenning, 1983; Johnston, 2005). Nevertheless, the collaboration between private and public organisations does not seem to be optimal according to our results despite the co-dependency of new collaborative initiatives by coordinating institutions and ILOs. While it is acknowledged that the police and private companies have distinct goals (public safety (Lemieux, 2018) vs. capitalisation (Carr, 2016)) (Dodge and Burruss, 2019), our results illustrate that, in supplement of this disparity in objectives, the companies' attitude towards law enforcement also has a significant impact on collaboration.

Thus, in the light of the results obtained, we suggest that future research should envision the types of collaboration without making any doctrinal distinction between public vs private collaborations, even if they have their own components, limits and uses. In the end, they are all worthy and essential for the success of those investigations.

The results allow us to identify different types of collaboration carried out by investigators from different countries and levels of police agencies and how these materialised. Like any study, this one has significant limits on its scope due to its small sample of participants but also to the number of countries it represents. We recommend that future studies deepen the knowledge of the types of collaboration and especially on how to improve them by structuring research to identify possible solutions, for example, how to accelerate formal collaborations, how to legally accept the use of informal police to police collaboration and above all, how to facilitate collaboration between private companies in order to increase their trusts and report rate.

[25] For example: “BAE Systems, CSRA, General Dynamics and Northrop Grumman” (Lemieux, 2018, p.16).

CHAPITRE 5 : DISCUSSION

Dans ce chapitre, nous discuterons des résultats obtenus dans les deux articles qui composent ce mémoire. Pour ce faire, chacune des thématiques identifiées sera présentée afin de discuter de leurs implications et de les mettre en relation avec la littérature mobilisée au premier chapitre. Nous poursuivrons en répondant à l'objectif général et en décrivant les apprentissages cumulés afin de pousser la compréhension du sujet d'étude. Finalement, nous discernerons les limites des résultats, ce qui guidera nos recommandations pour les avenues de recherche.

Ce mémoire avait comme objectif principal de comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb grâce à l'expérience de participants. Précisément, les résultats obtenus proviennent de l'analyse qualitative de 20 entretiens représentant des enquêteurs policiers de différentes agences policières réparties dans cinq pays : le Canada, les États-Unis, l'Australie, le Royaume-Uni et la Suède. Cette étude exploratoire s'est donc basée sur le vécu des enquêteurs afin d'accroître la compréhension de ce nouveau phénomène empiriquement peu recherché.

1. Sous-objectif 1 : les motivations des enquêteurs

Tout d'abord, le premier sous-objectif de ce mémoire consistait à décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière dans le cadre d'enquêtes impliquant l'utilisation du darkweb. À la lumière des résultats présentés dans le premier article (Chapitre 4, Article 1), nous avons décrit et identifié cinq principales motivations qui ont incité un corpus de 20 enquêteurs à réaliser des collaborations dans le cadre de leur fonction. Les motivations représentent des thématiques identifiées à l'aide de la méthode d'analyse et de codification classique.

Dans l'ensemble, les résultats exploratoires de cet article ont illustré que les enquêteurs désirent et possèdent de la volonté à collaborer, et ce, malgré les barrières institutionnelles et législatives auxquelles ils font face. En effet, il est important de se remémorer que la collaboration interagence policière, qu'elle soit intra ou interpays n'est pas implicite et s'avère une nouveauté dans l'histoire de la police. Malgré tout, nous avons pu observer un grand désir à collaborer auprès des participants, et ce, pour de multiples raisons. En effet, selon les expériences des enquêteurs que nous avons interrogés, les collaborations internationales permettent de partager efficacement l'information (1), de rendre les enquêtes plus efficaces (2), d'aider à identifier les suspects (3) et

les victimes (4), en plus d'assurer la poursuite des enquêtes criminelles qui mènent à des arrestations dans de multiples juridictions (5). Toutefois, bien que nous ayons identifié et décrit cinq principales raisons qui motivent les enquêteurs à collaborer, il est notable d'observer que la première motivation, le partage d'informations, est une thématique sous-jacente aux autres. En effet, le partage d'informations est une thématique qui se veut à la fois une motivation et un outil sous-entendu dans les autres thèmes. La distinction fut toutefois réalisée dans un but descriptif, étant donné l'importance et le désir profond de collaborer pour obtenir des informations. D'autre part, les thématiques présentées sont interreliées. En effet, un enquêteur peut avoir plusieurs motivations à collaborer avec une autre agence. Par exemple, celui-ci peut avoir contacté une agence policière dans un but précis et changer d'idées en cours de route, tout dépendamment des besoins pour l'avancement de l'enquête. Les thématiques sont donc dynamiques et ne représentent pas des catégories fermées.

À l'aide de l'interprétation des résultats, nous suggérons que les enquêteurs désirent collaborer pour de multiples raisons qui visent principalement à accroitre leur pouvoir et contrôle sur le déroulement de l'investigation. Ainsi, la collaboration leur permet de contrer les limites importantes auxquelles ils font face au quotidien.

En effet, nos résultats suggèrent que trois des motivations, à savoir le partage d'informations, l'identification des suspects et l'identification des victimes contribuent à la désanonymisation du darkweb et permettent aux enquêtes policières d'avancer. Le partage d'informations permet de contrer les limitations imposées par les juridictions, en échangeant des informations ou encore en transférant le dossier à un service de police ayant la capacité juridique d'entreprendre des poursuites judiciaires contre un ou plusieurs suspects identifiés. De plus, les collaborations policières sont particulièrement opportunes pour agir rapidement et contrer les délais imposés par la détection parfois lente de la victimisation. Enfin, les collaborations permettent de pallier le manque de formation des policiers, en permettant l'échange de conseils voire d'outils. Comme le mentionnent de nombreux chercheurs (ex., Burns et al., 2004; Calderoni, 2010; Bossler et Holt, 2013; Leukfeldt et al., 2013; Brown, 2015; Boes et Leukfeldt, 2017; Harkin et al., 2018; Dolliver, 2019; Faubert et al., 2021), le manque de formation en profondeur est une barrière significative à la réponse policière efficace pour ces types de crimes, notamment en raison du retard des policiers face à l'évolution constante des technologies. Nos résultats illustrent ainsi que la collaboration se

veut utile afin de contrer le sentiment d'incompétence des policiers que certaines études ont démontrés (voir Bossler et Holt, 2013; Burns et al., 2004; Hadlington et al., 2018; Harkin et al., 2018; Burruss et al., 2019).

Par ailleurs, il est possible d'observer que les motivations exprimées par nos participants correspondent étroitement à l'une des dimensions de la typologie d'actions collaboratives de Whelan et Dupont (2017) : l'échange d'informations. Cette dimension étant décrite comme des actions facilitant le partage d'information à l'interne et à l'externe des limites légales d'une organisation (Whelan et Dupont, 2017). En supplément, nous observons des ressemblances entre deux autres motivations identifiées et d'autres dimensions de la typologie. L'identification de suspects pourrait représenter la génération de connaissances. Toutefois, il est précisé que cette catégorie représente davantage les connaissances orientées sous le concept de la police fondée sur les preuves donc des informations qui visent à orienter les actions de la police (voir Sherman, 1998; Sherman, 2013; Lum et Koper, 2015; Lum et Koper, 2017; Fleming et Rhodes, 2018). Les exemples offerts se concentrent sur le crime organisé et l'évaluation de menaces terroristes. Ainsi, nos résultats amènent un nouvel angle bien précis aux crimes commis sur le darkweb à cette typologie, la génération de savoirs représente à la fois la démystification des individus impliqués par le crime, que ce soient les suspects ou victimes et le partage d'outils et astuces afin de générer de nouvelles connaissances sur les technologies (aptitudes cognitives). D'un autre côté, la motivation à gagner du temps et à accélérer les enquêtes pourrait correspondre à la résolution de problèmes. Il fut largement documenté dans la littérature que la lenteur des institutions formelles cause des problèmes aux agences policières (voir Lavers et Chu, 1997 ; Bayer, 2010 ; Deflem, 2016), principalement car celles-ci impliquent de lourdes procédures bureaucratiques (Lavers et Chu, 1997 ; Den Boer, 2013). Nos résultats permettent de documenter empiriquement les insatisfactions que les policiers vivent face aux institutions formelles. Ils ont donc recours à des collaborations informelles qui sont caractérisées par l'échange d'informations ou l'entraide entre contacts accumulés grâce au réseautage (Kreiner et Schultz, 1993 ; Lavers et Chu, 1997 ; White, 2011 ; Inyang et Abraham, 2013 ; Kim et al., 2013) afin d'accélérer leurs enquêtes. Ces contraintes amènent certains policiers à collaborer de manière informelle avec d'autres afin d'échanger des informations. En effet, suivant la définition de Scott et Boyd (2020) de la collaboration publique interagences, le partage d'informations de manière informelle devient ainsi crucial dans la réponse

policière aux crimes et a un impact significatif sur l'identification des suspects (Raustiala, 2002 ; Slaughter, 2004).

Ainsi, bien que la typologie de Whelan et Dupont (2017) soit basée la littérature et se concentre sur les fonctions de réseaux créés au sein des organisations policières qui désirent collaborer, les motivations identifiées dans ce mémoire représentent le justificatif des actions de collaboration réalisée par nos participants. Il est donc possible de tisser des liens entre ces deux études. Par conséquent, plus de détails concernant ces dimensions seraient requis afin de s'assurer avec certitude de la cohésion des résultats. Cette typologie fut par ailleurs construite afin de guider les recherches futures sur le sujet (Whelan et Dupont, 2017). Une mise à jour de cette typologie permettrait d'inclure et d'ajuster celle-ci au besoin des unités responsables des crimes technologiques à la lueur des résultats obtenus ainsi que des conclusions des études sur les unités spécialisées en cybercriminalité (ex., Harkin et al., 2018; Nowacki et Willits, 2020).

En somme, étant la première étude à se pencher sur ce qui motive les enquêteurs à collaborer dans le cadre de leur fonction, la description des motivations identifiées mises en relation avec la littérature permet de comprendre pourquoi les enquêteurs désirent collaborer. En outre, les résultats de l'étude illustrent que les collaborations peuvent prendre différentes formes dépendamment du motif. Bien que le deuxième article nous informe davantage sur les types de collaboration, les résultats de ce sous-objectif ont mis la lumière sur le caractère subjectif et/ou discrétionnaire qui influence les raisons qui poussent les enquêteurs à collaborer, décision de l'enquêteur de collaborer d'une façon ou d'une autre.

2. Sous-objectif 2 : les types de collaboration

Le deuxième sous-objectif de ce mémoire consistait à *décrire et comprendre les types de collaboration mobilisés dans le cadre d'une enquête policière sur le darkweb.* Tenant compte des résultats obtenus dans le deuxième article (Chapitre 4, Article 2), il est possible d'observer que nous avons identifié et décrit trois types de collaboration expérimentés par nos participants dans le cadre de leur emploi : 1) formelle 2) informelle 3) privée.[26]

[26] Prendre note qu'un quatrième type fut codifié dans le cadre de nos analyses. Toutefois, par manque de validité interne, causé par l'absence de cette thématique dans une grande proportion des entretiens, celui-ci fut omis des résultats. Ce type représentait les collaborations auprès des institutions publiques, pouvant représenter des organismes gouvernementaux ou des institutions académiques. Quelques études récentes se sont concentrées sur le sujet des partenariats entre les agences policières et ces institutions, par exemple sur le sujet des affaires classées (« cold case »

À priori, dans la littérature, on retrouve deux des types de collaboration décrites dans notre article : la collaboration formelle (voir Lavers et Chu, 1997; Rothe et Friedrichs, 2015; Lemieux, 2018) et informelle (voir Kreiner et Schultz,1993; Lavers et Chu, 1997; Bayer, 2010; White, 2011; Inyang et Abraham, 2013; Kim et al., 2013). En supplément, on retrouve par ailleurs de nombreuses études sur le partenariat public-privé, donc entre les compagnies privées et les agences policières/publiques (ex., Shearing et Stenning, 1983; Johnston, 2005; Levi et Williams, 2013; Pomerleau, 2019; Pomerleau et Lowery, 2020). Cependant, ces collaborations sont traitées comme étant distinctes dans la littérature, séparant les collaborations en fonction des parties prenantes dans celles-ci. Précisément, elles sont distinguées entre celles qui impliquent des agences policières, généralement définies comme des institutions publiques ayant pour mission d'appliquer la loi civile, criminelle et pénale afin de maintenir l'ordre dans la société (Lemieux, 2018) et toutes autres organisations qui possèdent des objectifs différents.

Toutefois, nos résultats illustrent que pour le contexte des cybercrimes et précisément les crimes commis à l'aide du darkweb, les trois types de collaboration sont essentiels aux enquêtes et font partie intégrante du travail des policiers. Ainsi, à la lumière des résultats obtenus grâce aux témoignages des participants, nous suggérons d'observer les types de collaboration comme étant un tout, sans faire de distinction doctrinale en les unissant sous la même étude. Il est notable que chacun de ces types possède des composantes, limites et utilités qui leur sont propres.

Plus en détail, les résultats de l'étude dévoilent que les collaborations prennent différentes formes comme il est mentionné dans la littérature. Entre organisations policières, elles peuvent être formelles, faisant ainsi référence à l'utilisation de procédures de communication inter-agences (ex. Interpol ou Europol) ou par l'intermédiaire d'un organisme officiel tout comme l'expliquent les chercheurs sur le sujet (Lavers et Chu, 1997; Rothe et Friedrichs, 2015; Lemieux, 2018). Or, ces chercheurs se sont concentrés sur d'autres types de crimes pour leur analyse que ceux observés dans ce mémoire, soit le terrorisme et le trafic de drogues. Par ailleurs, nos participants ont aussi signalé vivre des désagréments face à la collaboration formelle, en raison des longs délais de transfert des informations, ce qui avait été rapporté dans des études précédentes (voir Lavers et Chu, 1997 ; Bayer, 2010 ; Deflem, 2016). En 1997, les chercheurs Lavers et Chu dénonçaient

en anglais) (voir. Fox et al., 2020; Holt et al., 2022) ou sur l'exploitation sexuelle des enfants en ligne (ex. Sinclair, Duval et Fox, 2015). Malgré la faible présence de témoignage à ce propos dans nos données, il serait important d'explorer ce sujet dans de futures recherches afin de l'inclure comme thème à aborder dans le cadre d'entretiens ou à prendre en considération dans le devis de recherche.

l'incompétence des institutions officielles chargées de faciliter la coopération et collaboration policière internationale, expliquant que celles-ci répondent inefficacement à leur mandat. En conséquence, malgré les efforts de ces institutions, il est préoccupant que deux décennies plus tard, cette problématique soit encore d'actualité.

De ce fait, les enquêteurs ont exprimé avoir recours à des collaborations informelles qui se matérialisent par des communications rapides et efficaces entre policiers issus des différentes agences policières, et ce, surtout lorsque des victimes sont potentiellement à risque de subir des torts physiques ou sexuels. Comme le mentionnent Raustiala (2002) et Slaughter (2004), le partage d'informations de manière informelle peut être crucial dans le déroulement des enquêtes policières et avoir un impact significatif sur l'identification des suspects.

Par ailleurs, comme le décrit Bayer (2010) dans son ouvrage, les relations formelles sont aidantes et essentielles, mais les relations informelles sont puissantes, car elles redonnent le pouvoir aux policiers. Il est noté dans la littérature que les officiers de police apprécient et désirent avoir de l'autonomie face à leur centre de décision (Deflem, 2002). Avoir recours aux institutions de collaboration formelle, enlève le contrôle des mains des enquêteurs sur leurs propres enquêtes. Ils deviennent ainsi dépendants des actions de ces institutions et doivent se confondre aux délais qu'elles imposent. Par ailleurs, les collaborations informelles permettent de mettre de l'avant les expertises des enquêteurs en échangeant non seulement du renseignement criminel, mais aussi des informations techniques sur comment trouver des informations (Bayer, 2010). Nos participants ont partagé que les collaborations informelles les aident à se tenir à jour sur les nouvelles techniques et outils qui peuvent les aider à démasquer les criminels sur le darkweb.

Cependant, ces interactions informelles ne sont généralement pas acceptées devant les tribunaux, ce qui signifie qu'elles peuvent être utiles à des fins de renseignement ou pour des interventions sur le darkweb par exemple, mais ne peuvent pas être utilisées pour poursuivre ni être prises en compte comme preuve à la cour. Elles permettent donc d'initier des enquêtes, d'améliorer la compréhension du phénomène observé et d'obtenir des informations sur des outils, mais ne peuvent représenter des preuves digitales. Tout comme il est précisé dans la littérature, les policiers collaborent informellement grâce à l'accumulation de contacts de confiance grâce au réseautage (Kreiner et Schultz,1993; Lavers et Chu, 1997; White, 2011; Inyang et Abraham, 2013; Kim et al., 2013).

En dehors des organisations policières, des collaborations peuvent également avoir lieu avec des entreprises privées. Néanmoins, ces collaborations sont amenées comme pouvant être très efficaces, mais aussi inexistantes. En effet, nos résultats suggèrent que certaines entreprises privées refusent tout simplement de collaborer pour de multiples raisons, par exemple par refus général de vouloir travailler avec la police ou par l'absence de réponse aux demandes d'informations. Certaines études ont également souligné la nécessité d'améliorer les relations d'échange d'information entre les organisations policières et les entreprises privées (voir Levi et Williams, 2013; Pomerleau et Lowery, 2020). Néanmoins, la collaboration entre les organisations privées et publiques ne semble pas optimale selon nos résultats malgré la dépendance des enquêtes sur les crimes commis à l'aide du darkweb sur celles-ci. Dans le cas d'un refus de collaboration auprès d'une entreprise privée, les enquêteurs doivent faire des demandes légales auprès de juges afin d'obtenir les mandats légaux nécessaires. Par la suite, les compagnies privées engagent des avocats afin de procéder aux demandes légales en protégeant leurs intérêts. Ce processus est coûteux tant sur le plan temporel que sur les ressources policières. Nos participants ont partagé que dans les rares cas où les compagnies privées acceptent de collaborer sans que des mandats légaux les obligent, les enquêtes sont efficaces et ils obtiennent des résultats considérables.

Bref, ces résultats nous permettent de comprendre comment des enquêteurs issus d'agences policières de différents niveaux et pays collaborent. La description des types de collaboration expérimentés par les sujets nous permet de comprendre comment elles prennent forme, mais aussi comment celles-ci sont vécues par les policiers. En effet, grâce à l'unité narrative des participants, nous avons non seulement pu identifier quel type de collaboration ils ont expérimenté, mais comment celles-ci ont été vécues en mettant en lumière le justificatif, les attitudes et les émotions qui en ressortent.

3. Discussion générale : la compréhension de la collaboration policière internationale

À la suite de cette discussion, il est possible d'établir un portrait de la collaboration policière à l'appui de données empiriques. Nos résultats permettent de décrire et de comprendre ce qui motive les policiers chargés d'enquêter sur des crimes commis à l'aide du darkweb à collaborer, tout en décrivant les types de collaboration expérimentés.

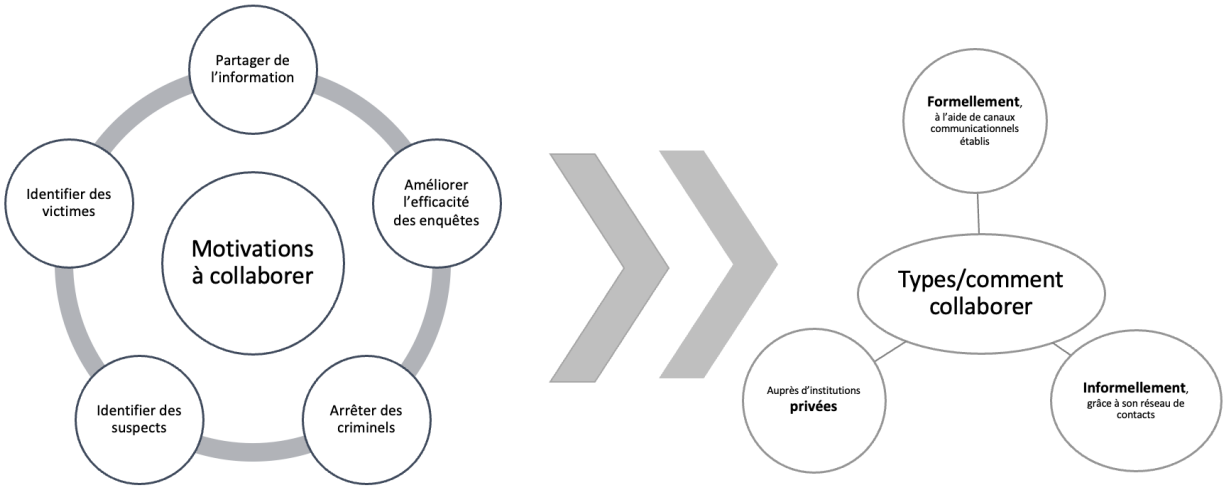
Précisément, c'est en produisant des connaissances sur le contexte dans lequel les collaborations prennent forme que nous pouvons compléter notre objectif principal. Comme le précise le philosophe Duncan Pritchard, la compréhension d'un phénomène se manifeste par l'accumulation des connaissances qui sont mises en contexte et que la connaissance à elle seule ne possède pas de valeur (Pritchard, 2008). Ainsi, nous répondons à l'objectif principal de ce mémoire en réunissant les connaissances sur le sujet de la collaboration et sur les crimes commis à l'aide du darkweb afin d'améliorer la compréhension de ce sujet. En plus de la revue de la littérature, nos données empiriques présentent des connaissances nouvelles et offrent une perspective internationale sur un sujet sous observé à l'aide de preuves empiriques. Dans cette section, nous allons détailler les apports empiriques issus des résultats qui contribuent à la compréhension de l'objet d'étude.

3.1.Collaborer, un choix ou un besoin?

À la lumière de nos résultats, nous pouvons conclure que la collaboration internationale s'avère efficace pour l'enquête policière sur les crimes commis à l'aide du darkweb. Toutefois, nos participants ont partagé que la collaboration internationale ne s'avère pas simplement utile, mais bien essentielle à la réalisation d'enquête sur le darkweb. En effet, les participants de l'étude n'ont à aucun moment remis en question la légitimité ou la pertinence des collaborations, c'est-à-dire qu'ils partagent l'opinion que les collaborations sont essentielles et efficaces pour réaliser le travail de la police sur le darkweb. À l'opposé, dans la littérature sur le terrorisme, le trafic de drogues et le crime organisé, la collaboration est amenée comme un étant un choix, une option ou une solution afin d'améliorer l'efficacité des enquêtes, d'éviter de conduire en double des enquêtes, etc. (Burns et coll., 2004; Sanders et Henderson, 2013, Sarre et al., 2018). Pour les crimes sur le darkweb, nos résultats illustrent que les enquêteurs n'ont simplement pas le choix de collaborer afin de puiser de l'information à l'international et d'acquérir des preuves digitales. Ainsi, la collaboration internationale est essentielle afin de combattre les crimes sur le darkweb (Europol, 2023, 2 mai).

Néanmoins, bien que les enquêteurs aient besoin de collaborer, ils sont maîtres de choisir comment celles-ci vont prendre forme. À l'aide de l'illustration des sous-thèmes identifiés dans ce mémoire (Figure 1), il est possible de les observer comme un tout. Bien qu'ils aient fait l'objet d'articles séparés dans ce mémoire en raison de leurs caractéristiques et objectifs de recherche distincts, il est possible de tisser des liens entre les motivations à collaborer et les types de collaboration expérimentés par les enquêteurs.

Figure 1. Conceptualisation dynamique des sous-thèmes identifiés



En premier lieu, les enquêteurs peuvent décider d'entreprendre différents types de collaboration dépendamment des motivations qui ont initié leur intérêt à faire de telles actions. Toutefois, nos résultats ont démontré qu'il n'y a pas de lignes directionnelles ni de relation de cause à effet entre une motivation et un type. Les enquêteurs prennent leur décision en fonction de leurs besoins, ressources et capacités. À titre d'exemples, nos participants ont décrit avoir eu recours à des collaborations privées afin d'identifier des suspects, à des collaborations informelles afin d'obtenir des connaissances sur un nouveau cryptomarché, à des collaborations formelles afin de transférer un dossier à une agence policière ayant le pouvoir légal de procéder à l'arrestation d'un criminel situé dans une juridiction éloignée. Tous ces exemples démontrent que derrière chaque type de collaboration mobilisé se trouve une motivation qui a poussé l'enquêteur à prendre certaines actions.

En somme, la collaboration ne s'avère pas un choix, mais un besoin central afin de réaliser des enquêtes sur des crimes commis à l'aide du darkweb. Or, les enquêteurs doivent prendre de nombreuses décisions afin de diriger leurs actions et répondre aux besoins qui ont initialement motivé cette collaboration.

3.2.L'impact des conflits d'objectifs sur la collaboration

Il est possible d'identifier un point commun dans les nombreuses définitions recensées au premier chapitre de ce mémoire; une collaboration prend forme lorsque deux ou plusieurs acteurs désirent accomplir des actions dans un objectif commun (voir Agranoff, 2006; Thomson et Perry, 2006; Whelan, 2017; Scott et Boyd, 2020, Cigler, 2001; Keast et al., 2004; Keast et al., 2007.). Ainsi, face à l'absence d'intérêts ou d'objectifs communs, les collaborations ne peuvent se matérialiser.

En effet, même si des institutions désirent collaborer, il n'en demeure pas moins qu'il n'est pas rare qu'elles soient en conflit d'agendas (Lemieux 2018). Comme évoqué dans la littérature, les instances policières ont tendance à peu prioriser la collaboration pour enquêter sur les cybercrimes en raison de leur paradigme face à ceux-ci. En effet, plus une agence policière place les cybercrimes comme étant au bas de l'échelle de gravité moins ils représentent des priorités nécessitant l'investissement de temps et de ressources (Wall, 2007, 2008; Bossler et Holt, 2012; Holt et Bossler, 2012a, 2012b; Cross, 2015, 2018, 2020; Hadlington et al., 2018; Correia, 2019; Bossler et al., 2020; Leukfeldt et al., 2020; Cross et al., 2021; Notté et al., 2021; Paek et al., 2021).

Par ailleurs, la présence de compétition afin d'obtenir des ressources, par exemple aux États-Unis, peut aussi causer une disparité dans les objectifs. En effet, la présence d'un système de distributions des ressources basées sur la productivité des agences policières crée un environnement compétitif dans lequel les policiers thésaurisent leur information (Sanders et Henderson, 2013; Pickering et Fox, 2022) et travaille en silo pour ne pas partager le succès de la résolution d'un crime (Lemieux, 2018) par crainte de nuire à leur réputation aux yeux du public et du gouvernement (Boba et al., 2009). Cela cause de graves problèmes à la collaboration entre ces agences, mais aussi auprès d'agences internationales désirant obtenir des informations ou du support.

En supplément des conflits d'objectifs, Lemieux (2018) précise que les pays développés rapportent avoir de la difficulté à collaborer avec des pays non développés. Cela serait causé par les divergences significatives dans l'application des lois, les procédures judiciaires et le respect de standards des droits humains. Nos participants ont rapporté rencontrer des difficultés à collaborer avec certains pays, issus du BRICS[27], distinctement la Russie et la Chine. Comme le précise

[27] BRICS fait référence au regroupement économique et politique de pays émergents incluant le Brésil, la Russie, l'Inde, la Chine et l'Afrique du Sud (voir O'neill, 2001; Wilson et Purushothaman, 2003; Stuenkel, 2020).

Deflem (2002), les collaborations internationales entre agences policières sont fortement influencées par le contexte géopolitique. Les services de police répondent aux préoccupations de leurs dirigeants politiques qui orientent leurs actions en fonction de la politique. Cela restreint directement la liberté des services de police de collaborer à l'échelle internationale (Deflem, 2002). En conséquence, le manque de collaboration de certaines agences peut se transformer en relations conflictuelles (Crawford, 1997), précisément lorsque les agences sont incohérentes ou cachent des informations aux autres (Sedgwick et Hawdon, 2019). Or, malgré le manque de détails sur les raisons qui nuisent aux communications entre certains pays, nos résultats démontrent que les collaborations se font principalement avec des pays qui disposent de systèmes judiciaires similaires.

D'autant plus, les participants de notre étude ont partagé avoir vécu des difficultés à collaborer avec des compagnies privées en raison d'opinions et de mentalités discordantes. Nous réitérons qu'il est légalement périlleux d'obtenir des preuves judiciaires sans compromettre la confidentialité digitale des clients d'une entreprise privée (Tun et al., 2016; Vincze, 2016). Ainsi, la collaboration entre la police et les compagnies navigue sur des bases légales complexes. Outre cette difficulté, la police et les compagnies privées ont des objectifs antagonistes. En effet, la police a pour objectif et mandat d'assurer l'ordre public (Lemieux, 2018) et les institutions privées visent à accumuler du profit en fournissant des produits ou services à leurs clients (Carr, 2016). Bien qu'il soit mentionné dans la littérature que cette disparité pose des problèmes au PPP (voir Carr, 2016; Dodge et Burrus, 2019; Pomerleau et Lowery, 2020), nos résultats exposent que la disparité des opinions a aussi un impact. En effet, les enquêteurs ont partagé avoir vécu des refus de collaboration, car, selon eux, les compagnies ne voulaient simplement pas s'associer ni encourager les actions de la police.

En somme, la divergence entre les intérêts des parties impliquées peut causer l'absence complète de collaboration.

3.3.Synthèse des contributions à la littérature sur la collaboration internationale

Nous réitérons que les études théoriques, conceptuelles et empiriques sur la collaboration policière se sont concentrées sur l'étude des crimes dont le terrorisme, le trafic de drogues et le crime organisé par le passé. Ce mémoire a ainsi permis de générer de nouvelles connaissances afin de

combler un manque de données empiriques et un vide dans la littérature. Pour ce faire, nous avons utilisé une perspective internationale afin d'avoir un aperçu global des collaborations et microscopique observant les enquêteurs directement, et non leur environnement. En résultat, ce mémoire permet de contribuer à la littérature scientifique à différents niveaux.

En premier lieu, grâce à la recension de la littérature, nous avons mis en œuvre les ouvrages existants sur des thématiques distinctes et peu recherchées. Nous avons ainsi tissé des liens entre la collaboration policière, les cybercrimes et le darkweb. La recension a permis de synthétiser sous un même écrit les défis que les technologies anonymisantes, dont le darkweb, causent aux enquêtes.

En deuxième lieu, ce mémoire contribue à la littérature en disposant de preuves empiriques sur non seulement l'utilité des collaborations, mais bien sur la nécessité de celles-ci afin de réaliser des enquêtes sur le darkweb. Subséquemment, les résultats des articles scientifiques ont permis d'explorer la solution proposée par les chercheurs, soit d'accroître la collaboration internationale entre les agences policières (Burns et coll., 2004; Sanders et Henderson, 2013, Sarre et al., 2018) et de démontrer son utilité (Dupont, 2017; Lemieux, 2018) grâce à des données empiriques. En conséquence, ce mémoire génère de nouvelles connaissances, étant le premier à se concentrer sur les motivations des enquêteurs à collaborer dans le cadre de leur emploi en décrivant cinq motivations ayant motivé des enquêteurs issus de différents pays à collaborer.

En troisième lieu, cette étude permet d'établir les bases pour le domaine d'études sur la collaboration policière dans le contexte des crimes commis sur le darkweb et les cybercrimes en général. Nous proposons de nouvelles façons de concevoir les études sur la collaboration policière afin de les adapter à la réalité du darkweb. En effet, nous suggérons d'observer les trois types de collaboration comme un tout et d'y accorder autant d'importance considérant leur rôle primordial et égalitaire dans l'enquête des cybercrimes. Plus généralement, nous proposons de voir la collaboration comme étant situé au cœur des enquêtes policières sur le darkweb, étant un besoin essentiel pour sa réalisation. Finalement, nous mettons l'accent sur l'importance de prendre en considération la disparité des objectifs dans l'observation de collaborations. Les recherches futures qui désireraient trouver des solutions pratiques ou théoriques devraient se concentrer sur la fusion des objectifs comme point de départ à toute collaboration autant au sein de la police qu'avec les compagnies privées.

CONCLUSION

En conclusion, l'objet d'étude de ce mémoire portait sur la collaboration en contexte d'enquêtes policières sur les crimes commis à l'aide du darkweb. Le darkweb est un concept faisant référence à l'ensemble des réseaux qui masquent l'identification des utilisateurs d'Internet en offusquant les adresses IP (Mirea et al., 2019). Étant donné sa nature, celui-ci complique l'identification des utilisateurs par les forces de l'ordre. Comme le mentionnent (Dodge et Burrus, 2020), les cybercrimes causent de nombreuses difficultés aux enquêtes qui nuisent significativement à la réponse efficace de la police. Ainsi, spécifiquement, les technologies anonymisantes ajoutent une difficulté supplémentaire aux enquêtes policières. Plusieurs chercheurs ont proposé comme solution d'accroître la collaboration entre les forces de l'ordre afin de contrer ces difficultés qui impactent les enquêtes (Burns et al., 2004; Sanders et Henderson, 2013; Sarre et al., 2018). Toutefois, à ce jour, il n'a pas été démontré empiriquement que les connaissances issues de la littérature sur le sujet de la collaboration policière, initialement créée pour les crimes comme le terrorisme, le trafic de drogues et le crime organisé sont généralisables aux crimes commis sur le darkweb. Ces crimes nécessitent des connaissances, compétences et outils spécifiques aux enquêteurs afin d'y naviguer et d'obtenir des informations sur l'acte commis et les suspects qui diffèrent grandement des crimes étudiés par la littérature.

Afin de contrer ce vide empirique, l'objectif principal de cette étude exploratoire consistait à comprendre les collaborations internationales dans les enquêtes policières sur les crimes commis à l'aide du darkweb. De ce fait, la méthodologie qualitative issue d'entretiens fut la méthode la mieux adaptée pour répondre à cet objectif. Un total de 20 entretiens auprès d'enquêteurs provenant de cinq pays (Canada, États-Unis, Royaume-Uni, Australie et Suède) a été analysé à l'aide de l'analyse thématique classique. Cette méthodologie a permis d'avoir accès aux perceptions, expériences et vécus au sein des membres de la police.

À la suite de la codification des données, deux articles scientifiques ont été réalisés afin de répondre aux sous-objectifs de recherche. Le premier sous-objectif visait à décrire et comprendre les motivations qui poussent les enquêteurs à collaborer à l'extérieur de leur agence policière. Dans cet article, cinq motivations ont été décrites ((1) le partage d'information, (2) l'efficacité de l'enquête, (3) l'identification de victimes, (4) l'identification de suspects et (5) l'arrestation de criminels)), ce qui a permis de comprendre pourquoi les enquêteurs désirent collaborer dans le cadre de leur emploi. Le deuxième sous-objectif avait pour but de décrire et comprendre les types

de collaboration nécessaire à la réalisation d'une enquête policière sur le darkweb. Cela nous a permis de comprendre comment les collaborations prennent forme dans le cadre des trois types identifiés et décrites ((1) formelle, (2) informelle et (3) privée).

À l'aide de données empiriques, cette recherche démontre la valeur ajoutée des collaborations policières aux enquêtes sur les crimes à l'étude. Les collaborations interrégionales et internationales sont présentées comme une solution afin d'augmenter l'efficacité des enquêtes et de lutter contre les nombreuses difficultés causées par les technologies anonymisantes, comme le darkweb, aux opérations/mécanismes de réponse policière, mais aussi comme un besoin essentiel au cœur des opérations policières sur le darkweb. Étant donné sa nature exploratoire, ce mémoire propose des bases sur lesquelles les futures études peuvent bénéficier.

Néanmoins, étant donné l'utilisation secondaire des données, cette étude présente des limites quant à son échantillonnage et à sa portée. En effet, les verbatims utilisés ne se concentraient pas entièrement sur la collaboration, les entretiens initiaux étant davantage orientés vers les types d'interventions policières ou d'enquêtes menées sur le darkweb. Au cours des entretiens, les participants ont discuté s'ils s'engageaient ou non dans des collaborations dans leurs activités et comment celles-ci se déroulaient. Des études ultérieures pourraient ainsi reproduire cette méthodologie en mettant l'accent sur les collaborations internationales en plus d'élargir la taille de l'échantillon pour permettre une plus grande représentativité des pays. Une autre limite concerne le choix de définitions de l'objet d'étude. Bien que nous ayons utilisé une définition large qui décrit la collaboration publique inter-agences comme la pratique par laquelle les divisions administratives gouvernementales assurent une responsabilité partagée pour atteindre un objectif commun (Scott et Boyd, 2020), nous proposons aux futures études d'analyser les types de collaboration le long d'un continuum entre coopération, coordination et collaboration (voir Mandell, 2001, Bryson et al., 2006 ; Keast et al., 2007 ; Mattessich et al., 2001 ; Thomson et Perry 2006 ; McNamara, 2012 ; O'Leary et Vij, 2012 ; Whelan, 2017). Cela permettrait d'approfondir la nature des différentes actions impliquées dans la collaboration. Nos données ne nous permettaient pas de classer les actes de collaboration par manque de précisions. Toutefois , les études devraient inciter les participants à apporter plus d'éléments et de détails dans leurs interactions afin de distinguer les types de collaboration dans leurs analyses.

Par ailleurs, nous reconnaissons que de nombreuses avenues rester à être explorées afin d'avoir une compréhension complète du sujet à l'étude. Par exemple, nous recommandons aux recherches d'explorer les collaborations au sein des pays issus du BRIC afin de comparer les résultats avec les pays qui bénéficient du Five Eyes Partnership. Aussi, nous suggérons d'approfondir les connaissances sur les types de collaboration et surtout sur la façon de les améliorer en structurant la recherche pour identifier les solutions possibles (ex., comment accélérer les collaborations formelles, comment accepter légalement le recours à la collaboration informelle entre des agences policières et surtout, comment faciliter la collaboration entre les entreprises privées afin d'augmenter leur confiance et leur taux de signalement).

Finalement, nous espérons que cette étude met en lumière la pertinence des collaborations internationales. Toutefois, considérant les limites de cette étude, il serait important de déterminer le rôle, soit l'implication concrète, de la collaboration internationale entre les agences policières dans le succès des cyberenquêtes. Des preuves empiriques et statistiques pourraient inciter les centres décisionnels et les dirigeants à faciliter les collaborations internationales (voir Nadelmann, 1993; Roberson et al., 2010; Lemieux, 2010) ou du moins, à favoriser le réseautage et les collaborations informelles entre les agents travaillant étroitement dans la réponse policière en contexte de cybercrimes.

RÉFÉRENCES

Abu Rajab, M., Zarfoss, J., Monrose, F. et Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. Dans J. Almeida, V. Almeida et P. Barford (*dir.*), *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement* (pp. 41–52). ACM.

Agranoff, R. (2006). Inside collaborative networks: Ten lessons for public managers. *Public Administration Review, 66*(1), 56–65.

Aldridge, J. et Décary-Hétu, D. (2014). Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *SSRN*. http://dx.doi.org/10.2139/ssrn.2436643

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. https://doi.org/10.1016/j.drugpo.2016.04.020

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

Andreas, P. et Nadelmann, E. (2008). *Policing the globe: criminalization and crime control in international relations.* Oxford University Press.

Armat, M. R., Assarroudi, A., Rad, M., Sharifi, H. et Heydari, A. (2018). Inductive and deductive: Ambiguous labels in qualitative content analysis. *The Qualitative Report*, *23*(1), 219-221.

Aromaa, K. et Viljanen, T. (2005). *Enhancing international law enforcement co-operation, including extradition measures: proceedings of the workshop held at the eleventh united nations congress on crime prevention and criminal justice*, *bangkok, thailand, 18-25 april 2005* (Ser. Publication series, no. 46). European Institute for Crime Prevention and Control affiliated with the United Nations (HEUNI).

ASIO (2023). *About*. https://www.asio.gov.au/

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal*, *18*(4), 383-400.

Bandow, D. (1991). War on drugs or war on America. *Stanford Law & Policy Review*, *3*, 242.

Banks, D., Hendrix, J., Hickman, M. et Kyckelhahn, T. (2016). *National Sources of Law Enforcement Employment Data* (publication n° NCJ 249681). U.S. Department of Justice. https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-sources-law-enforcement-employment-data

Barratt, M. et Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy, 35,* 1-6. https://doi.org/10.1016/j.drugpo.2016.07.005

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.

Bassiouni, M. C. (2013). *Introduction to international criminal law* (2nd rev., Ser. International criminal law series, v. 1). Martinus Nijhoff.

Bayer, M. D. (2010). *The blue planet: Informal international police networks and national intelligence*. Government Printing Office.

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

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

Bigo, D. (2000). Liaison officers in Europe: New officers in the European security field. Dans J. W. E. Sheptycki (dir.), *Issues in transnational policing* (pp. 67–99). Routledge.

Boba, R., Weisburd, D. et Meeker, J. W. (2009). The limits of regional data sharing and regional problem solving. *Police Quarterly, 12*(1), 22–41.

Boes, S. et Leukfeldt, R. (2017). Fighting cybercrime: A joint efforts. Dans R. M. Clark et S. Hakim (dir.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 185-203). Springer.

Boister, N. (2012). *An introduction to transnational criminal law.* Oxford University Press.

Bossler, A. M. et Holt, T. J. (2013). Assessing officer perceptions and support for online community policing. *Security Journal, 26*, 349-366.

Bossler, A. M. et Holt, T. J. (2016). On the need for policing cybercrime research. *ACJS Today*, *41*(1), 14-24.

Bossler, A.M. et Holt, T.J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management, 35*(1): 165–181.

Bossler, A.M., Holt, T.J., Cross, C. et Burruss, G.W. (2020). Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal,* (33), 311–328.

Bowling, B. et Sheptycki, J. (2012). *Global policing*. SAGE.

Braga, A. et Weisburd, D. (2007). *Police innovation and crime prevention: Lessons learned from police research over the past 20 years.* National Institute of Justice.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization, 75(*1), 39-70.

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

Braun, V. et Clarke, V. (2013). *Successful Qualitative Research*. SAGE Publications.

Brenner, S., et Schwerha, J. (2004). Cybercrime: A Note on International Issues. *Information Systems Frontiers, 6*, 111-114. https://doi.org/10.1023/B:ISFI.0000025779.42497.30

Bressler, F. (1992). *Interpol*. Presses de la Cité.

Brewer, R. (2013). Enhancing crime control partnerships across government: Examining the role of trust and social capital on American and Australian waterfronts. *Police Quarterly, 16*(4), 371–394.

Brodeur, J.P. (1983). High Policing and Low Policing: Remarks About the Policing of Political Activities, *Social Problems*, *30*(5), 507–520. https://doi.org/10.2307/800268

Broséus, J., Morelato, M., Tahtouh, M. et Roux, C. (2017). Forensic drug intelligence and the rise of cryptomarkets. Part I: Studying the Australian virtual market. *Forensic science international, 279*, 288-301.

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.

Brown, C. S. D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55-119. doi:10.5281/zenodo.22387

Bryson, J., Crosby, B. et Stone, M. (2006). The design and implementation of cross-sector collaborations: Propositions from the literature. *Public Administration Review, 66*, 44–55.

Burns, R. G., Whitworth, K. H. et Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice, 32*, 477-493.

Burruss, G., Howell, C. J., Bossler, A. et Holt, T. J. (2019). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: A latent class analysis. *Policing: An International Journal, 43*(1), 105-119. https://doi.org/10.1108/PIJPSM-08-2019-0142

Butler, S. (2019, 6 février). *The Role of PGP Encryption on the Dark Web*. TechNadu. https://www.technadu.com/pgp-encryption-dark-web/57005/

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R. et Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice*, *0*(0). https ://doi.org/10.1177/17488958221128128

Calderoni, F. (2010). The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change, 54*, 339-357.

Çalışkan, E., Minárik, T. et Osula, A.-M. (2015). *Technical and legal overview of the tor anonymity network*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43-62. doi:10.1111/1468-2346.12504

Casey, E. (2011). Digital evidence in the courtroom. Dans Casey, E. (Dir.), *Digital Evidence and Computer Crime*, 49-82. Elsevier.

Casey, E. (2019). The checkered past and risky future of digital forensics. *Australian Journal of Forensic Sciences, 51*(6), 649-664.

Chaiken, J. M., Chaiken, M. R., Karchmer, C. et Abt Associates. (1990). *Multijurisdictional drug law enforcement strategies: Reducing supply and demand* (pp. 43-47). US Department of Justice, Office of Justice Programs, National Institute of Justice.

Chainanalysis (2020). *The 2020 State Of Crypto Crime*.

Chang, Y. C. (2012). Combating cybercrime across the Taiwan Strait: investigation and prosecution issues. *Australian Journal of Forensic Sciences*, *44*(1), 5-14. http://dx.doi.org/10.1080/00450618.2011.581246

Cheurprakobkit, S. et Lerwongrat, K. (2023). Criminal justice officials' attitudes towards addressing computer crimes in Thailand: Difficulties and recommendations. *Trends in Organized Crime*, 1-21. https://doi.org/10.1007/s12117-023-09493-2

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.

Cigler, B. (2001). Multiorganizational, Multisector, and Multicommunity Organizations: Setting the Research Agenda. Dans M. P. Mandell (dir.), *Getting Results through Collaboration: Networks and Network Structures for Public Policy and Management* (pp. 71 – 88). Quorum Books.

Clasen, A. (2023, 25 avril). *West clashes with China, Russia over UN Cybercrime Convention. EURACTIV*. https://www.euractiv.com/section/law-enforcement/news/west-clashes-with-china-russia-over-un-cybercrime-convention/

Clifford, R. D. (2001). Cybercrime: The investigation, prosecution and defense of a computer-related crime. *Prosecution and Defense of a Computer-Related Crime*. https://ssrn.com/abstract=287574

CNC3 (2023). *Centre national de coordination en cybercriminalité*. Gendarmerie royale du Canada. https ://www.rcmp-grc.gc.ca/fr/gnc3

Cohen, G. (2018). Cultural fragmentation as a barrier to interagency collaboration: A qualitative examination of Texas law enforcement officers' perceptions. *American Review of Public Administration, 48*(8), 886–901.

Collaboration (2022). Dans *Larousse*. https://www.larousse.fr/dictionnaires/francais/collaboration/17137

Coopération (2022). Dans *Larousse*. https://www.larousse.fr/dictionnaires/francais/coop%c3%a9ration/19056

Correia, S.G. (2019). Responding to 125ictimization in a digital world: A case study of fraud and computer misuse reported in Wales. *Crime Science,* 8(1), 1–12.

Crawford, A. (1997). *The local governance of crime: Appeals to community partnerships.* Clarendon Press.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187–204.

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice,* 55, 1–12.

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology and Criminal Justice, 20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Cross, C., Holt, T., Powell, A. et Wilson, M. (2021) Responding to cybercrime: Results of a comparison between community members and police personnel. *Trends and Issues in Crime and Criminal Justice,* 635, 1–20.

Davies, G. (2020). Shining a light on policing of the dark web: an analysis of UK investigatory powers. *The Journal of Criminal Law*, *84*(5), 407-426.

Davis, S. et Arrigo, B. (2021). The Dark Web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change*, *76*(4), 367-386. https://doi.org/10.1007/s10611-021-09972-z

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. et Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice, 15*(2), 1429-1445.

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. https://doi.org/10.1007/s10611-016-9644-4

Deflem, M. (2000). Bureaucratization and social control: Historical foundations of international police cooperation. *Law and Society Review*, 739-778. https://doi.org/10.2307/3115142

Deflem, M. (2002). *Policing world society: Historical foundations of international police cooperation.* Oxford University Press.

Deflem, M. (2006). Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective. *Justice Quarterly, 23(3), 336-359*. DOI: 10.1080/07418820600869111

Deflem, M. (2016). Interpol. *The Encyclopedia of Crime and Punishment*, 1-4. https://doi.org/10.1002/9781118519639.wbecpx031

Den Boer, M. (2013). 3 Towards a governance model of police cooperation in Europe: the twist between networks and bureaucracies. Dans F. Lemieux (*dir.*), *International Police Cooperation* (pp. 60-79). Willan.

Den Boer, M. et Block, L. (2013). *Liaison officers: Essential actors in transnational policing.* Eleven International Publishing.

Denhardt, R. B. et Catlaw, T. J. (2014). *Theories of public organization.* Cengage Learning.

DiPiero, C. (2017). *Deciphering cryptocurrency: Shining a light on the deep dark web*. U. Ill. L. Rev.

Dodge, C. et Burruss, G. W. (2019). Policing cybercrime: Responding to the growing problem and considering future solutions. Dans R. Leukfeldt et T. J. Holt (dir.), *The Human Factor of Cybercrime* (Chapitre 15). Routledge.

Dolliver, D. S. (2019). Emerging technologies, law enforcement responses, and national security. *Journal of Law and Policy for the Information Society, 15*, 123-150.

Donalds, C. et Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior, 92*, 403-418. https://doi.org/10.1016/j.chb.2018.11.039

Duchesne, S. (2000). Pratique de l'entretien dit'non-directif'. Dans *Les méthodes au concret. Démarches, formes de l'expérience et terrains d'investigation en science politique* (p. 9-30). Presses Universitaires de France (PUF).

Dupont, B. (2004). Security in the age of networks. *Policing and society, 14*(1), 76–91. https://doi.org/10.1080/1043946042000181575

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change, 67,* 97-116. https://doi.org/10.1007/s10611-016-9649-z

Dupont, B., Manning, P. K. et Whelan, C. (2017). Introduction for special issue policing across organisational boundaries: developments in theory and practice. *Policing and society*, *27*(6), 583-585. https://doi.org/10.1080/10439463.2017.1356300

ElBahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A. et Baronchelli, A. (2020). Collective dynamics of dark web marketplaces. *Scientific reports*, *10*(1), 1-8.

Emerson, K. et Nabatchi, T. (2015). *Collaborative governance regimes*. Georgetown University Press.

Epstein, E. J. (1990). *Agency of fear: Opiates and political power in America*. Verso.

European Union (2022). Agence de l'Union européenne pour la coopération des services répressifs (Europol). https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_fr

Europol (2022). *European Cybercrime Centre - EC3 : Combating Crime in a digital age.* About Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol (2023, 2 mai). *288 dark web vendors arrested in major marketplace seizure.* Europol Media & Press. https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Europol (2023). *Joint Cybercrime Action Taskforce (J-CAT).* Operations, Services & Innovation. https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce

Faizan, M. et Khan, R. A. (2019). Exploring and analyzing the dark Web: A new alchemy. *First Monday*, *24*(5). https://doi.org/10.5210/fm.v24i5.9473

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J. et Dupont, B. (2021). Law enforcement and disruption of offline and online activities: a review of comptemporary challenges. *Cybercrime in context: the human factor in victimization, offending, and policing,* 351.

Finkelstein, L. S. (1995). What is global governance. *Global governance*, *1*, 367.

Fleming, J. et Rhodes, R. (2018). Can experience be evidence? Craft knowledge and evidence-based policing. *Policy & politics*, *46*(1), 3-26.

Fooner, M. (1989). *Interpol. Issues in world crime and international justice*. Plenum Press.

Fox, B., Miley, L. N., Allen, S., Boness, J., Dodge, C., Khachatryan, N., ... et Rozo, M. (2020). Law enforcement and academics working together on cold case investigations: lessons learned and paths forward. *Journal of Criminal Psychology*, *10*(2), 93-111.

Frank, R., Thomson, M., Mikhaylov, A. et Park, A. J. (2018). Putting all eggs in a single basket: A cross-community analysis of 12 hacking forums. Dans *2018 IEEE international conference on intelligence and security informatics (ISI)* (pp. 136-141). IEEE. DOI:10.1109/ISI.2018.8587322

Futter, A. (2018). 'Cyber' semantics: Why we should retire the latest buzzword in security studies. *Journal of Cyber Policy, 3*(2), 201-216.

Gavin, H. (2008). Thematic analysis. Understanding research methods and statistics in psychology, 3(2), 273-282.

Gendarmerie Royale du Canada (2015). *Stratégie de lutte contre la cybercriminalité de la gendarmerie royale du Canada.* GRC. https://www.rcmp-grc.gc.ca/wam/media/1089/original/e1a9d988ea543658c8ea1463d588c6b0.pdf

Gerspacher, N. et Dupont, B. (2007). The nodal structure of international police cooperation: an exploration of transnational security networks. *Global Governance, 13*(3), 347-364.

Ghiglione, R. et Matalon, B. (1978). *Comment interroger? Les entretiens. Les enquêtes sociologiques: théories et pratiques*. Armand Colin.

Gordon, F., McGovern, A., Thompson, C. et Wood, M. A. (2022). Beyond Cybercrime: New Perspectives on Crime, Harm and Digital Technologies. *International Journal for Crime, Justice and Social Democracy*, *11*(1). https://doi.org/10.5204/ijcjsd.2215

Gouvernement du Canada (2023). Mutual Legal Assistance in Criminal Matters Act (R.S.C., 1985, c. 30 (4th Supp.)). Justice Law Website. https://laws-lois.justice.gc.ca/eng/acts/M-13.6/

Graham, E. (1997). Philosophies Underlying Human Geography Research. Dans Flowerdew, R. et Martin, D. (Dir.) *Methods in Human Geography: A Guide for Students Doing a Research Project,* Longmans, 6-30.

Greenberg, A. (2014). *Hacker Lexicon: What Is the Dark Web?* WIRED. https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/#:~:text=The%20Dark%20Web%20is%20a,users%20from%20surveillance%20and%20censorship.

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

Hadlington, L., Lumsden, K., Black, A. et Ferra, F. (2018). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: An International Journal of Police Strategies & Management*, *15*(1), 1-10. https://doi.org/10.1093/police/pay090

Harkin, D. et Whelan, C. (2022). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management*, *24*(1), 66-76. https://doi.org/10.1177/14613557211036565

Harkin, D., Whelan, C. et Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research, 19*(6), 519-536. doi:10.1080/15614263.2018.1507889

Haslebacher, A., Onaolapo, J. et Stringhini, G. (2017). All your cards belong to us: Understanding online carding forums. *IEEE Conference.* doi: 10.1109/ECRIME.2017.7945053.

Heikkila, T. et Gerlak, A. (2015). Collaboration dynamics: Principled engagement, shared motivation, and the capacity for joint action. *Collaborative governance regimes*, 57-80.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. *International Journal of Cyber Criminology*, *1*, 1-26. https://doi.org/10.5281/zenodo.18275

Holloway, L. et Hubbard, P. (2001). *People and Place – The Extraordinary Geographies of Everyday Life.* Pearson education limited.

Holt, K., Rojek, A., Mason, M. et Rothman, L. (2022). "Who is Where?" Cold Case Investigation and Collaborations Between Law Enforcement and Academia. *Homicide Studies*.

Holt, T. J. et Lee, J. R. (2022). A crime script model of Dark web Firearms Purchasing. *American Journal of Criminal Justice,* 1-21. https://doi.org/10.1007/s12103-022-09675-8

Holt, T., 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. https://doi.org/10.1080/17440572.2015.1013211

Holt, TJ., Bossler, AM. (2012a). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice, 37*(3), 396–412.

Holt, TJ., Bossler, AM. (2012b). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 464–472.

Horsman, G. (2017). Can we continue to effectively police digital crime. *Science and Justice, 57*(6), 448-454.

Horst, H.A. et Miller, D. (2020). *Digital anthropology*. Abingdon: Routledge. Https://Go.Chainalysis.Com/Rs/503-FAP-074/Images/2020-Crypto-Crime-Report.Pdf.

Internet Crime Complaint Center (IC3) (2020). *Internet Crime Report 2020.* Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Interpol (2017). *Cybercriminalité*. https://www.interpol.int/Crimes/Cybercrime

Interpol (2022). *Qu'est-ce qu'INTERPOL?* https://www.interpol.int/fr/Qui-nous-sommes/Qu-est-ce-qu-INTERPOL

Inyang, J. D. et Abraham, U. E. (2013). Policing Nigeria: A case for partnership between formal and informal police institutions. *Merit Research Journal of Art, Social Science and Humanities*, *1*(4), 53-58.

Jardine, E. (2021). Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice, 46*(6), 980-1005. https://doi.org/10.1007/s12103-021-09656-3

Johnston, L. (2005). *The rebirth of private policing*. Routledge.

Jones, T. et Newburn, T. (2006). *Plural policing: A comparative perspective*. Routledge.

Jurgenson, N. (2012). When atoms meet bits: Social media, the mobile web and augmented revolution. *Future Internet, 4*(1), 83-91. https://doi.org/10.3390/fi4010083

Kaspersky (2023). *What is an IP Address – Definition and Explanation*. https://www.kaspersky.ca/fr

Kaur, S. et Randhawa, S. (2020). Dark Web: A Web of Crimes. *Wireless Personal Communications, 112*. https://doi.org/10.1007/s11277-020-07143-2

Keast, R., Brown, K. et Mandell, M. (2007). Getting the right mix: Unpacking integration meanings and strategies. *International Public Management Journal, 10*(1), 9-33. https://doi.org/10.1080/10967490601185716

Keast, R., Mandell, M. P., Brown, K. et Woolcock, G. (2004). Network structures: Working differently and changing expectations. *Public administration review, 64*(3), 363-371.

Kim, B., Gerber, J., Beto, D. R. et Lambert, E. G. (2013). Predictors of Law Enforcement Agencies' Perceptions of Partnerships with Parole Agencies. *Police Quarterly, 16*(2), 245–269. https://doi.org/10.1177/1098611113477646

Kim, S. et Lee, H. (2006). The impact of organizational context and information technology on employee knowledge-sharing capabilities. *Public Administration Review, 66*, 370-385.

Koops, B.-J. (2013). Police investigations in Internet open sources: Procedural-law issues. *Computer Law & Security Review, 29*(6), 654-665. https://doi.org/10.1016/j.clsr.2013.09.004

Kreiner, K. et Schultz, M. (1993). Informal collaboration. Dans R et D. The formation of networks across organizations. *Organization studies, 14*(2), 189-209.

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.

Lambert, D. E. (2019). Addressing challenges to homeland security information sharing in American policing: Using Kotter's leading change model. *Criminal Justice Policy Review, 30(*8), 1250–1278.

Lammers, M. et Bernasco, W. (2013). Are mobile offenders less likely to be caught? The influence of the geographical dispersion of serial offenders' crime locations on their probability of arrest. *European Journal of Criminology, 10*(2), 168–186.

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

Lavers, J. et Chu, Y.-K. (1997). Informal police cooperation: the fight against international crime. *The Police Journal: Theory, Practice and Principles, 70*(2), 127–132. https://doi.org/10.1177/0032258X9707000206

Lavoie, P.-É., Fortin, F. et Tanguay, S. (2013). Problèmes relatifs à la définition et à la mesure de la cybercriminalité. Dans F. Fortin (dir.), *Cybercriminalité : Entre inconduite et crime organisé*. Presses internationales Polytechnique.

Legard, R., Keegan, J. et Kit, W. (2003). In-depth Interviews. Dans J. Ritchie et J. Lewis (dir.), *Qualitative research practice: a guide for social science students and researchers* (p. 138-169). Thousand Oaks, SAGE.

Lemieux, F. (2010). *International Police Cooperation: Emerging issues, theory and practice*. William Publishing.

Lemieux, F. (2014). Challenges posed by existing and emerging forms of international police cooperation. Report prepared for *the International Sociological Association, 2014 United Nations Conference*. Vienna, Austria.

Lemieux, F. (2015). Inside the global policing system: Liaison officers deployed in Washington, DC. *Global Governance: A Review of Multilateralism and International Organizations, 21*(1), 161–180.

Lemieux, F. (2018). Police Cooperation Across Jurisdictions. *Oxford Research Encyclopedia of Criminology.*

Leukfeldt, E. R., Veenstra, S. et Stol, W. (2013). High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *International journal of Cyber Criminology, 7*(1), 1-17.

Leukfeldt, ER, Notté RJ, Malsch M (2020) Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims and Offenders* 15(1): 60–77.

Lum, C. et Koper, C. S. (2015). Evidence-based policing. *Critical Issues in Policing: Contemporary Readings*, 260-274.

Lum, C. M. et Koper, C. S. (2017). *Evidence-based policing: Translating research into practice*. Oxford University Press.

Lupton, D. (2015). *Digital sociology*. Routledge.

Macdonald, K. (2020). *Cybercrime: Awareness, Prevention and Response.* Emond Montgomery Publications Limited.

Mandel, R. (2011). *Dark logic: transnational criminal tactics and global security*. Stanford Security Studies.

Mandell, M. P. (2001). *Getting results through collaboration: Networks and network structures for public policy and management*. Praeger.

Marres, N. (2017). *Digital sociology: The reinvention of social research*. Cambridge: Polity Press.

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

Mattessich, P., Murray-Close, M. et Monsey, B. (2001). *Collaboration: What makes it work?,* Wilder Foundation.

Mazeika, D., Bartholomew, B., Distler, M., Thomas, K., Greenman, S. et Pratt, S. (2010). Trends in Police Research: A Cross-Sectional Analysis of the 2000-2007 Literature. Police *Practice and Research: An International Journal, 11*(6), 520-547. https://doi.org/10.1080/15614263.2010.497390

Mazerolle, L., Soole, D. et Rombouts, S. (2007). Drug Law Enforcement. *A review of the Evaluation Literature, Police Quarterly, 10* (2), 115-153. https://doi.org/10.1177/1098611106287776

McGuire, M. (2007). *Hypercrime: The new geometry of harm*. Routledge. https://doi.org/10.4324/9780203939529

McNamara, M. (2012). Starting to Untangle the Web of Cooperation, Coordination, and Collaboration: A Framework for Public Managers. *International Journal of Public Administration, 25*(6). https://doi.org/10.1080/01900692.2012.655527

Michelat, G. (1975). Sur l'utilisation de l'entretien non directif en sociologie. *Revue française de sociologie, 16*(2), 229-247. doi:10.2307/3321036

Miles, M. B., Huberman, A. M. et Saldana, J. (2014). Qualitative Data Analysis, A Methods Sourcebook (3e éd.). Thousand Oaks, CA: SAGE.

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.

Mirea, M., Wang, V. et Jung J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal, 32*, 102–118. https://doi.org/10.1057/s41284-018-0150-5

Moore, D. et Rid, T. (2016). Cryptopolitik and the Darknet. *Survival, 58*(1), 7-38. https://doi.org/10.1080/00396338.2016.1142085

Moore, R. (2015). *Cybercrime: Investigating High-Technology Computer Crime*. 2e edition. Routledge. Taylor & Francis Group.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S. et Voelker, G. (2011). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference*, 71- 80. https://doi.org/10.1145/2068816.2068824

Mulford, C. L. et Rogers, D. (1982). Definitions and Models. Dans D. L. Rogers et D. A. Whetten (dir.), *Organizational Coordination: Theory, Research and Implementation* (pp. 9-31). Iowa State University Press.

Munksgaard, R., Décary-Hétu, D., Malm, A. et Nouvian, A. (2021). Distributing tobacco in the dark: assessing the regional structure and shipping patterns of illicit tobacco in cryptomarkets. *Global Crime*, *22*(1), 1-21. https://doi.org/10.1080/17440572.2020.1799787

Nadelmann, A, E. (1993). *Cops across borders: The Internationalization of U.S. Criminal Law Enforcement.* Pennsylvania State University Press.

Naseem, I., Kashyap, A. K. et Mandloi, D. (2016). Exploring anonymous depths of invisible web and the digi-underworld. *International Journal of Computer Applications, 3*, 21–25.

National Police Chief Council (NPCC). (2020). *Digital forensics science strategy.* https://www.npcc.police.uk/FreedomofInformation/Reportsreviewsandresponsestoconsultations.aspx.

Nations Unies (2023a, 20 avril). *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Fifth session*, Vienna, 11-21. https://docdro.id/u6XwKHJ

Nations Unies (2023b). *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

New Zealand Government (2020, 15 juillet). *What is the Budapest Convention?* https://consultations.justice.govt.nz/policy/budapest-convention

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

Notté, R., Leukfeldt, E.R. et Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology,* 27(3): 272–294.

Nowacki, J. et Willits, D. (2020). An organizational approach to understanding police response to cybercrime. *Policing: An international journal, 43*(1), 63-76.

O'neill, J. (2001). Building better global economic BRICs. *Global Economics Paper* (66).

O'Leary, R. et Vij, N. (2012) Collaborative public management: Where have we been and where are we going? *The American Review of Public Administration, 24*(5): 507–522.

O'Reilly, C. A., Caldwell, D. F., Chatman, J. A. et Doerr, B. (2014). The promise and problems of organizational culture: CEO personality, culture, and firm performance. *Group & Organization Management, 39*, 595-625.

O'Reilly, C. A., Chatman, J. A. et Caldwell, D. F. (1991). People and organizational culture: A profile comparison approach to assessing person-organization fit. *Academy of Management Journal, 14,* 487-516.

Paek, S.Y., Nalla, M.K., Chun, Y.T. et Lee, J. (2021). The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage. *Sustainability, 13*(8), 4351.

Paillé, P. et Mucchielli, A. (2012). Chapitre 11 - L'analyse thématique. Dans P. Paillé et A. Mucchielli (dir.), *L'analyse qualitative en sciences humaines et sociales, 2*, 31- 314. Armand Colin. https://doi.org/10.3917/arco.paill.2012.01.0231

Pettigrew, A. M. (1979). On studying organizational cultures. *Administrative Science Quarterly, 24*, 570-581.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S. et Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*(2), 379-398.

Pickering, J. C. et Fox, A. M. (2022). Enabling Collaboration and Communication Across Law Enforcement Jurisdictions: Data Sharing in a Multiagency Partnership. *Criminal Justice Policy Review, 33*(7). https://doi.org/10.1177/08874034211066756

PMI Impact (2023). *Combating illegal trade, together*. https://www.pmi-impact.com/home/

Polenske, K. R. (2012). *Competition, collaboration and cooperation: an uneasy triangle in networks of firms and regions* (pp. 45-60). Routledge.

Pomerleau, P. L. (2019). *Countering the Cyber Threats Against Financial Institutions in Canada: A Qualitative Study of a Private and Public Partnership Approach to Critical Infrastructure Protection* (Doctoral dissertation, Northcentral University).

Pomerleau, P.L. et Lowery, D.L. (2020). *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection.* Springer Nature.

Pool, R. L. D. et Custers, B. H. M. (2017). The police hack back: Legitimacy, necessity and privacy implications of the next step in fighting cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice, 25*, 123-144.

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*. Gaëtan Morin éditeur.

Prince, H., Lum, C. et Koper, C.S. (2021). Effective police investigative practices: an evidence-assessment of the research. *Policing: An International Journal,* 44(4), 683-707. https://doi.org/10.1108/PIJPSM-04-2021-0054

Pritchard, D. (2008). Knowing the Answer, Understanding and Epistemic Value. *Grazer Philosophische Studien - Internationale Zeitschrift für Analytische Philosophie*, *77*, 325-339. doi:10.1163/18756735-90000852

Radzinowicz, L. (1956). *History of English Criminal Law and Its Administration from 1750* (vol. 3). Stevens.

Ratcliffe, J. H. (2007). *Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders*. Police Foundation.

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

Raustiala, K. (2002). The Architecture of International Cooperation: Transgovernmental Networks and the Future of International Law. *Virginia Journal of International Law, 43*(1), 63-64.

Rhumorbarbe, D., Staehli, L., Broséus, J., Rossy, Q. et Esseiva, P. (2016). Buying drugs on a Darknet market: A better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic science international, 267*, 173-182.

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

Ritchie, J., Spencer, L. ry O'Connor, W. (2003). Carrying out qualitative analysis. *Qualitative research practice: A guide for social science students and researchers*, 219-62.

Roberson, C., Das, D, K. et Singer, J. (2010). *Police without borders: The Fading Distinction Between Local and Global.* CRC Press Taylor & Francis Group.

Rogers, C. (2016). *Plural policing: Theory and practice*. Policy Press.

Ross, J. (2010). Foreword. Dans M.D. Bayer (dir.), *The blue planet: Informal international police networks and national intelligence* (pp. vii – xi). Government Printing Office.

Rothe, D. et Friedrichs, D. O. (2015). *Crimes of globalization*. Routledge.

Roulston, K. et Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Qualitative Inquiry, 21*(4), 332–342.

Royal Canadian Mounted Police (2015). Stratégie de lutte contre la cybercriminalité de la gendarmerie royale du Canada. GRC. https://www.rcmp-grc.gc.ca/wam/media/1089/original/e1a9d988ea543658c8ea1463d588c6b0.pdf

Rudolph, P.A. et Kleiner, B.H. (1998). The Art of Motivating Employees. Journal of Managerial Psychology, 4(5), i-iv. Cité dans Mullins, L.J. (2002). *Management and Organisational Behaviour,* (6). FT Prentice Hall.

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

Sanders, C. B. et Henderson, S. (2013). Police 'empires' and information technologies: uncovering material and organisational barriers to information sharing in Canadian police services. *Policing and society*, *23*(2), 243-260.

Sarre, R., Yiu-Chung Lau, L. et Chang, L. (2018) Responding to cybercrime: current trends. *Police Practice and Research*, 19(6), 515-518, DOI: 10.1080/15614263.2018.1507888

Schaefer-Morabito, M. (2010). Understanding community policing as an innovation: Patterns of adoption. *Crime & Delinquency, 56*(4), 564–587.

Schein, E. H. (1992). *Organizational culture and leadership*. Jossey-Bass.

Scott, R. J. et Boyd, R., 2020. Determined to succeed: Can goal commitment sustain interagency collaboration. *Public Policy and Administration*, 1-31.

SCRS (2023). *Service canadien de renseignement de sécurité.* https://www.canada.ca/fr/service-renseignement-securite.html

Sécurité publique Canada (2021). *Réunion ministérielle des cinq pays.* https://www.securitepublique.gc.ca/cnt/ntnl-scrt/fv-cntry-mnstrl-fr.aspx

Sedgwick, D. et Hawdon, J. (2019). Interagency cooperation in the era of homeland policing: Are agencies answering the call? *American Journal of Criminal Justice, 44*, 167–190.

Shearing, C. D. et Stenning, P. C. (1983). Private security: implications for social control. *Social problems, 30*(5), 493-506.

Sheptycki, J. (2004). Organizational pathologies in police intelligence systems: Some contributions to the lexicon of intelligence-led policing. *European Journal of Criminology, 1*(3), 307–332. DOI: 101177/1477370804044005

Sherman, L. W. (1998). *Evidence-based policing* (p. 15). Police Foundation.

Sherman, L. W. (2013). The rise of evidence-based policing: Targeting, testing, and tracking. *Crime and justice*, *42*(1), 377-451.

Simons, H. (2009), *Case Study Research in Practice*. Sage Publications.

Sinclair, R., Duval, K. et Fox, E. (2015). Strengthening Canadian law enforcement and academic partnerships in the area of online child sexual exploitation: The identification of shared research directions. *Child & Youth Services*, *36*(4), 345-364.

Slaughter, A-M. (2004). Sovereignty and Power in a Networked World Order. *Stanford Journal of International Law, 40*, 283-327.

Soska, K. et Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. *24th USENIX Security Symposium (USENIX Security 15)*, 33-48.

Stenning, P. et Shearing, C. (2012). The shifting boundaries of policing: Globalisation and its possibilities. Dans T. Newburn et J. Peay (dir.), *Policing: Politics, culture and control* (pp. 265–284). Hart.

Stuenkel, O. (2020). *The BRICS and the future of global order*. Lexington books.

Taylor, R. et Russell, A. (2012). The failure of police "fusion" centers and the concept of a national intelligence sharing plan. *Police, Practice, & Research, 13*, 184–200.

Tewksbury, R. (2009). Qualitative versus quantitative methods: Understanding why qualitative methods are superior for criminology and criminal justice. *Journal of Theoretical and Philosophical Criminology, 1*(1).

Thomas, D.R. (2006). A general inductive approach for analysing qualitative evaluation data. *American Journal of Evaluation, 27*(2), 237-246.

Thomson, A.M. et Perry, J. (2006). Collaboration processes: Inside the black box. *Public Administration Review, 66,* 20–32.

Toure, H. et Mef, F. U. (2011). *International Telecommunication Union.* ICT Statistics.

Tremblay, M. (2009, décembre). *Réseaux de coopération policière internationale à l'ère de la mondialisation* (Rapport 8). École nationale d'administration publique. https://cerberus.enap.ca/leppm/docs/Rapports_securite/Rapport_8_securite.pdf

Tsuchiya, Y. et Hiramoto, N. (2021). Dark web in the dark: Investigating when transactions take place on cryptomarkets. *Forensic Science International: Digital Investigation, 36*. https://doi.org/10.1016/j.fsidi.2020.301093

Tun, T., Price, B., Bandara, A., Yu, Y. et Nuseibeh, B. (2016). Verifiable Limited Disclosure: Reporting and Handling Digital Evidence in Police Investigations. *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, 102-105. https://doi.org/10.1109/REW.2016.032

Turgeman-Goldschmidt, O. (2005). Hackers accounts: hacking as a social entertainment. *Social Science Computer Review, 23*(8), 8-23. https://doi.org/10.1177/0894439304271529

Turgeman-Goldschmidt, O. (2011). Identity construction among hackers. *Cyber criminology: Exploring Internet crimes and criminal behavior*, 31-51.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy, 56*, 176-186. https://doi.org/10.1016/j.drugpo.2018.01.022

Tzanetakis, M., Kamphausen, G., Werse, B. et Von Laufenberg, R. (2015). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy, 35*, 58-68. https://doi.org/10.1016/j.drugpo.2015.12.010

Union européenne (2022). *Agence de l'Union européenne pour la coopération des services répressifs (Europol).* https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_fr

United States Attorney's Office (2021, 3 mai). *Operation Ceasefire and the Safe Community Partnership*. https://www.justice.gov/usao-ndca/operation-ceasefire-and-safe-community-partnership

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. https://doi.org/10.1016/j.drugalcdep.2017.01.004

Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R. et Burns, L. (2016). Who sells what? Country specific differences in substance availability on the Agora cryptomarkets.

International Journal of Drug Policy, 35, 16-23. https://doi.org/10.1016/j.drugpo.2016.07.004

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

Van Slobbe, J. (2016) The drug trade on the deep web: a law enforcement perspective**.** Dans EMCDDA insights, *The internet and drug markets*, 77-83. Publications Office of the European Union. https://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf

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

Verbeek, P-P. (2005). *What things do: Philosophical reflections on technology, agency, and design*. University Park: Pennsylvania State University Press

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183-194. https://doi.org/10.1080/15614263.2015.1128163

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age* (Vol. 4). Cambridge: Polity.

Wall, D. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology*, *22*(1-2), 45–63.

Wall, D. S. (2007a). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wall, D. S. (2007b). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research, 8*(2), 183-205.

Wang, S.-Y. K., Hsieh, M.-L., Chang, C. K.-M., Jiang, P.-S. et Dallier, D. J. (2020). Collaboration between Law Enforcement Agencies in Combating Cybercrime: Implications of a

Taiwanese Case Study about ATM Hacking. *International Journal of Offender Therapy and Comparative Criminology, 65*(4), 390–408. https://doi.org/10.1177/0306624X20952391

Warren, R. L., Rose, S. M. et Bergunder, A. F. (1974). *The structure of urban reform: Community decision organizations in stability and change.* Lexington Books.

Weare, C., Lichterman, P. et Esparza, N. (2014). Collaboration and culture: Organizational culture and the dynamics of collaborative policy networks. *Policy Studies Journal, 42*, 590-619.

Wexler, C. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime.*

Whelan, C. (2012). *Networks and National Security: Dynamics, Effectiveness and Organisation*. Ashgate.

Whelan, C. (2017). Managing dynamic security networks: Towards the strategic managing of cooperation, coordination and collaboration. *Security Journal, 30*, 310–327. https://doi.org/10.1057/sj.2014.20

Whelan, C. et Dupont, B. (2017). Taking stock of networks across the security field: a review, typology and research agenda. *Policing and Society, 27*(6), 671-687. DOI: 10.1080/10439463.2017.1356297

White, R. (2011). Environmental law enforcement: The importance of global networks and collaborative practices. *Australasian Policing, 3*(1), 12–16. https://search.informit.org/doi/10.3316/informit.935090957550992

Whitford, A., Lee, S.-Y., Yun, T. et Jung, C. (2010) Collaborative behavior and the performance of government agencies. *International Public Management Journal, 13*(4), 321–349.

Wilson-Kovacs, D. (2021). Digital media investigators: challenges and opportunities in the use of digital forensics in police investigations in England and Wales. *Policing: An International Journal, 44*(4), 669-682. https://doi.org/10.1108/PIJPSM-02-2021-0019

Wilson, D. et Purushothaman, R. (2003). Dreaming with BRICs: The path to 2050. *Global economics paper*, (99), 1.

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

Zhang, J. et Dawes, S. S. (2006). Expectations and perceptions of benefits, barriers, and success in public sector knowledge networks. *Public Performance & Management Review, 29*, 433-466.

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

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

Zulkarnine, A. T., Frank, R., Monk, B., Mitchell, J. et Davies, G. (2016). Surfacing collaborated networks in dark web to find illicit and criminal content. Dans *2016 IEEE Conference on Intelligence and Security Informatics (*ISI) (pp. 109-114). IEEE.

Annexe A: Description de l'échantillon secondaire

Descriptive characteristics	Statistics
Gender:	
Female	6 (30%)
Male	14 (70%)
Age (Mean):	46 years old [range: 33-59]
Missing	1 (5%)
Education:	
Master's degree	3 (15%)
Bachelor's degree	11 (55%)
Collegial degree	2 (10%)
High School degree	3 (15%)
Missing	1 (5%)
Years of experience in policing (Mean):	20 years [range: 12-37]
Missing	0 (0%)
Rank/role:	
Investigator/Inspector	14 (70 %)
Chef Inspector/Sergeant Investigator	6 (30 %)
Missing	0
Country:	
Canada	9 (45%)
United States	2 (10%)
United Kingdom	5 (25%)
Australia	3 (15%)
Sweden	1 (5%)
Work status:	
Still in law enforcement	18 (90%)
Retired	1 (5%)
Quit law enforcement	1 (5%)
Interview time:	51:45 minutes [range: 29 :29 – 1 :12 :27]
Agency level:	
Provincial/Regional/State	7 (35%)
Municipal/Local	7 (35%)
Federal/National	2 (10%)
Mixed responsibilities	2 (10%)
Others	2 (10%)

Annexe B: Guide d'entretiens

Disrupting The Darknet: Law Enforcement Operations and Their Impact On Darknet Offenders

Interview Guide

*Please complete demographic information before or after the interview

Research objective:
To assess the perceptions of law enforcement officers on the impact of their interventions on darknet markets[28].

More specifically, using interviews, we will discuss how police interventions are designed, what their aims were, whether there are constraints on the police interventions and how they unfold and focus on targets.

Section 1: Intervention design

- Please explain your career path that brought you to work in the regulation of Darknet illicit activities and cybercrime.
    - How much training had you received in Darknet operations?
- Please describe the last police intervention aiming to disrupt darknet market activities you participated in and can discuss. We are interested in hearing about:
    - The triggers that launched this police intervention (How did the intervention originate? What prompted the intervention?)
    - The aims of this police intervention (How were the targets chosen?)
    - The roles and responsibilities of those involved in the planning of the intervention, including those of people from outside your organization.
        - Collaborations with outside partners: other police forces, parapublic and private organisations and businesses
            - Who assigns the tasks? Does someone take the lead?
            - Approximately, how many people were involved?
    - The intervention techniques (IP addresses, going into servers? Or more traditional police investigation techniques such as wiretapping and interviews?)
    - The resources (human, financial, material) involved in the intervention (Were the resources provided sufficient?)
    - The constraints in the planning and launch of the intervention.
    - The outcome of the intervention (was it considered a success by the organization?)

[28] If participant has not participated in a police intervention on a darknet illicit market, the participant will be invited to talk about police operations targeting other online activities, or, alternatively, to talk about what their perception is of what their colleague have been doing in that space. In addition, they will be asked their perceptions as to why they have never participated in operations targeting darknet illicit markets and if they identify challenges that could explain why their organisation doesn't take part in or lead this type of operations. They will be inquired about what are, in their opinion, the skills lacking in their organisations to undertake such interventions.

Section 2: Intervention impacts

- Please describe the impacts of the last police intervention aiming to disrupt darknet market activities you participated in and can discuss. We are interested in hearing about:
  - The methods used to measure the impact (evaluation methods)
  - The general impacts of the intervention
  - The impacts on the size and scope of illicit transactions on darknet markets
  - The impacts on the structure of ties between darknet market participants
  - The period of time the impacts were felt (short-term VS long-term impacts)
  - The difference between the expected outcomes and the intervention real impacts
  - The impacts on other markets (ex. offline physical markets)
  - The perceived cost-effectiveness of the intervention

Section 3: Looking forward to future interventions.

- Please describe how you believe future interventions should be designed and what their likely impacts will be. We are interested in hearing about:
  - The frequency and intensity of future interventions
  - Specific improvements that should be made to interventions to maximize their impacts (What should you do differently next time?)
  - The size and scope of resources (human, financial, material) that are needed to improve interventions in the future.
- Since the 1960s, the police have shown a will to develop more effective strategies to prevent and disrupt crime, slightly abandoning the traditional unfocused paradigm to test hot spots policing, crackdowns, community policing and problem-oriented policing. Research seems to conclude, in broad terms, that problem-oriented policing (including intelligence-led policing and focused-deterrence policing) seems to be the most effective police paradigm. Now that we know all this about the effectiveness of police strategies and have 50 years of studies on street crimes, can we possibly think of transposing these policing strategies to online crime? We are interested in hearing about:
  - How police could regulate the darknet with either a hot spot, a crackdown, a community-policing or a problem-oriented policing approach?
  - New and innovative models that should be implemented.
  - Is the prevention of Darknet illicit activities and cybercrime a focus or your organization? Are these techniques effective?