Intégrer la cybercriminalité aux activités de prévention de la délinquance : le défi des organisations policières locales

Par **Adeline VEYRINAS*** et **Benoît DUPONT****

RÉSUMÉ

Face à une délinquance en constante évolution, les forces de l'ordre sont tenues d'adapter leurs réponses et les ressources qu'elles mobilisent pour maintenir l'efficacité de leurs modes d'intervention, ce qui s'applique en premier lieu à la cybercriminalité. En raison de leur proximité avec la population, les policiers locaux en uniforme jouent un rôle majeur dans les activités de prévention, car ils informent et conseillent le public sur les caractéristiques des diverses formes de délinquance et sur les mesures de protection à adopter. Pourtant, les quelques recherches empiriques menées dans le domaine de la cybercriminalité ont montré que les agents de police disposent rarement d'un accès à des capacités suffisantes pour contrôler ce phénomène. Cependant, ces études se sont essentiellement consacrées aux activités d'enquête et ont négligé l'aspect préventif du travail policier. Il est donc nécessaire de mieux comprendre les défis auxquels sont confrontés les policiers spécialisés dans les activités de prévention afin de disposer d'une image complète de la situation. Grâce à la combinaison d'un sondage et d'entretiens approfondis avec des agents en uniforme et des enquêteurs spécialisés en cybercriminalité, cette étude décrit l'expérience d'un organisme local d'application de la loi canadien dans ses efforts d'offrir au public des activités et contenus de prévention de la cybercriminalité. Les résultats démontrent que les intervenants de première ligne expriment des besoins importants en termes de formation, de communication, et d'outils mis à leur disposition afin de soutenir leurs activités de prévention.

Mots clés: cybercrime, police, policing, formation policière, prévention, partenariats.

ABSTRACT

In the face of constantly evolving crime, law enforcement agencies are required to adapt their responses and resources to maintain the effectiveness of their intervention methods, and this applies primarily to cybercrime. Because of their proximity to the public, local uniformed police officers play a major role in prevention activities by informing and advising the public about the characteristics of various forms of crime and the protective measures to be adopted. Yet, the limited empirical research conducted in the area of cybercrime has shown that police officers rarely have access to sufficient capabilities to

* Chercheure boursière, Chaire de recherche en Prévention de la cybercriminalité, Centre international de criminologie comparée, Université de Montréal.

** Professeur titulaire, Centre international de criminologie comparée et École de criminologie, Titulaire de la Chaire de recherche du Canada en Cybersécurité et de la Chaire de recherche en Prévention de la cybercriminalité, Université de Montréal.

control this phenomenon. However, these studies have mainly focused on investigative activities and have neglected the preventive aspect of police work. Therefore, there is a need to better understand the challenges faced by police officers involved in prevention activities in order to have a comprehensive understanding of the situation. Through a combination of a survey and in-depth interviews with uniformed officers and cybercrime investigators, this study describes the experience of a local Canadian law enforcement agency in its efforts to provide the public with cybercrime prevention activities and content. The results show that front-line workers express significant needs in terms of training, communication, and tools available to them to support their prevention activities.

Keywords: Cybercrime, police, policing, police training, prevention, partnerships.

Alors que les criminologues développent des connaissances empiriques de plus en plus détaillées sur les différentes formes que prennent les cybercrimes, sur l'organisation de ceux qui les commettent et sur l'impact qu'ils produisent sur ceux qui en sont victimes, les recherches sur l'évolution des pratiques policières face à cette transformation de la délinquance restent parcellaires. Pourtant, il s'agit de la criminalité qui connaît la plus forte progression depuis les vingt dernières années et celle dont les préjudices financiers augmentent de manière considérable (Levi, 2017 ; Anderson et al., 2019). Par exemple, en 2018, au Royaume-Uni, 86 % des fraudes enregistrées avaient été commises aux moyens d'une technologie numérique (Karagiannopoulos, Sugiura & Kirby, 2019). Aux Etats-Unis, le nombre de plaintes liées à la cybercriminalité est passé d'environ 289 000 en 2015 à 468 000 en 2019 (FBI, 2019). Au Canada, 57 % des Canadiens reportaient avoir été victime d'un incident de cybercriminalité en 2018 (Statistique Canada, 2019).

Ainsi, bien qu'il fasse l'objet d'une préoccupation grandissante de la part des acteurs de la sécurité et de la population (Bossler & Holt, 2012 ; Dodge & Burruss, 2020 ; Hadlington, Lumsden, Black & Ferra, 2021 ; Holt, 2018), ce phénomène semble encore méconnu des services de police, en particulier en ce qui concerne ses caractéristiques et les façons de le combattre (Burruss, Howell, Bossler & Holt, 2020 ; Holt, Burruss & Bossler, 2018 ; Hull, Eze & Speakman, 2018 ; Lee, Holt, Burruss & Bossler, 2021). Pourtant, la dimension technologique et la rapidité de développement et d'évolution de la cybercriminalité rendent primordiales des connaissances et compétences adaptées de la part des services de police, s'ils veulent développer et mettre en œuvre des stratégies adéquates afin de contrôler ce phénomène. D'autant que ces services présentent des spécificités organisationnelles et de fonctionnement qu'ils doivent considérer dans l'intégration de ces activités nouvelles, comme des ressources budgétaires limitées et une difficulté historique à implanter rapidement des réformes organisationnelles durables.

En pratique, l'adaptation policière à la cybercriminalité concerne principalement les services d'enquête, notamment avec la création d'équipes

spécialisées et l'adoption d'outils et de compétences plus techniques (Dodge & Burruss, 2020). La prévention, c'est-à-dire le fait d'agir de manière proactive en essayant d'empêcher l'acte criminel d'être commis (Cusson, 2007a ; Welsh & Farrington, 2012), n'a pas reçu la même attention. Pourtant, la police assure un rôle central en la matière. Cela est particulièrement vrai pour les services de police locaux qui ont joué un rôle déterminant dans le développement de la police communautaire, particulièrement axée sur la prévention des infractions et le soutien aux citoyens (Quéro & Dupont, 2019). De ce fait, ils travaillent au plus près de la population pour l'aider et la conseiller afin de l'encourager à mieux se protéger des risques criminels. Ainsi, alors qu'ils sont moins dotés en termes de ressources que leurs homologues nationaux, on demande à ces services d'être préparés au mieux en la matière. La population fait d'ailleurs preuve d'une volonté importante d'être informée et rassurée par la police quant aux moyens de se prémunir des effets néfastes de la cybercriminalité (Accenture, 2017). Face à cette nouvelle réalité opérationnelle et à ces attentes de la population, il semble donc impératif que les policiers locaux soient préparés au mieux pour prévenir et contrôler ce phénomène, ce qui passe par l'évaluation des défis précis auxquels ils font face dans l'acquisition et l'utilisation de ces compétences.

C'est dans cette perspective que la présente recherche se situe. Elle s'intéresse aux défis relevés par les services de police locaux qui doivent s'adapter à l'apparition d'une « nouvelle » forme de criminalité, en privilégiant notamment l'expérience des intervenants de première ligne spécialisés en prévention. À travers l'analyse d'entrevues qualitatives et d'un sondage réalisé dans un service de police municipal canadien, nous examinons les pratiques mises en œuvre par les policiers spécialisés dans les missions de prévention de la délinquance afin de s'approprier les connaissances nécessaires à l'intégration des risques numériques dans leur mandat. Nous examinons leurs besoins, ainsi que les diverses stratégies mobilisées par ces derniers pour y répondre.

La prévention de la cybercriminalité en contexte policier

L'expansion de la cybercriminalité et son exposition médiatique ont créé un fort sentiment d'insécurité auprès de la population. Cela a ainsi entraîné une forte demande du public qui souhaite être mieux informé des caractéristiques de cette délinquance émergente et des moyens de s'en protéger (Accenture, 2017 ; Wall, 2008, 2010). Cependant, l'évolution rapide de la cybercriminalité présente d'importants défis de prise en charge aux organisations policières. Ainsi, celles-ci disposent de ressources générales limitées pour répondre à un phénomène dont l'évolution technique est si rapide et l'ampleur si étendue (Dupont, 2016 ; Webster & Drew, 2017). Comme mentionné précédemment, en pratique, les principales tentatives d'adaptation par les services de police ont été réalisées en enquête, rôle généralement

représentatif du volet répressif des fonctions policières. En matière de cybercriminalité, la réponse policière réactive et centrée sur le délinquant qui caractérise l'enquête criminelle est cependant exposée à de nombreuses contraintes, comme la difficulté d'identifier les suspects en raison de la nature transnationale des affaires ou d'obtenir des preuves en l'absence de ressources techniques spécialisées (Levi & al., 2015). Les activités de prévention de la cybercriminalité ont par contraste fait l'objet d'un intérêt moindre, en dépit de son efficacité prometteuse (Drew & Farrell, 2018).

Ainsi, quelques études se sont penchées sur les perceptions que les policiers américains en uniforme et anglais ont de la cybercriminalité, puisque ce sont les premiers intervenants auprès de la population dans ce type d'affaires. La cybercriminalité est généralement perçue comme un problème sérieux par ces policiers en ce qu'elle occupe une part de plus en plus importante de leur travail (Bossler & Holt, 2012 ; Holt & Bossler, 2011 ; Holt & al., 2018). Cependant, une forte proportion estime que s'occuper de ce type de crimes ne relève pas forcément de leur responsabilité immédiate (Bossler & Holt, 2012 ; Holt & Bossler, 2011 ; Holt & al., 2018). Cela peut notamment s'expliquer par le fait que ces crimes sont considérés comme étant moins « intéressants » et moins graves que les autres, du fait de leur dimension dématérialisée et des faibles taux de résolution qui leur sont associés (Holt & Bossler, 2011 ; Holt & al., 2018 ; Huey 2002 ; Powell & Henry, 2018). Également, ces policiers ne se sentent pas suffisamment préparés et seraient ambivalents quant au rôle qu'ils auraient à jouer en la matière (Burruss & al., 2020 ; Hadlington & al., 2021 ; Holt & Bossler, 2011 ; Holt & al., 2018). Ceci pourrait s'expliquer par un manque de formations et d'outils en la matière (Burruss & al., 2020 ; Cross, 2015 ; Cross & Blackshaw, 2015 ; Hadlington & al., 2021), ainsi que par l'absence de directives claires sur les méthodes d'intervention appropriées (Bossler & Holt, 2012 ; Bossler, Cross & Burruss, 2020 ; Holt & Bossler, 2011 ; Senjo, 2004). Ils rechercheraient alors l'appui d'experts pour soutenir leur rôle en patrouille (Hadlington & al., 2021) et augmenter leurs connaissances et compétences en cybercriminalité (Burruss & al., 2020). Cela dit, les études en la matière ont été réalisées auprès de policiers en uniforme qui ont généralement des fonctions, certes, de premier intervenant auprès de la population, mais aussi de pré-enquête en donnant des conseils à une victime potentielle, conservant des preuves, interrogeant des témoins, etc. (Hull et al., 2018). Ils jouent ainsi un rôle principalement orienté vers l'enquête qui peut requérir des connaissances et des besoins différents de ceux des agents principalement dédiés à la prévention.

Les études sur l'adaptation des organisations policières à la cybercriminalité se sont donc essentiellement concentrées sur les enquêtes criminelles et sur l'expérience des policiers de première ligne qui opèrent majoritairement sur un mode réactif. À notre connaissance, très peu de recherches ont considéré les missions de prévention, pourtant elles aussi essentielles afin de répondre à une problématique criminelle d'aussi grande ampleur. Cette recherche tente donc de combler ce déficit de connaissances en privilégiant l'expérience de policiers

spécialisés dans les tâches de prévention au sein d'une organisation policière canadienne intervenant à l'échelle locale, c'est-à-dire devant combiner des capacités d'enquête complexe avec un rôle de sécurité urbaine. L'objectif principal est de questionner les intervenants spécialisés en prévention sur leur expérience d'intégration de nouvelles formes de cyberdélinquance à leur répertoire d'expertise, et sur leur capacité perçue à répondre aux besoins de la population dans ce domaine.

Données et méthode

Les données ont été collectées au sein d'un service de police municipal canadien entre l'automne 2019 et l'hiver 2020 à l'aide de deux instruments. Tout d'abord, un questionnaire auto-administré portant sur le phénomène de la cybercriminalité et de sa prévention a été diffusé parmi les agents spécialisés en prévention au sein du service par la voie de son système de courriel interne. Ensuite, un groupe de discussion semi-dirigé a été organisé et des entrevues complémentaires ont été menées en personne dans les locaux de l'organisation.

Le recrutement a été effectué sur la base du volontariat en diffusant un appel à travers le courriel interne du service de police à l'ensemble des agents détenant des fonctions dédiées à la prévention, afin de répondre à un questionnaire et/ou participer à un groupe de discussion. Les enquêteurs spécialisés en cybercriminalité ont également été invités à des entrevues. Les questions du sondage portaient sur les expériences des participants en lien avec la prévention de la cybercriminalité, comme les formations reçues, leurs connaissances générales et la perception de leur rôle en la matière, ainsi que les activités menées. Le taux de réponse obtenu a été de 90 %, avec 54 questionnaires retournés pour 60 participants sollicités. Cependant, trois questionnaires ont été exclus des analyses pour des questions de consentement non confirmé (n = 1) ou un formulaire incomplet (n = 2). Concernant le groupe de discussion, pour des questions d'intérêt et de pertinence de l'entretien, une dizaine d'agents ayant exprimé leur intérêt au stade du questionnaire ont été conviés à une rencontre et sept se sont effectivement présentés. Les thématiques abordées portaient sur des enjeux plus opérationnels qui semblaient ressortir des résultats du questionnaire, comme leurs pratiques et activités en prévention de la cybercriminalité, les ressources et outils à leur disposition dans ce cadre, leurs perceptions quant aux compétences et formations reçues en la matière, ainsi que les interrelations nouées avec les autres acteurs de la cyber-prévention. Enfin, concernant les entrevues avec les enquêteurs spécialisés, l'ensemble de l'équipe s'est portée volontaire, mais pour des questions de pertinence et de temps, seulement cinq entretiens ont pu été réalisés. Les discussions ont essentiellement porté sur l'articulation entre les fonctions d'enquête et de prévention, notamment en matière de transferts de connaissances. Ainsi,

l'échantillon final pour le questionnaire était composé de 51 participants, dont 39 femmes et 11 hommes. Le tableau 1 décrit de manière plus détaillée la composition de l'échantillon.

Tableau 1 :
Profil de l'échantillon

		n	%
Méthode de collecte de données	Questionnaire Groupe de discussion Entretien individuel	51 7 5	81 11,1 7,9
	Total	63	100
Rôle	Agent Enquêteur	58 5	92,1 7,9
	Total	63	100
Sexe	Homme Femme Valeur manquante	17 45 1	27 71,4 1,6
	Total	63	100

Les instruments de mesure utilisés ont été créés en utilisant des questions adaptées de celles posées dans le cadre d'autres études, concernant principalement les perceptions et le rôle des policiers locaux sur le phénomène de la cybercriminalité, ainsi que les défis rencontrés par les services de police en général dans la lutte contre la cybercriminalité (e.g. Bossler & Holt, 2012 ; Burruss & al., 2020 ; Hadlington & al., 2021 ; Harkin & al., 2018 ; Hull & al., 2018 ; Holt & Bossler, 2011 ; Lee & al., 2021 ; Senjo, 2004). Le questionnaire comprenait 22 questions, dont 19 à choix de réponse et trois ouvertes. La durée de remplissage a été estimée à une quinzaine de minutes. La grille d'entrevue pour le groupe de discussion comprenait cinq thématiques à aborder (en plus du parcours de vie/professionnel des participants) et le groupe s'est exprimé pendant une heure et 35 minutes. La grille d'entrevue pour les entretiens avec les enquêteurs spécialisés comprenait cinq thématiques à aborder et la durée de chaque entretien était d'environ 40 minutes.

Les résultats du questionnaire ont été analysés à l'aide du logiciel SPSS (version 25). Pour les entretiens, une analyse qualitative thématique du discours des participants a été réalisée afin de faire ressortir les différents concepts abordés par ceux-ci. D'abord, un codage sur la base des concepts présents dans la grille d'entretien a été effectué en faisant ressortir des unités et dimensions de sens. Ensuite, une extraction des principaux thèmes a été faite en sélectionnant les données pertinentes pour répondre aux questions et objectifs de recherche abordés lors du groupe de discussion. De plus, une analyse statistique par analyse de fréquence a été réalisée quant aux éléments de ces thématiques afin de faire ressortir leur fréquence d'apparition dans la rencontre et également en fonction des différents participants.

Une adaptation indispensable, freinée par le manque de confiance des intervenants

Les données collectées par le biais du questionnaire viennent d'abord confirmer les résultats déjà identifiés dans la littérature concernant la perception des policiers quant à la cybercriminalité. Ainsi, les répondants de notre échantillon estiment que la cybercriminalité est un problème important (moyenne = 3,49 sur 4). Il en découle que la majorité des répondants estime que les services de police ont une responsabilité importante à jouer en prévention de la cybercriminalité (82,4 %), devant les organismes communautaires (35,3 %) et les entreprises (27,5 %). Toutefois, si les répondants plébiscitent les fonctions de prévention, ils semblent privilégier pour les remplir des policiers issus d'organisations nationales ou provinciales (41,2 %), ou ceux affectés à des unités d'enquête spécialisées (41,2 %), ces deux catégories n'étant pas mutuellement exclusives. Par contraste, ceux qui œuvrent au sein d'unités dédiées à la prévention de la délinquance dans des services municipaux (leurs homologues donc) semblent moins fréquemment cités avec seulement 31,4 % des réponses. Il en découle que la majorité des répondants (52,9 %) estiment qu'ils ne détiennent pas les compétences et les connaissances suffisantes pour conseiller la population sur les façons de se protéger contre la cybercriminalité. Pour comprendre ce manque de confiance dans leur capacité à intégrer cette nouvelle forme de délinquance à leur portfolio de tâches de prévention, il est indispensable d'analyser les entrevues et les expériences partagées par les policiers lors du groupe de discussion.

L'intégration de la cybercriminalité aux activités de prévention

La majorité des activités menées par les policiers spécialisés en prévention sont destinées à un jeune public et se déroulent dans des établissements scolaires allant du primaire au secondaire. Les parents des enfants auprès desquels les officiers interviennent sont également mentionnés comme un public clé. Certains participants ont également cité les personnes âgées comme prioritaires en matière de cybercriminalité. Les types de cybercrimes auxquels les policiers sont le plus confrontés varient selon les clientèles : ainsi, chez les jeunes, figurent principalement l'intimidation, les menaces et la diffamation, la pornographie juvénile, la diffusion d'images intimes, le proxénétisme, la prostitution, les agressions sexuelles et l'extorsion. Quant aux personnes âgées, les répondants ont mentionné la fraude et la maltraitance.

La plupart des tâches relatives à la cybercriminalité que réalisent les participants relèvent de l'offre de conseils et de recommandations à la population sur les façons de se protéger contre les dangers de ce phénomène (100 % des officiers ayant répondu au questionnaire) et le fait de communiquer et de coopérer avec des organismes communautaires agissant en prévention de celui-ci (49 % des officiers ayant répondu au questionnaire). La fréquence de ces activités demeure faible comparativement à celle des activités de prévention portant sur la criminalité traditionnelle. En effet, les répondants interviendraient environ deux fois par mois (médiane) auprès de leurs clientèles cible dans le cadre

des formations sur la prévention de la cybercriminalité, en privilégiant le recours à des supports écrits de sensibilisation comme des dépliants ou des présentations Powerpoint (43,1 %), des programmes d'intervention interactifs comme *Dare to Care* (25,5 %) visant à développer des compétences et des comportements particuliers, ou des contenus de sensibilisation interactifs accessibles en ligne comme des capsules vidéos (19,6 %). Il faut souligner que 41 % des répondants estiment ne pas disposer d'outils internes de prévention adaptés à la cybercriminalité, et qu'ils recourent alors à des ressources développées par des partenaires externes comme d'autres services de police ou des organismes sans but lucratif. Il s'agit alors principalement d'outils audiovisuels comme des vidéos ou des clips d'animation. Les répondants ont déclaré recevoir en moyenne 7,8 formations par an (médiane de 3,5) sur les diverses formes et les caractéristiques de la cybercriminalité, généralement dispensées par des enquêteurs spécialisés, mais seulement une séance par an consacrée aux stratégies de prévention (médiane de 0).

Une charge de travail en forte augmentation

Un enjeu mentionné à de multiples reprises lors des entretiens est le fait que les agents de police ne disposent pas du temps suffisant pour répondre à toutes les demandes d'activités de prévention de la cybercriminalité. Cette problématique d'une surcharge de travail a ainsi été mentionnée en tout 31 fois pendant le groupe de discussion par les sept officiers : « Euh puis effectivement les chiffres que vous avez donné ça, ça, ça, ça a vraiment un beau portrait parce qu'effectivement depuis deux ans, euh la cyber (…). Y'a deux ans au primaire, je parlais pas de ça. Puis, depuis l'année passée, puis cette année beaucoup là, j'ai des demandes pour faire des présentations, puis de la prévention à ce niveau-là. » (Agent 1)

Cette surcharge de travail se manifeste par un sentiment de surmenage (mentionné quatre fois), et une implication moindre dans les activités de prévention, faute de temps (mentionné quatre fois) : « Fak, on peut l'faire en une fois, mais c'est de l'accéléré là. T'sais c'est, on garoche le stock, puis ça finit... » (Agent 3). Cela semble entraîner une perception négative quant à l'augmentation du nombre d'activités en prévention de la cybercriminalité, ce qui pourrait à long terme éroder leur volonté et leur motivation de s'impliquer plus dans ce domaine : « C'est ça qu'est le pire là. C'est que si on commence à en régler plus, il va y en avoir encore plus qui vont nous en parler. » (Agent 5)

Ainsi, les spécificités liées à la cybercriminalité, telles que sa dimension « fluide » et son évolution constante, semblent contribuer à la surcharge de travail des policiers remplissant des fonctions de prévention. En effet, cela nécessite une adaptation rapide des ressources existantes (par ailleurs déjà limitées) à l'évolution du phénomène et à la demande du public.

Des connaissances et des outils insuffisants

Une problématique importante rapportée par les policiers est le manque et l'inadéquation des outils disponibles pour soutenir leurs activités en prévention de la cybercriminalité (cité 24 fois par sept agents) : « T'es comme à (...) tu fais

ce que tu veux, tu présentes ce que tu veux. Ils veulent pas savoir ce qu'on fait dans les écoles. Ils savent bien qu'à la base on fait des présentations. Ils nous en fournissent pas. On n'a pas le droit d'en faire, mais ils nous en fournissent pas. Ils pensent qu'on fait quoi ? Fak, ils le savent, mais ils veulent pas le savoir. » (Agent 4)

Plus précisément, les officiers ont fait référence à plusieurs sous-problématiques en la matière : outils manquants (peu et principalement des power-points), outils inadaptés ou pas efficaces (trop longs, trop statiques, pas représentatifs de la clientèle), outils désuets, et outils difficiles à localiser, décentralisés ou pas répertoriés.

Les participants ont pu ainsi partager des suggestions sur les méthodes et les outils qui semblaient faciliter la sensibilisation du public et bénéficier d'un accueil positif auprès de ce dernier. Cependant, faute de connaissances théoriques sur ce qui est efficace et de données probantes, ils se basent essentiellement sur leur ressenti informel et leur expérience de praticien, afin de déterminer ce qui est susceptible de retenir l'attention de leur clientèle.

Les agents de police expriment un important besoin de connaissances sur la cybercriminalité et sa prévention (thème mentionné 17 fois par cinq officiers). Plus précisément, ils pointent un manque de connaissances techniques sur certains aspects de la cybercriminalité (cité neuf fois par cinq officiers) : « C'est, c'est ça que je trouve difficile un peu. C'est qu'on a à travailler en prévention, on a à faire de l'intervention avec ces jeunes-là qui utilisent des choses qu'on ne connaît même pas nous même… » (Agent 6). Ce déficit de connaissance concerne principalement trois aspects : les tendances récentes en matière de cybercriminalité telles que les plateformes émergentes (ex : TikTok) et les modes opératoires des délinquants (ex : hameçonnage) ; le jargon technique utilisé par les jeunes usagers comme les « nudes », les « memes », le « scam », le « dark web » ou encore le « black market » ; et enfin les stratégies/méthodes de prévention ayant fait la preuve de leur efficacité.

Cette problématique du manque de connaissances par les agents est confirmée par les cyberenquêteurs qui se montrent favorables à l'intégration de ressources spécialisées en prévention qui pourraient diffuser leurs connaissances ainsi que leur expertise technique, juridique ou policière dans le domaine. Par conséquent, le déficit de connaissances de base en cybercriminalité parmi les policiers en uniforme, qui par ailleurs sont souvent les premiers répondants sur les scènes de crime (afin de préserver la preuve, conseiller les victimes, prendre les témoignages, etc.), semble à la base de plusieurs problématiques, telles que la banalisation du phénomène, une mauvaise sauvegarde de la preuve et un sentiment de manque de préparation. Cela serait alors de nature à les rendre moins enclins et capables de prendre d'initiatives dans le domaine et ainsi freiner l'efficacité de leur organisation. En effet, un des grands enjeux rencontrés par les cyberenquêteurs est le recueil et le traitement fiable de la preuve pour contribuer à la condamnation de l'auteur présumé d'une infraction de cybercriminalité.

En résumé, bien que les policiers spécialisés dans les missions de prévention estiment que la cybercriminalité est un phénomène en expansion, ils ne disposent pas des connaissances adéquates sur les caractéristiques spécifiques de celle-ci, qu'il s'agisse des tendances les plus récentes en la matière ou des profils des auteurs et des victimes. Cela peut alors influencer les priorités qu'ils définissent en matière de formation à dispenser au public. Par exemple, lors du groupe de discussion, un policier a mentionné la chose suivante : « On rencontre juste les filles, pas les gars. Parce qu'on ne veut pas donner des idées aux gars ! » (Agent 7), alors que les hommes sont majoritairement victimes pour certains types de cybercriminalité. En termes de connaissances plus précises sur les tendances en matière de cybercriminalité, le langage technique et les stratégies et méthodes de prévention, les agents perçoivent également le besoin de mises à jour régulières axées sur leurs besoins opérationnels. Ce constat vient confirmer les observations faites dans d'autres pays (Burruss & al., 2020 ; Hadlington & al., 2021 ; Hinduja, 2004 ; Hull & al., 2018).

Les tensions de la collaboration : entre distanciation organisationnelle et volonté de partenariat

Une dernière thématique fréquemment abordée au cours des entretiens concerne les liens et interactions que les policiers spécialisés en prévention de la délinquance entretiennent au sein de leur organisation, ainsi qu'avec une constellation de partenaires externes disposant de capacités conséquentes en matière de lutte contre la cybercriminalité.

La distanciation organisationnelle des spécialistes de la cybercriminalité

De manière générale, la problématique qui a été la plus fréquemment mentionnée pendant la discussion de groupe est une certaine distanciation organisationnelle, c'est-à-dire une méconnaissance de la part du service de police des diverses formes de cybercriminalité et des réalités opérationnelles vécues par les intervenants de première ligne (cité 45 fois par les sept agents). Il semble exister un écart important entre la représentation que leur institution se ferait de la cybercriminalité et la réalité de celle-ci : « Il faut qu'ils [les cadres de l'organisation] viennent observer sur le terrain ce qui se passe parce que ce n'est pas dans le bureau qu'ils vont se le figurer... » (Agent 6). Cela génère concrètement la perception d'un manque de soutien opérationnel et l'imposition de procédures bureaucratiques qui constituent un irritant majeur. Ainsi, les participants à l'étude déplorent la lourdeur et la lenteur des processus de création des outils de prévention de la cybercriminalité, qui leur font défaut ou ne sont plus adaptés à leurs besoins quand ils finissent par être prêts. Pourtant, la rapidité d'élaboration et de diffusion des ressources de prévention modulables semble être un critère central du fait de la spécificité de la cybercriminalité qui évolue à un rythme

très rapide : « On n'a pas le droit d'en faire, mais ils ne nous en fournissent pas. » (Agent 4) « Bah c'est comme dans tous les autres domaines. Le bateau est tellement gros à faire tourner là. Peu importe ce que tu veux faire comme outil là, le temps que... tu l'fais, puis là ça se rend... tout a changé. » (Agent 6) « Ça arrive en haut, tu descends, c'est fini ! C'est, c'est même plus à jour ! Comme le programme [nom du programme], ça vient de nous être présenté. Ça fait combien d'années qu'ils travaillent là-dessus ? Il est même plus à jour. » (Agent 4)

Ensuite, la méconnaissance de ce phénomène et de son importance entraînerait une absence de suivi aux enquêtes qui rendrait le travail des spécialistes en prévention plus difficile et aurait un impact direct sur la banalisation du phénomène au sein de la population (cité 16 fois) : « On a un gros problème avec ça. On a un gros problème avec ça. Le nombre de rapports que moi je prends moi-même, j'suis même pas supposée prendre des rapports selon, théoriquement, mon boss. Mais j'en prends énormément de rapports. Puis, je pousse aux enquêtes. Je pousse ci, je pousse ça. Puis, le nombre de fois que j'ai le nom du suspect, j'ai le nom de tout, puis c'est [le dossier] fermé euh… « terminé non résolu ». Y me niaisent-tu ? Tu as le nom de mon suspect dedans ! « Ouais, mais là elle voulait plus vraiment porter plainte là » [Imite un policier enquêteur]. Ça fait que, le jeune là, il se rend compte que y'en a pas de conséquences. » (Agent 4)

Cette distanciation organisationnelle entraîne, en toute logique, la diffusion de messages contradictoires auprès de la population entre les agents agissant en prévention qui souhaitent intensifier le traitement des dossiers liés à la cybercriminalité et les autres policiers qui semblent y accorder une bien moins grande importance (cité cinq fois). C'est-à-dire que ces derniers sembleraient aborder la cybercriminalité comme un phénomène « routinier » qui ne rentrerait pas forcément dans les paramètres de base de leurs interventions répressives : « Exactement. Il s'agit juste qu'une fois que le gars soit arrêté, puis qu'il y ait pas eu de conséquences pour que le mot se passe que peu importe ce qui se passe, on s'en fout. On a beau dire n'importe quoi là, il se passera rien [acquiescement des autres agents]. Ça, malheureusement... (…) Esti qu'ils [les policiers] te scrapent ça en 3 mn, parce que lui, ça le fait chier d'être là, parce qu'il n'a pas le goût d'être là, puis qu'il trouve que c'est du maudit niaisage quand ils [la population] ont appelé le 911. Toi après ça, t'en as pour des semaines à rattraper ça pour essayer de reconstruire ça. » (Agent 4)

Plus encore, ce double message serait de nature à venir renforcer cette perception de banalisation déjà sous-jacente au sein de la population : « Ouais, ben juste, j'ai relevé une absurdité dans notre message. On dit qu'il faut puncher sa loi, c'est ça qui pogne. Puis, de l'autre côté, on dit qu'il se passe comme pas grand-chose parce qu'on le banalise. Ce qui fait que, si on veut puncher, à un moment donné, faut aller plus loin parce que sinon, quand ils [les délinquants] se font prendre : « ah, mais il ne s'est rien passé ». Le policier va avoir un gros problème avec ça. » (Agent 5)

En outre, du côté des enquêteurs spécialisés en cyberenquête, ce déficit de communication entre les agents spécialisés en prévention et leur organisation semble être problématique à plusieurs niveaux. Ainsi, les enquêteurs se sentent insuffisamment informés des besoins et attentes des agents concernant les outils et les connaissances requises, alors que ce sont eux qui sont responsables de partager leur expertise technique à travers des formations. Cela produit alors un impact direct sur la pertinence et la qualité de celles-ci, qui pourraient être élaborées en tenant mieux compte des besoins des utilisateurs finaux de ces connaissances. De plus, ce manque de communication avec les enquêteurs spécialisés empêche ces derniers d'obtenir des données et des statistiques sur la cybercriminalité qui pourraient les aider à mieux démontrer l'ampleur du phénomène à la direction du service et ainsi à obtenir plus de ressources : « Parce qu'on nous demande des statistiques, par exemple, côté cyber, c'est sûr qu'il y a beaucoup de choses, on sait que ça se rend pas à nous. Mais tu sais, si vous ne nous appelez pas, bah on ne le saura jamais… C'est ce qui se rend à nous seulement. Tout le reste là, on ne le sait pas là. » (Enquêteur 4)

En résumé, cette distanciation organisationnelle, amplifiée par un déficit de communications entre les agents dédiés à la prévention de la cybercriminalité et l'équipe spécialisée en cyberenquête, qui possède les compétences et l'expertise dont les premiers auraient besoin ainsi qu'une meilleure écoute de la direction, renforce cette perception d'un manque de ressources au service des activités de prévention.

Des partenariats valorisés, mais sous-développés

Les policiers spécialisés en prévention ont souvent mis de l'avant la recherche et l'utilisation d'outils provenant d'autres organismes, ainsi que l'établissement de liens de collaboration avec ces derniers afin de combler un manque perçu de ressources internes. Lors du groupe de discussion, plusieurs catégories de partenaires externes ont été évoquées, qu'il s'agisse d'autres services de police, d'associations intervenant auprès de populations vulnérables et exposées à une sur-victimisation, ou d'organismes jouant un rôle en prévention générale de la criminalité. Outre le fait que ces partenaires semblent offrir des outils diversifiés d'aide à la sensibilisation et à la formation qui font défaut aux agents de police dans leurs activités de prévention de la cybercriminalité, ces ressources semblent particulièrement efficaces comparées à celles mises à disposition par leur organisation. Il s'agit par exemple d'outils interactifs comme des posters, des clips vidéo, ou même des applications mobiles aidant les individus à identifier des situations de cybercriminalité et à s'en prémunir : « Ils [un organisme intervenant en prévention du crime] ont des outils fantastiques hein ! Ils ont des affaires, des manettes pour faire voter les gens [acquiescement des autres participants sur le côté positif de la chose]. C'est interactif, c'est débile ce qu'ils ont comme budget là ! Puis, nous autres on arrive avec notre petit power-point au tableau, on fait un petit peu dur. » (Agent 4)

De plus, ces partenaires externes semblent, outre l'efficacité de leurs outils, intervenir sur des volets différents, mais complémentaires des services de police lors de leurs activités en prévention, en sensibilisant par exemple aux facteurs de victimisation, en diffusant les coordonnées des services d'aide aux victimes à contacter en cas de besoin, voire en offrant des possibilités de soutien psychologique : « Moi je les réfère au site là euh [nom de l'organisme], puis [programme de l'organisme en question]. A un moment donné, on a chacun nos forces. Bah pas nos forces, mais nos… t'sais c'est chacun son métier là comme on dit là. » (Agent 1)

Un autre avantage des partenariats externes plus formels est qu'ils permettraient de freiner l'utilisation de stratégies d'adaptation par les agents de police (cité 14 fois par quatre agents), qui pour combler le manque d'outils de prévention fournis par leur employeur utilisent parfois leur équipement informatique personnel (téléphone intelligent ou ordinateur portable), ce qui peut causer des problèmes de sécurité (cité 3 fois par trois agents) : « On n'est pas supposé ! Sauf que, t'sais, encore là, le service devrait nous fournir quelque chose, qu'on puisse aller voir ces affaires là (…) Moi, je suis obligée d'aller voir sur mes affaires personnelles, puis je le sais qu'on n'est pas supposé faire ça, mais... » (Agent 4)

Ainsi, les partenariats avec des organismes pouvant partager des ressources efficaces en prévention de la cybercriminalité semblent très appréciés des agents, à l'instar des partenariats qu'entretiennent les enquêteurs spécialisés en cyberenquête avec leurs homologues policiers, du secteur privé et du monde de la recherche.

Conclusion

La cybercriminalité génère une demande croissante d'informations et d'activités de sensibilisation de la part de la population envers les services de police (Dodge & Burruss, 2020 ; Wall, 2008, 2010). Ceci est notamment lié au sentiment d'insécurité émergent qui est associé aux risques numériques et qui résulte de leur complexité technique et de leur constante évolution, à un rythme parfois difficile à suivre pour les utilisateurs lambda (Hull & al., 2018 ; McGuire, 2020). Les services de police, notamment ceux qui opèrent à l'échelle locale, font ainsi face à de nouvelles formes de délinquance et à des besoins pour lesquels ils disposent de ressources limitées (Dupont, 2016 ; Webster & Drew, 2017 ; Dupont, 2021). Pourtant, il est particulièrement important, en ce qui concerne la prévention, que les services de police locaux soient préparés à intervenir dans le domaine de la cybercriminalité, du fait de leur proximité avec la population. L'objectif de cet article était ainsi d'identifier les défis rencontrés par les agents ayant des fonctions dédiées à la prévention au sein d'un service de police canadien agissant au niveau local. Le but était alors de faire apparaître les besoins prioritaires perçus par les agents de première ligne.

Ces derniers ont exprimé un sentiment de distanciation organisationnelle qui rend leur hiérarchie moins réceptive à leurs besoins et semble limiter leur accès à des ressources informationnelles de soutien aux activités de prévention auprès du public. Par ailleurs, ce manque de ressources adéquates renforcerait leur surcharge de travail et ainsi leur manque de confiance et de motivation à traiter de ce phénomène. Si les participants à cette étude estiment que la cybercriminalité est un phénomène que les services de police doivent prendre en charge, en raison notamment de son ampleur, nous avons aussi pu constater que les agents n'étaient pas forcément très confiants dans leurs capacités à assumer ce rôle. Cela semble en grande partie dû au manque de ressources mises à leur disposition et non pas à une aversion pour ce type de criminalité au détriment de la criminalité traditionnelle. Ce serait également le cas, plus largement, pour l'ensemble des policiers confrontés à des cybercrimes, qui semblent les banaliser en raison d'un manque de connaissances sur les modes d'intervention efficaces. Contrairement à certaines observations similaires faites dans la littérature scientifique (Holt & Bossler, 2011 ; Holt & al., 2018 ; Huey 2002 ; Powell & Henry, 2018), ce déficit d'intérêt et de motivation ne serait pas lié à une préférence pour le traitement des crimes traditionnels, mais plutôt des lacunes perçues dans leurs capacités à prendre en charge les cybercrimes. Les participants, eux-mêmes, à l'instar d'autres études menées dans des services de police américains et britanniques (Burruss & al., 2020 ; Hadlington & al., 2021 ; Hull & al., 2018), semblent démontrer la volonté d'être formés et outillés par des « experts » en prévention de la cybercriminalité afin de développer les compétences requises pour répondre à cette nouvelle demande : « C'est qu'on n'a pas de gens qui sont spécialisés au service, puis c'est ça qui est triste. C'est que quelque part on veut que ça soit des policiers qui le fasse parce que ça coûte moins cher, mais on n'est pas des spécialistes là. Y'a des gens-là qui ont fait des hautes études là-dedans, dans des programmes de prévention, des criminologues, des... Nous autres on, on fait ce qu'on peut avec ce qu'on a… Non, mais c'est vrai, c'est vrai ! Ça devrait être ça, le service de police devrait engager des gens, des spécialistes là-dedans, les mettre au QG [quartier général] et dire : « Parfait, c'est quoi vos besoins ? On va vous en pondre nous autres des projets de prévention ». (Agent 4)

Cette recherche présente deux limites principales qui pourraient faire l'objet de futures recherches sur le sujet. La première est que la taille de l'échantillon des répondants reste modeste, dans la mesure où une seule organisation policière a participé à cette étude, ce qui nous empêche de généraliser les résultats obtenus ou de procéder à des comparaisons inter-organisationnelles afin d'identifier des variations probables et de possibles innovations. De plus, la pandémie de COVID-19 a interrompu la collecte des données et il ne nous a pas été possible d'interviewer les membres de la direction du service concerné, ce qui nous aurait permis d'identifier les contraintes internes et les arbitrages organisationnels qui doivent être faits dans le cadre de la gestion simultanée de nombreuses formes de délinquance et de problèmes de sécurité urbaine. Cette étude demeure toutefois l'une des seules existantes à notre connaissance sur les pratiques

policières de prévention de la cybercriminalité, la majorité des recherches dans ce domaine se focalisant sur les méthodes et stratégies d'enquête.

À la lumière des résultats obtenus, il nous semble possible d'identifier quelques pistes de réflexion sur les adaptations qui faciliteraient le développement de capacités policières répondant mieux aux besoins de la population en matière de prévention de la cybercriminalité. En premier lieu, il nous paraît important que les organisations policières s'attaquent à la distanciation organisationnelle qui marginalise au sein des organisations policières les unités qui traitent de la cybercriminalité, un phénomène également observé en Australie (Harkin & Whelan, 2019). Dans la mesure où la cybercriminalité constitue désormais la forme de délinquance dominante par nombre d'incidents, les organisations policières devraient l'intégrer de manière plus systématique à chacune de leurs stratégies et de leurs décisions opérationnelles, et cesser de la considérer comme une spécialité réservée à un petit nombre d'enquêteurs et d'agents de prévention passionnés par les nouvelles technologies. Cela faciliterait aussi la création de liens transversaux entre enquêteurs et spécialistes de la prévention, et par ricochet de l'intégration des connaissances complémentaires générées par les deux groupes de praticiens. Dans le but de renforcer une expertise en prévention qui reste fragmentaire, il pourrait également être pertinent d'envisager le recrutement de spécialistes civils disposant de connaissances plus pointues sur la cybercriminalité, les techniques de prévention, mais aussi la conception et la diffusion de programmes de formation et de sensibilisation attrayants et efficaces (Whelan & Harkin, 2021 ; Dupont, 2021). Finalement, la complexité de l'écosystème des risques numériques est tel qu'il semble illusoire d'espérer que les organisations policières, et celles qui opèrent à l'échelle locale de surcroît, soient capables de remplir seules le mandat de prévention et de contrôle de la délinquance qui est le leur (Dupont, 2019). Un réseau dense de partenaires publics, privés et associatifs incorporant les moyens techniques et les connaissances des autorités régulatrices, des géants du web, des opérateurs de télécommunication, des institutions financières, des laboratoires de recherche en informatique et en sciences sociales, et de toute une constellation d'organismes communautaires (Boes & Leukfeldt, 2017), semble être le meilleur moyen de fédérer et de coordonner les capacités requises pour une gouvernance plus inclusive et plus efficace de la prévention de la cybercriminalité.

Références

Accenture (2017). Canada Cybercrime Survey 2017. Repéré à https://www.accenture.com/ca-en/company-news-release-canada-cybercrime-survey-2017

Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganan, C., Levi, M., Moore, T., & Vasek, M. (2019). Measuring the changing cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security*, Boston.

Bennett, D., & Stephens, P. (2014). Preventing digital crime. Dans R. Bryant & S. Bryant (eds.), *Policing digital crime* (pp. 63-82). UK : Ashgate.

Boes, S., & Leukfeldt, E. R. (2017). Fighting cybercrime : A joint effort. In R.M. Clarke & S. Hakim (dir.), *Cyber-physical security* (pp. 185-203). Springer, Cham.

Bossler, A. M., Holt, T. J., & May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, 44(4), 500-523.

Bossler, A. M., Holt, T. J., Cross, C., & Burruss, G. W. (2020). Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. *Security Journal, 33*(2), 1-18.

Burruss, G., Howell, C. J., Bossler, A., & Holt, T. J. (2020). Self-perceptions of English and Welsh constables and sergeants preparedness for online crime. *Policing: An International Journal, 43*(1), 105-199.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime : The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

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

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice, 9*(2), 119–128.

Cusson, M. (2007a). De l'action de sécurité. Dans M. Cusson, B. Dupont & F. Lemieux (dir.), *Traité de Sécurité intérieure* (p. 43-57). Montréal, Québec : Hurtubise.

Cusson, M. (2007b). Questions de stratégie pour la police. Dans M. Cusson, B. Dupont & F. Lemieux (dir.), *Traité de sécurité intérieure* (p. 130-139). Montréal, Québec : Éditions Hurtubise.

Denat, F. (2002). Prévention… Le rôle de la police. *Éthique publique, 4*(2), 1-21.

Dodge, C., & Burruss, G. (2020). Policing cybercrime : Responding to the growing problem and considering future solutions. Dans R. Leukfeldt & T. J. Holt (dirs.), *The Human Factor of Cybercrime* (pp. 339-358). New-York : Routledge.

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies : Developing police-led cyber fraud prevention programs. Police Practice and Research, 19(6), 537-549.

Dupont, B. (2016). La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale. *Cultures & Conflits*, (102), 95-120.

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*(1), 97-116.

Dupont, B. (2019). L'écologie de la cybersécurité. Dans M. Cusson et al. (dirs.), Nouveau traité de sécurité : Sécurité intérieure et sécurité urbaine (pp. 55-68). Montréal : Hurtubise.

Dupont, B. (2021). La police et la prévention de la cybercriminalité. Dans B. Dupont et al., *L'avenir du travail policier* (pp. 49-88). Montréal : Les Presses de l'Université de Montréal.

Dupont, B., & Gautrais, V. (2010). Crime 2.0 : le web dans tous ses états !. *Champ pénal/ Penal field, 7*, 1-26.

Federal Bureau of Investigation. (2019). *2019 Internet Crime Report*. Repéré à https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2021). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing : A Journal of Policy and Practice, 15*(1), 34-43.

Harkin, D., & Whelan, C. (2019). Exploring the implications of 'low visibility' specialist cyber-crime units. *Australian and New Zealand Journal of Criminology, 52*(4), 578-594.

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

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing : An International Journal of Police Strategies & Management, 27*(3), 341-357.

Holt, T. J. (2018). Regulating cybercrime through law enforcement and industry mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140-157.

Holt, T. J., & Bossler, A. M. (2011). 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, T. J., Burruss, G. W., & Bossler, A. M. (2018). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906-921.

Huey, L. (2002), Policing the abstract : Some observations on policing cyberspace, Canadian *Journal of Criminology, 44(*3), 243-254.

Hull, M., Eze, T., & Speakman, L. (2018, October). Policing The Cyber Threat : Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond. In *2018 European Intelligence and Security Informatics Conference (EISIC)* (pp. 15-22). IEEE Computer Society.

Karagiannopoulos, V., Sugiura, L., & Kirby, A. L. (2019). *The Portsmouth Cybercrime Awareness Clinic Project : Key Findings and Recommendations*. University of Portsmouth. http://www2.port.ac.uk/institute-of-criminal-justice-studies/strategic-projects/cybercrime-awareness-clinic/

Lee, J. R., Holt, T. J., Burruss, G. W., & Bossler, A. M. (2021). Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review, 31*(1), 20-39.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes : overview and issues. *Crime, Law and Social Change, 67*(1), 3-20.

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. L. (2015). *The implications of economic cybercrime for policing*. Londres : City of London Corporation.

Loubet del Bayle, J. L. (2007). Sécurité et contrôle social. Dans M. Cusson, B. Dupont & F. Lemieux (dir.), *Traité de Sécurité intérieure* (pp. 58-66). Montréal : Hurtubise.

McGuire, M. (2020). It ain't what it is, it's the way that they do it ? Why we still don't understand cybercrime. Dans R. Leukfeldt & T. J. Holt (dirs.), *The Human Factor of Cybercrime* (pp. 3-28). New-York : Routledge.

Powell, A., & Henry, N. (2018). Policing technology-facilitated sexual violence against adult victims : Police and service sector perspectives. *Policing and Society, 28*(3), 291-307.

Quéro, Y.-C., & Dupont, B. (2019). Police communautaire, résolution de problèmes et évaluation d'efficacité : bilan et perspectives. Dans M. Cusson, O. Ribaux, E. Blais & M. M. Raynaud (dirs.), *Nouveau traité de sécurité : Sécurité intérieure et sécurité urbaine* (p. 69-81). Montréal : Hurtubise.

Senjo, S. R. (2004). An analysis of computer-related crime : Comparing police officer perceptions with empirical data. *Security journal, 17*(2), 55-71.

Statistique Canada. (2019). Le cybercrime au Canada. Repéré à https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-fra.htm

Wall, D. (2010). Criminalising cyberspace : the rise of the Internet as a 'crime problem'. Dans Y. Jewkes & M. Jar (dirs.), *Handbook of Internet Crime* (pp. 88-103). UK : William Publishing.

Wall, D. S. (2008). Cybercrime and the culture of fear : Social science fiction (s) and the production of knowledge about cybercrime. *Information, Communication & Society, 11*(6), 861-884.

Webster, J., & Drew, J. M. (2017). Policing advance fee fraud (AFF) : Experiences of fraud detectives using a victim-focused approach. *International Journal of Police Science and Management, 19*(1), 39–53.

Welsh, B. C., & Farrington, D. P. (2012). Crime prevention and Public Policy. Dans D. P Farrington & B.C. Welsh, *The Oxford Handbook of Crime Prevention* (pp. 1-19). Oxford University Press.

Whelan, C., & Harkin, D. (2021). Civilianising specialist units : Reflections on the policing of cybercrime. *Criminology & Criminal Justice, 21*(4), 529-546.