Rapport synthèse au conseil d'administration de l'ACCP
… de l'équipe des Études internationales ACCP 2015

Cybercrime : Rôles et responsabilités de la police dans un cadre de collaboration

À l'automne 2014, le conseil d'administration de l'ACCP a chargé l'équipe du Programme d'études internationales pour cadres supérieurs de l'ACCP (Études internationales ACCP), récemment remanié, de mener des recherches sur la cybercriminalité au Canada et dans le monde. En délimitant cette mission, le conseil d'administration reconnaissait la cybercriminalité comme un problème émergent *« qui met à l'épreuve les compétences, les capacités, les rôles et les modes d'intervention de la police »*, précisant que *« la nécessité d'une action nationale cohérente devenait une priorité pour les dirigeants policiers au Canada »*. À partir de janvier, la cohorte 2015 des Études internationales ACCP, comprenant 17 cadres policiers de la relève, s'est mise à l'œuvre. Elle comprenait des représentants de 11 corps policiers de ressort fédéral, provincial, local et militaire. Fidèles à la tradition des sept cohortes précédentes, ils ont entrepris leurs recherches dans un cadre d'apprentissage transformateur, en suivant une démarche axée sur les problèmes.

Après plus de sept mois de recherches au Canada et d'études sur le terrain à l'étranger, d'interactions intensives en ligne et d'ateliers en résidence, la cohorte présentera à l'Assemblée générale annuelle et Conférence nationale de l'ACCP à Québec six produits qui, ensemble, constituent les fruits du Programme 2015 d'études internationales pour cadre supérieurs de l'ACCP :

1. Rapport synthèse : Études internationales ACCP 2015 – le présent bref document;
2. Cybercrime : Passons à l'action – un document évolutif, annexe du présent sommaire, qui suit le cours des recherches de la cohorte et constitue un journal des enjeux abordés et des observations qui sous-tendent les autres produits;
3. Études internationales ACCP 2015 : Un guide pour l'action policière contre le cybercrime au Canada – un guide de référence rapide à l'intention des cadres et des membres des services de police à tous les échelons, présentant des suggestions immédiates d'action pour tous les acteurs policiers face au problème de la cybercriminalité (version anglaise ci-jointe; sera distribué dans les deux langues officielles à la Conférence et par la suite, par le Bureau national);
4. Résolution 07-2015 de l'ACCP : Cybercrime : Rôles et responsabilités de la police dans un cadre national de collaboration – qui sera soumise en août 2015 à l'Assemblée générale annuelle (voir la page 4 du guide ci-joint);
5. Cybercrime : Préparer une action policière multipartite au Canada – un exposé de 30 minutes et une discussion d'experts, dans le cadre du programme professionnel de la Conférence annuelle de l'ACCP;
6. *Cybercrime : Passons à l'action* – une vidéo ACCP ' Take 5 ' qui servira d'introduction à l'exposé présenté à la Conférence et, par la suite, de catalyseur de discussions et d'une prise de conscience dans l'ensemble du milieu policier au Canada.

En plus de signaler la conclusion fructueuse des travaux officiels de la cohorte, ces produits visent à baliser une voie d'avenir pour le milieu canadien de l'application de la loi face à la cybercriminalité,

dans le contexte d'une action plus vaste, axée sur la collaboration, de l'ensemble de la société pour contrer cette criminalité de plus en plus répandue et pernicieuse.

Le message fondamental véhiculé par tous les produits est à la fois cohérent et relativement simple : un cybercrime est un crime qui victimise nos citoyens; les forces policières de tous les paliers doivent participer à l'action; et il est temps d'agir. Le présent document décrit brièvement le travail entrepris par la cohorte et résume les produits ci-joints.

Notre méthode

En premier lieu, la cohorte s'est livrée à un exercice de débroussaillage afin de définir la problématique, passer en revue la documentation et dresser un bilan de référence du problème au Canada. Elle a réalisé l'exercice et en a discuté avec des représentants du Comité sur la cybercriminalité et du Comité international de l'ACCP. Il a conduit à la constatation que « cyber » a une vaste portée; qu'il se fait énormément de travail sur le « cyber » à l'échelle locale, nationale et internationale; et que cette activité est confrontée à huit problèmes persistants au Canada :

- définition (« qu'est-ce qui est *cyber* »?);
- capacité d'action de la police;
- aptitudes policières;
- coordination et harmonisation;
- domaines de compétence de la police;
- lacunes et possibilités législatives;
- dialogue public;
- l'avenir prévisible.

L'analyse initiale et les discussions qui en ont découlé avec divers groupes d'experts invités ont aidé la cohorte à circonscrire un objectif de recherche et un ensemble de dimensions de recherche à titre de cadre de référence pour la question soumise par le conseil d'administration. Elle a ainsi résolu **« d'examiner l'approche adoptée dans certains pays pour cerner les rôles les plus efficaces de la police au sein d'un cadre de collaboration »**. À cette fin, elle s'est penchée sur diverses dimensions :

- la portée et l'incidence de la cybervictimisation (quelqu'un a-t-il une bonne idée de l'ampleur du problème?);
- démarches stratégiques (que visent à accomplir d'autres : renforcer les cibles; accroître la sensibilisation; attraper des malfaiteurs?);
- facteurs du succès et de la viabilité d'une démarche collaborative face au cybercrime (qui devrait participer et qu'est-ce qui assure l'efficacité de la collaboration?);
- rôles et responsabilités face au cybercrime (quel rôle les divers paliers de forces de l'ordre jouent-ils, et qu'en est-il du secteur privé?);
- attitudes de la société (comment le public, à l'extérieur du Canada, perçoit-il le problème?);
- évaluations (comment savons-nous si nous progressons?).

Nos études internationales sur le cybercrime

Ces dimensions étant posées, la cohorte a ensuite cherché des pays qui pourraient receler des leçons intéressantes pour le Canada. Neuf pays ont été retenus en vue de visites sur place, et des sous-équipes ont été formées pour mener des études sur le terrain :

Royaume-Uni et Espagne
France, Allemagne et Pays-Bas
Inde et Singapour
Australie et Nouvelle-Zélande

Ces pays ont été choisis pour plusieurs raisons, que ce soit des pratiques exemplaires dont s'inspirer ou des situations laissant présager les défis qu'il faudra relever au Canada. Par exemple, le Royaume-Uni, l'Australie et la Nouvelle-Zélande sont très semblables dans la façon dont elles abordent les services de police et dans leur état de préparation aux cyber-réalités. Aux Pays-Bas et à Singapour, des recherches indiquaient que le centre EC3 d'Europol et le Complexe mondial INTERPOL pour l'innovation avaient des pratiques exemplaires instructives en matière de collaboration. L'Inde a été retenue en raison de l'essor de son secteur de la technologie et parce qu'elle est une importante source de pourriels et d'autres formes de cyberactivité malicieuse.

La cohorte a effectué ses visites sur place entre la fin mars et le début de mai 2015. Pendant ces visites, les équipes ont mené des entrevues structurées approfondies avec presque 100 experts représentatifs des milieux policier, gouvernemental, universitaire et de l'industrie privée.

En plus de mener des études sur le terrain, l'ensemble de la cohorte a reçu plusieurs délégations au cours de son travail en résidence. Les participants ont ainsi pu discuter, entre autres, avec :

- un cadre supérieur de la National Cyber Forensics and Training Alliance (NCFTA), de Pittsburgh, qui a apporté à l'ensemble de la cohorte une perspective informée sur l'expérience d'une collaboration intersectorielle public-privé aux États-Unis;
- des représentants de l'embryonnaire initiative JORM sur le cybercrime, à Toronto, qui réunit les perspectives aussi bien de dirigeants policiers (crimes financiers) que de banquiers sur les stratégies émergentes du secteur bancaire;
- des représentants de l'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité Canada, de Montréal, qui ont présenté des outils de recherche et de contrôle en cours de mise au point et d'essais en vue d'une utilisation au Canada.

Synthèse des principaux éléments à retenir

Chaque pays a révélé de précieuses perspectives, et divers thèmes étaient communs à tous les pays étudiés. Ces thèmes étaient du reste tout à fait pertinents au regard de notre analyse de référence au Canada :

- l'énormité du problème;
- l'importance vitale de relations étroites entre la police et le secteur privé;
- la nécessité urgente d'accroître la déclaration des cybercrimes à la police;
- la nécessité d'améliorer l'échange d'information entre tous les acteurs;

- le manque de sensibilisation au cybercrime parmi la population;
- le manque de compétences nécessaires parmi la police;
- le manque de connaissances nécessaires parmi la magistrature, et des pratiques judiciaires inadéquates en matière d'enquêtes et de poursuites visant le cybercrime;
- le manque d'indicateurs communs pour mesurer le cybercrime et ses répercussions;
- l'importance croissante de la coordination et de l'harmonisation;
- la futilité de solutions bornées par les frontières face à ce qui est effectivement une criminalité sans frontières.

Nous avons ensuite examiné ces observations dans la perspective de divers modèles théoriques, pour tenter d'en dégager au mieux des leçons applicables au Canada. Initialement, la cohorte a considéré le cybercrime comme un *problème de santé publique* : parer à la propagation d'une maladie (en l'occurrence la criminalité en ligne) exige une démarche systémique s'appuyant sur une écologie d'acteurs liés entre eux et privilégiant la prévention systémique. Dans un tel modèle, le rôle de la police consisterait à maîtriser les éclosions et à mettre *en quarantaine* ceux qui propagent la maladie.

Nous avons examiné une démarche stratégique classique des « 4 P » : se préparer, prévenir, poursuivre et protéger. Cette démarche a été mise en œuvre au Royaume-Uni et est semblable à des stratégies visant d'autres problèmes de sécurité actuels, comme la stratégie antiterroriste du Canada. Elle a semblé abstraite à la cohorte, paraissant mieux convenir à des rôles non policiers, auxquels elle attache une plus grande importance.

Nous avons considéré un modèle observé en Allemagne, au G4C (German Competence Centre against Cyber Crime). Ici, la lutte contre le cybercrime vise à faire en sorte qu'il soit plus complexe de commettre des attaques, ce qui augmente les coûts et réduit la récompense pour les délinquants. Cette démarche a vivement intéressé la cohorte en raison de sa simplicité et de sa ressemblance à des méthodes policières traditionnelles.

Cette dernière démarche a amené la cohorte à sa conclusion : *s'attaquer au cybercrime est question de reconnaître qu'il s'agit de crime* et, par conséquent, *le modèle traditionnel du crime est l'optique la plus opportune*. Une démarche face au cybercrime mettant l'accent sur une intervention policière structurée autour des trois éléments principaux du modèle de base du crime – *le délinquant, la victime et le lieu et/ou l'occasion du crime* – contribuerait grandement à contrer la perception que le cybercrime est un phénomène plus complexe qu'il ne l'est réellement.

Nos trois vérités au sujet du cybercrime

Pour situer nos recommandations d'action, nous croyons nécessaire d'exprimer d'abord trois vérités, de les étoffer et de les faire mieux comprendre de l'ensemble du milieu policier canadien :

> Le cybercrime est un crime... et il crée des victimes véritables, qui souvent subissent des effets dévastateurs.
> Le cybercrime est une priorité pour la sécurité des collectivités, partout.
> Les services de police à tous les niveaux peuvent agir, jusqu'à un certain point.

Nos recommandations au milieu policier canadien

Dans ce cadre de référence – *fondé sur la reconnaissance que le cybercrime n'est autre chose qu'un crime du 21e siècle* –, l'équipe des Études internationales ACCP 2015 en est arrivée à six grandes recommandations. Nous croyons qu'elles sont pertinentes pour les dirigeants policiers à tous les paliers de l'application de la loi au Canada, et que les dirigeants policiers peuvent agir en conséquence.

1) **Cybercrime courant**

   Un changement de paradigme s'impose. Les forces de l'ordre doivent former les unités de police au contact du public pour qu'elles reconnaissent le crime en ligne comme un crime qui a des répercussions pour leurs citoyens, et elles doivent encourager sa déclaration.

   Les unités d'enquêtes générales doivent acquérir et développer des capacités d'enquête dans le monde en ligne. Le monde en ligne ne doit pas rester le domaine exclusif d'unités spécialisées.

2) **Augmenter la sensibilisation de la communauté et le soutien aux victimes**

   Reconnaissant qu'elles ont affaire à un crime, les forces de l'ordre doivent offrir un soutien aux victimes. Elles doivent aussi faire connaître les moyens d'éviter la victimisation. Comme pour d'autres crimes et menaces à la sécurité communautaire, la meilleure solution est sans doute l'éducation auprès des jeunes, qui doit être précoce et fréquente. Les forces de l'ordre ne doivent pas pour autant être seules face au problème. Il existe de puissantes ressources, par exemple des initiatives comme *pensezcybersecurite.ca*, dont la police peut tirer parti. L'ACCP devrait envisager une « Journée de la cybersécurité », de la même façon qu'il y a une Journée nationale de retour des médicaments d'ordonnance.

3) **Instaurer la confiance et la collaboration au-delà des forces de l'ordre**

   Le Canada a besoin d'un modèle solide et structuré de collaboration entre secteurs. La colocalisation assortie de protocoles appropriés d'échange de renseignements est une solution idéale. Même si elle crée un certain niveau de risque, elle est possible dans le cadre législatif actuel.

   Nous devons tirer parti des structures et initiatives existantes, les réorganiser ou les réorienter pour créer une démarche intégrée. Il faudrait le faire rapidement pour empêcher une plus grande fragmentation qui ferait du dispositif canadien un ensemble disparate de centres de coordination.

4) **Mettre en place des mécanismes et des structures de coordination et d'échange d'information aux paliers local, provincial, national et international**

   Il manque au Canada de mécanismes et de structures comme on en voit dans d'autres pays qui assurent la coordination et l'échange d'information aux paliers local, provincial, national et international.

   Le crime en ligne remet en question les modèles d'intervention, les pouvoirs et les territoires de

compétence actuels. Une conversation fédérale-provinciale-territoriale s'impose de toute urgence au sujet de la lutte contre une criminalité qui ne connaît pas les frontières, en vue de parer à la dispersion constitutionnelle de l'action policière au Canada.

5) Rehausser les aptitudes et la capacité d'action du système judiciaire

Nous devons rehausser les aptitudes et la capacité d'action des forces de l'ordre et du système judiciaire, de diverses façons :

- formation – les rudiments du monde numérique devraient faire partie de la formation de tous les cadets, et il faudrait prévoir de la formation spécialisée en milieu de travail, ainsi que la formation de poursuivants spcialisés;
- capacités d'enquête – il faudrait des équipes régionales d'enquête sur le cybercrime;
- outils – des outils numériques de criminalistique doivent être utilisés en première ligne;
- recrutement – des stratégies de recrutement non traditonnelles devraient être envisagées.

6) Militer en faveur de certains changements aux lois et aux règlements

Des réformes législatives soutenues sont nécessaires pour suivre l'évolution de la technologie et de l'environnement en ligne. Il faut de toute urgence des normes sur la durée de conservation de données, pour parer aux tendances récentes des entreprises à conserver les données de moins en moins longtemps. De la même façon, la possibilité de demander des ordonnances de communication visant des données étrangères simplifierait grandement de nombreuses enquêtes. En même temps, pour se préparer à l'avenir, il est vital de continuer de revendiquer un accès légal efficace et l'amélioration du processus d'entraide juridique.

C'est dans l'optique de ces recommandations que la cohorte a formulé la résolution 07-2015 soumise à l'AGA. Nous croyons que cette résolution traduit l'esprit des recommandations de la cohorte des Études internationales ACCP 2015, et qu'elle fait fond sur le travail que poursuit le Comité de l'ACCP sur la cybercriminalité. En somme, nous croyons que la résolution est un appel à l'action nécessaire, voulant que l'ACCP souscrive à un message global découlant de ce vaste exercice d'études internationales :

Cybercrime : Passons à l'action.

« [Le cybercrime]… c'est comme le sel dans les aliments. Il est dans tout. »

- *Insp. Gupta, Central Bureau of Investigation Academy (Inde)*