Résolutions adoptées à la 111e Conférence annuelle

Août 2016

Ottawa, Ontario

ASSOCIATION CANADIENNE DES CHEFS DE POLICE

Sûreté et sécurité pour tous les Canadiens grâce à un leadership policier innovateur

300, promenade Terry Fox, bureau 100, Kanata (Ontario) K1K 0E3
t : 613-595-1101 f : 613-383-0372
c : cacp@cacp.ca w : www.cacp.ca

Table des matières

Résolution #01 - 2016

RÉSOLUTION D'APPUI À UN CADRE DE GESTION DES RESSOURCES HUMAINES AXÉE SUR LES COMPÉTENCES POUR LES SERVICES DE POLICE CANADIENS

Présentée par le Comité sur les ressources humaines et l'apprentissage

ATTENDU QUE le Comité de l'ACCP sur les ressources humaines et l'apprentissage a reconnu l'immense valeur du cadre de gestion des ressources humaines axée sur les compétences (CGAC);

ET ATTENDU QUE la province de la Colombie-Britannique a reconnu la valeur de la formation axée sur les compétences et, en 2010, a recommandé que toutes les recrues policières soient formées selon un curriculum fondé sur les compétences désignées par le Conseil sectoriel de la police;

ET ATTENDU QUE l'Association des chefs de police de l'Alberta a résolu de demander au gouvernement du Canada, par l'entremise de Sécurité publique Canada, d'affecter les fonds nécessaires pour assurer l'avenir et la mise à jour continue du CGAC;

ET ATTENDU QUE l'Association des chefs de police de l'Ontario, à sa 64^{e} assemblée générale en juin 2015, a résolu d'encourager et soutenir l'utilisation du CGAC par les services de police de l'Ontario;

ET ATTENDU QUE des membres du personnel et des services de police, partout au Canada, consultent chaque jour du matériel du CGAC pour des fins de formation, de préparation de la relève, de perfectionnement des cadres supérieurs et de gestion des promotions, des talents, des plans d'apprentissage et du rendement;

ET ATTENDU QUE nous tous, dans les services policiers, avons largement investi dans l'élaboration du CGAC et avons intérêt à ce qu'il continue d'être disponible, accessible, mis en application et tenu à jour,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police demande au gouvernement (Sécurité publique Canada) de prévoir les fonds nécessaires pour assurer l'avenir et la mise à jour continue du CGAC.

Résolution #01 - 2016

RÉSOLUTION D'APPUI À UN CADRE DE GESTION DES RESSOURCES HUMAINES AXÉE SUR LES COMPÉTENCES POUR LES SERVICES DE POLICE CANADIENS

Contexte

Pendant neuf ans, le Conseil sectoriel de la police, financé par le gouvernement du Canada, s'est employé à mettre au point un Cadre de gestion des ressources humaines axée sur les compétences (CGAC) afin d'améliorer et rehausser la gestion des ressources humaines et le professionnalisme policier.

Investi du mandat de fournir des solutions innovatrices et pratiques pour relever les défis en matière de planification et de gestion des ressources humaines dans le secteur policier canadien, le Conseil sectoriel de la police a entrepris l'élaboration d'un CGAC. Il y a travaillé sur une période de cinq ans, avec un investissement de 11 millions de dollars du gouvernement fédéral ainsi que d'innombrables heures de travail et les avis fournis par des services de police canadiens, des particuliers, des partenaires et d'autres parties intéressées. Le Cadre est fondé sur des recherches et des pratiques exemplaires canadiennes et étrangères. Il prescrit des processus fondés sur les compétences, des profils, des outils et des modèles pour 33 rôles policiers dans les domaines des fonctions générales, des enquêtes et de la direction/gestion.

Considérant les investissements de temps, d'argent et de ressources, il est clair qu'il y a une demande à l'égard d'une démarche axée sur les compétences dans la gestion des ressources humaines du secteur policier canadien. Le CGAC est une pierre angulaire dans l'optique plus vaste de la professionnalisation, contribuant à la gestion des effectifs, à la planification de carrière, à la mobilité de la main-d'œuvre et à la justification des actions policières, et il engendrera d'autres gains en efficience sur le plan économique du fait de l'adoption de normes communes sur la formation. En plus du travail effectué en Colombie-Britannique dans la formation des recrues policières, 8 des 13 académies de police évaluent le CGAC en vue de développer, raffiner ou reconsidérer leurs curriculums pour les harmoniser au cadre de référence national. De nombreux services de police utilisent le CGAC comme outil pour améliorer la gestion du personnel et des ressources à tous les échelons.

En avril 2013, le Conseil sectoriel de la police a été dissous faute de fonds. En 2015, le Cadre et la propriété intellectuelle en matière policière s'y rattachant ont été cédés au Réseau canadien du savoir policier (RCDSP). Le RCDSP veille maintenant à l'administration et à la protection du Cadre au nom de la communauté policière, notamment en contrôlant l'accès au CGAC. Depuis 2015, il a accordé un droit d'accès à 144 personnes de 75 services de police et organismes connexes.

Le CGAC et son matériel ne sont pas des ressources figées. Ils doivent être révisés et actualisés régulièrement de sorte qu'ils tiennent compte de l'évolution des pratiques dans le secteur policier et qu'ils puissent soutenir l'évolution en conséquence de la formation et des méthodes policières, de façon cohérente et sur le long terme. À défaut, l'investissement initial et les connaissances accumulées risqueraient d'être dilapidés. Jusqu'à présent, l'Association des chefs de police de

l’Ontario et l’Association des chefs de police de l’Alberta ont toutes deux adopté des résolutions demandant au gouvernement du Canada, par l’entremise de Sécurité publique Canada, de prévoir les fonds nécessaires pour assurer l’avenir et la mise à jour continue du CGAC.

Ces importants investissements de temps, d’efforts et de fonds du gouvernement et de nombreux acteurs du secteur policier ont mené à l’élaboration de normes professionnelles nationales et de matériel aisément accessible, pratique et précieux pour améliorer la façon dont nous gérons le personnel et les ressources à tous les échelons. Des fonds sont maintenant nécessaires pour réviser et actualiser le CGAC, puisque le RCDSP ne possède ni l’infrastructure ni les ressources financières voulues pour le faire.

Résolution #02 - 2016

IMAGES DE VIOLENCE PHYSIQUE À L'ÉGARD D'ENFANTS

Présentée par le Comité sur les amendements législatifs

ATTENDU QU'il y a une prolifération de matériel en ligne représentant de la violence physique à l'égard d'enfants;

ET ATTENDU QUE les images de violence physique à l'égard d'enfants violent la dignité, les droits et la vie privée des enfants victimisés et indiquent dans chaque cas qu'un enfant pourrait avoir désespérément besoin de protection;

ET ATTENDU QUE des dispositions du *Code criminel* visent à éliminer la pornographie infantile, mais qu'il n'y a pas de dispositions analogues interdisant expressément la publication sur Internet d'images de violence physique à l'égard d'enfants;

ET ATTENDU QU'en l'absence d'interdiction criminelle expresse, il est difficile de faire enquête sur des images de violence physique à l'égard d'enfants publiées sur Internet et de supprimer ces images et, surtout, il est impossible d'identifier et d'appréhender les individus se livrant à de telles activités néfastes,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police presse le gouvernement du Canada de protéger les enfants en modifiant le *Code criminel* de façon à interdire la production et la publication d'images de violence physique à l'égard d'enfants et autorisant le retrait et la suppression de telles images d'Internet.

Résolution #02 - 2016

IMAGES DE VIOLENCE PHYSIQUE À L'ÉGARD D'ENFANTS

Contexte

Tel qu'expliqué ci-dessous, cette proposition soumet deux options au gouvernement du Canada en vue de modifier le *Code criminel* pour interdire la production et la publication d'images de violence physique à l'égard d'enfants et autoriser le retrait et la suppression de telles images d'Internet. (*Voir à l'**annexe A** une analyse plus détaillée de cette proposition – en anglais seulement.*)

Production et publication

La publication d'images de violence physique à l'égard d'enfants apparaît comme une tendance préoccupante sur Internet. Des images de violence physique à l'égard d'enfants violent la dignité, les droits et la vie privée des enfants victimisés et indiquent dans chaque cas qu'un enfant pourrait avoir désespérément besoin de protection. Ces images peuvent comprendre des scènes de violence physique gratuite et de violence verbale qui violent la dignité d'un enfant. Pour protéger l'enfant du préjudice que causent ou que causeront les images ainsi que de préjudices physiques persistants, une enquête s'impose. En l'absence d'une enquête, un délinquant ne peut pas être identifié et l'enfant ne peut pas être protégé de violence physique persistante ou future. La coopération de réseaux et de fournisseurs de contenu est vitale au succès d'une enquête. Comme la publication d'images de violence physique à l'égard d'enfants n'est pas actuellement illégale, les réseaux n'ont pas d'obligation de fournir les renseignements nécessaires aux forces de l'ordre, et ils ont la latitude de déterminer quelles mesures ils prendront ou non.

Dispositions sur la saisie

Des images de violence physique à l'égard d'enfants sont choquantes pour le public et suscitent de graves inquiétudes. La nature du contenu figurant dans certaines vidéos publiées sur Internet peut être si horrible qu'elle serait choquante et perturbante pour quiconque les visionne sans les rechercher. La suppression de contenu représentant de la violence physique à l'égard d'enfants est essentielle pour atténuer le préjudice persistant causé aussi bien aux enfants qu'au public. Les images peuvent être dégradantes pour l'enfant et privées, et elles peuvent perturber et choquer le public, ou le désensibiliser. Voilà autant de raisons faisant qu'un mécanisme permettant la saisie est essentiel.

La collaboration des fournisseurs de contenu est essentielle pour prévenir la publication et la diffusion d'images de violence physique à l'égard d'enfants. Ils peuvent bloquer des utilisateurs, des publications et des images, et faire en sorte qu'il soit facile de signaler du contenu, de repérer des tendances, de sensibiliser les utilisateurs et d'établir des politiques internes en fonction de leurs objectifs. Actuellement, les fournisseurs de contenu sont en général des entités privées, qui peuvent seulement retirer du contenu illégal une fois qu'il leur est signalé par des utilisateurs ou sur ordonnance d'un tribunal. Cependant, comme les images de violence physique à l'égard

d’enfants ne sont pas illégales, il n’y a actuellement aucun moyen de les obliger à les retirer de leurs réseaux.

Compétence

Les images de violence physique à l’égard d’enfants sur Internet soulèvent des problèmes de compétence. D’abord, au Canada, aucun organisme en particulier n’a la responsabilité ou le mandat d’intervenir face à de telles images sur Internet. Les autorités compétentes locales peuvent ou non avoir conclu des accords d’entraide dans l’application des lois selon lesquels elles devraient donner suite à des ordonnances de tribunaux canadiens visant des demandes de renseignements ou la suppression de données. Cependant, lorsqu’un autre pays coopère avec les autorités canadiennes, il aurait besoin d’une ordonnance d’un tribunal pour intervenir, donc l’actuelle absence d’interdiction et de pouvoir de saisie exclut cette voie.

Proposition

Aux fins de la présente proposition, il faudra définir dans le *Code criminel* ce que sont des images de violence physique à l’égard d’enfants, et la définition devrait être suffisamment précise pour traduire l’intention de l’interdiction proposée et éliminer la publication d’images de violence physique à l’égard d’enfants sur Internet. Actuellement, la partie V du *Code criminel* contient divers articles de nature semblable à l’interdiction proposée d’images de violence physique à l’égard d’enfants. Cependant, aucune de ces dispositions ne précise adéquatement ce qui est requis pour interdire la publication d’images de violence physique à l’égard d’enfants sur Internet. Dès lors, des modifications seraient nécessaires, par exemple selon les deux scénarios suivants :

Option 1 : Ajout d’un nouveau paragraphe à l’article 163

Dans le premier scénario, un nouveau paragraphe serait ajouté à l’article 163 pour donner une définition de base de ce que sont des images de violence physique à l’égard d’enfants et des actes qui sont interdits à l’égard de telles images. Ces définitions viseraient spécifiquement l’interdiction de publication d’images de violence physique à l’égard d’enfants sur Internet. Comme il s’agirait d’une infraction en vertu de l’article 163, aucune modification ne serait nécessaire à l’article pertinent sur les peines (article 169). Cependant, l’article 164 devrait être modifié pour inclure « images de violence physique à l’égard d’enfants » dans le pouvoir de saisie.

Un paragraphe sur les images de violence physique à l’égard d’enfants pourrait être ajouté à l’article 163 à titre de « paragraphe 163(2.1) » :

> **163**(***2.1***) ***Images de violence physique à l’égard d’enfants***
>
> ***Commet une infraction quiconque publie, rend publique ou transmet, en vue de la rendre accessible au public ou de la publier, une représentation photographique, filmée, vidéo ou audio ou autre représentation sonore ou visuelle où figure une personne âgée de moins de dix-huit ans ou présentée comme telle soumise ou présentée comme étant soumise à des actes de violence ou de mauvais traitements explicites.***

** La modification proposée ci-dessus est fondée sur la formulation du paragraphe 163(1) et de l'article 162.1, avec les adaptations voulues pour interdire expressément la publication d'images de violence physique à l'égard d'enfants sur Internet. **

Option 2 : Nouvelle disposition déterminative

Dans le deuxième scénario, un nouveau paragraphe serait ajouté pour déterminer que des images de violence physique à l'égard d'enfants constituent une forme de contenu « obscène » visée par les dispositions actuelles des paragraphes 163(1) et (2). Cette option utiliserait le texte actuel des paragraphes 163(1) et (2) pour viser l'acte de publier des images de violence physique à l'égard d'enfants sur Internet.

Conclusion

La violence à l'endroit des enfants est un problème urgent pour la société et pour les enfants, auxquels la société veut assurer une protection spéciale en raison de leur vulnérabilité et de leur situation de dépendance. La publication d'images de violence physique à l'égard d'enfants sur Internet est un problème relativement nouveau, soulevant un risque réel de victimisation à répétition des enfants en même temps que de traumatisation et de désensibilisation du public qui ne cherche pas de telles images. Un tel contenu en ligne risque, pour certains, d'avoir l'effet de normaliser, promouvoir et encourager la violence à l'égard des enfants.

Les forces de l'ordre sont empêchées de faire enquête sur de telles affaires ainsi que leur mandat l'exigerait, du fait que, comme cela s'est vu souvent, la technologie Internet et son utilité sociale ont progressé plus rapidement que la loi. La présence sur Internet d'images de violence physique à l'égard d'enfants est l'équivalent d'une affiche matérielle ou d'une annonce télévisée montrant des violences à l'égard d'enfants. La communauté serait d'accord que de telles images sont odieuses et contraires aux normes de tolérance de la collectivité. Cependant, de telles images sont aujourd'hui permises en ligne même si la portée d'Internet est beaucoup plus grande que celle de toute annonce ou affiche matérielle.

Pour parer à la publication sur Internet d'images de violence physique à l'égard d'enfants, la loi doit l'interdire et prévoir des méthodes d'enquête et des pouvoirs de saisie en conséquence. Ce serait possible en modifiant le *Code criminel* pour ajouter une nouvelle disposition interdisant directement la publication de telles images ou déterminant qu'elles constituent du contenu obscène, et en modifiant les dispositions actuelles sur la saisie pour y inclure les images de violence physique à l'égard d'enfants.

Résolution #03 - 2016

DES MESURES LÉGISLATIVES RAISONNABLES FACE AUX IMPLICATIONS DU CHIFFREMENT ET DE LA PROTECTION PAR MOT DE PASSE SUR LES APPAREILS ÉLECTRONIQUES

Présentée par le Comité sur les amendements législatifs

ATTENDU QUE les appareils électroniques sont omniprésents dans les domaines tant licites qu'illicites de la société moderne;

ET ATTENDU QUE les appareils électroniques peuvent être utilisés et sont effectivement utilisés pour faciliter la perpétration de crimes graves et de crimes transfrontaliers, tels que crime organisé, crimes avec violence, fraude et autres crimes financiers, et crimes sur Internet et autres crimes informatiques;

ET ATTENDU QUE la criminalité informatique et sur Internet est un problème croissant qui menace la vie privée et la sécurité des Canadiens ainsi que les systèmes financiers du Canada;

ET ATTENDU QUE le contenu d'appareils électroniques peut receler des preuves de tels crimes;

ET ATTENDU QUE les utilisateurs d'appareils électroniques ont aisément accès à des moyens de chiffrement et de protection par mot de passe qui rendent leur contenu inaccessible aux organismes de sécurité publique même munis d'une autorisation judiciaire de perquisitionner;

ET ATTENDU QUE l'incapacité d'exécuter des mandats de perquisition d'appareils électroniques a entraîné et entraînera encore l'échec d'enquêtes criminelles et d'enquêtes de sécurité nationale;

ET ATTENDU QUE la loi ne prévoit aucun pouvoir visant expressément à contraindre une personne à remettre aux forces de l'ordre ou aux organismes de sécurité nationale le mot de passe ou la clé de chiffrement d'un appareil électronique dont la perquisition a été autorisée par un juge;

ET ATTENDU QUE d'autres pays ont accordé aux organismes d'application de la loi de tels pouvoirs en vertu de la loi et sont parvenus à défendre ces mesures législatives et à promouvoir les intérêts légitimes de l'application de la loi;

ET ATTENDU QUE la demande vise une solution possible;

ET ATTENDU QUE l'Association canadienne des chefs de police, en tant que porte-parole national des dirigeants policiers canadiens, s'emploie à soulever des questions justifiant des modifications au *Code criminel*,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police incite le gouvernement du Canada, aux fins de la sécurité communautaire, à déterminer un moyen législatif permettant aux organismes de sécurité publique et d'application de la loi, sur autorisation judiciaire, de contraindre le détenteur d'une clé de chiffrement ou d'un mot de passe à les révéler aux forces de l'ordre.

Résolution #03 - 2016

DES MESURES LÉGISLATIVES RAISONNABLES FACE AUX IMPLICATIONS DU CHIFFREMENT ET DE LA PROTECTION PAR MOT DE PASSE SUR LES APPAREILS ÉLECTRONIQUES

Contexte

James B. Comey, directeur du Federal Bureau of Investigation, a décrit comme suit l'expérience des États-Unis à l'égard des appareils électroniques aux données chiffrées ou protégées par mot de passe : « Même armés d'un mandat, nous sommes de plus en plus souvent incapables d'accomplir ce que les tribunaux nous ont autorisés à faire et de recueillir des renseignements transmis par des terroristes, des criminels, des pédophiles, des malfaiteurs en tous genres. » Face à la situation, la National District Attorneys Association et l'Association internationale des chefs de police militent en faveur de mesures législatives, dont une ébauche a été publiée le 13 avril 2016, qui contraindraient les entreprises à offrir une « assistance technique » aux forces de l'ordre en ce qui concerne les données chiffrées et protégées par mot de passe.

Au Canada, les forces de l'ordre sont confrontées aux mêmes défis dans leurs enquêtes, et elles ont besoin de mesures législatives semblables. Cependant, des mesures législatives visant les entreprises, dont bon nombre sont situées à l'étranger, ne suffiraient pas nécessairement. Des mesures législatives raisonnables, conformes à la Constitution et adaptées au contexte canadien sont nécessaires à l'application de la loi.

La technologie numérique de la sécurité a progressé au point où des protections impénétrables par mot de passe et par chiffrement se trouvent aisément – et souvent *gratuitement* – pour tous les appareils électroniques. Cette technologie immunise des appareils électroniques légalement saisis contre l'exécution d'un mandat de perquisition et oblige souvent à mettre fin prématurément, sans aboutir, à des enquêtes sur des crimes graves. L'expérience récente des forces de l'ordre révèle des exemples précis d'enquêtes criminelles qui ont ainsi déraillé.

Ce problème peut toucher un large éventail d'enquêtes, mais il a des répercussions en particulier pour les enquêtes sur des agissements en ligne – exploitation sexuelle ou violence physique à l'égard d'enfants, fraude et autres crimes financiers, crime organisé, affaires mettant en jeu l'entraide internationale dans l'application de la loi et affaires de sécurité nationale concernant des cas soupçonnés d'extrémisme et autres menaces pour le Canada.

Les progrès des techniques de cassage de mots de passe ne suffiront pas dans le cas des appareils plus récents, dont le système d'exploitation efface irrémédiablement les données après un certain nombre de tentatives infructueuses de saisir un mot de passe.

Le chiffrement apporte certes de nombreux avantages en matière de vie privée et de cybersécurité, par exemple dans le commerce électronique. Cependant, il est contraire à l'intérêt public de permettre que des criminels ou des individus qui menacent la sécurité des Canadiens créent une zone d'immunité en recourant au chiffrement et à la protection de leurs données par mot de passe et limitent ainsi la portée de mandats judiciaires valides. En revanche, des mesures

législatives raisonnables et proportionnelles permettant aux forces de l'ordre d'accéder à des données chiffrées et protégées par mot de passe, s'il y a lieu, après avoir demandé et obtenu une autorisation judiciaire, accroîtraient la sécurité des enfants canadiens sur Internet, l'intégrité du système financier canadien et la sécurité nationale, et elles aideraient aux enquêtes et aux poursuites visant le crime organisé et des criminels violents. Il faut insister sur ce que les organismes canadiens d'application de la loi ont souligné cette lacune dans la sécurité publique et demandent un processus légal selon lequel une autorisation judiciaire permettrait de contraindre une personne à donner un mot de passe ou une clé de chiffrement. Il est entendu que le recours à ce cadre légal empiétant sur la vie privée devrait être soumis à une règle de proportionnalité.

En janvier 2015, dans une allocution à la Conférence annuelle de l'Association canadienne pour les études de renseignement et de sécurité, en décrivant les défis que pose aux forces de l'ordre le problème élémentaire d'obtenir des renseignements, le commissaire Bob Paulson de la GRC a exprimé cet avis : « Nous avons besoin de nouveaux outils à cet égard, et peut-être même de façon encore plus urgente, afin d'être en mesure d'appliquer les lois criminelles de façon rapide et efficace tout en respectant les valeurs canadiennes et la *Charte canadienne des droits et libertés*. »

Expériences récentes des forces de l'ordre

Divers exemples récents, aux États-Unis et au Canada, illustrent la gravité du problème :

- En 2010-2011, la Police provinciale de l'Ontario faisait enquête sur un homme qui aurait dissimulé des caméras dans sa maison pour espionner une jeune femme travaillant pour son épouse. La police a obtenu un mandat de perquisition, fouillé la maison et trouvé une unité de disque dur cachée au sous-sol. L'Unité de la lutte contre la criminalité technologique n'est pas parvenue à percer le chiffrement. La police a par la suite trouvé des documents et des livres contenant des renseignements sur le matériel informatique du suspect, y compris une série de possibles mots de passe. Un d'eux a permis de déverrouiller le disque dur. Des milliers d'images voyeuristes ont été découvertes sur l'appareil. L'enquêteur a expliqué que l'enquête aurait échoué si le suspect n'avait pas inscrit le mot de passe dans les documents trouvés.

- En 2012, la police a saisi légalement des ordinateurs de Justin Gryba, à Saskatoon, dans le cadre d'une enquête concernant la pornographie juvénile. M. Gryba a refusé de fournir les mots de passe. Des techniciens en criminalistique de Saskatoon et d'Ottawa ne sont parvenus à percer le chiffrement d'un des appareils que deux ans et demi plus tard. L'appareil contenait de la pornographie juvénile représentant de nombreuses victimes. M. Gryba a été accusé de production et possession de pornographie juvénile. Le 15 avril 2016, il a été condamné à deux ans moins un jour d'incarcération (en supplément d'un crédit de 29 mois).

- En mai 2013, la Police provinciale de l'Ontario a reçu des indications qu'un individu possédait de la pornographie juvénile sur son appareil Apple iPad et peut-être sur son ordinateur Apple Macbook Pro. Un mandat a été exécuté à la résidence de l'individu, et les appareils ont été saisis. Les appareils ont été soumis à l'Unité de la lutte contre la criminalité technologique de la PPO pour examen et récupération de toutes images. Les deux appareils étaient protégés par mot de passe. L'Unité n'avait pas le moyen d'y accéder sans le mot de passe. L'enquêteur n'a pas pu obtenir d'ordonnances de communication et d'assistance visant Apple en Californie, et n'était pas disposé à envoyer les appareils en Californie compte tenu de leur probable contenu illégal. L'enquêteur n'a pas pu davantage obtenir une ordonnance de destruction, et a dû prendre des dispositions pour rendre les appareils au suspect. Des conditions ont été négociées à cette fin : le suspect fournirait le mot de passe afin que les appareils puissent être purgés avant d'être rendus, et aucune accusation ne serait portée.

- Entre octobre 2014 et juin 2015, les forces de l'ordre ont saisi à Manhattan (New York) 74 appareils Apple iPhone dans le cadre d'enquêtes sur des infractions telles que trois tentatives de meurtre, exploitation sexuelle persistante d'un enfant, réseau de trafic sexuel et nombre d'agressions et vols. Des mandats de perquisition des appareils ont été obtenus, mais aucun n'a pu être exécuté.

- À Fort Frances (Ontario), il y a récemment eu vol de stupéfiants d'un hôpital. Un téléphone a été saisi et transmis à l'Unité de la lutte contre la criminalité technologique de la Police provinciale de l'Ontario, qui n'est pas parvenue à le déverrouiller. L'enquête a abouti dans une impasse, quoique les spécialistes pensaient éventuellement pouvoir utiliser un nouveau logiciel pour déverrouiller le téléphone, dans 8 à 12 mois.

- En juin 2015, un homme, père de six enfants, a été abattu à Evanston (Illinois), 10 milles au nord de Chicago. Il n'y avait ni témoins ni images vidéo de surveillance. Les enquêteurs ont trouvé près du cadavre un téléphone Apple iPhone et un téléphone Samsung doté du système d'exploitation Android de Google. Les deux appareils étaient protégés par mot de passe. Un juge de l'État de l'Illinois a délivré un mandat ordonnant à Apple et à Google de déverrouiller les téléphones et de communiquer aux autorités toutes données qui pourraient élucider le meurtre. Apple et Google ont répondu qu'ils ne pouvaient pas le faire sans connaître le mot de passe de l'utilisateur. Le meurtre n'a pas été résolu.

Solutions possibles : L'expérience d'autres pays

Au Canada, les forces de l'ordre peuvent selon le cas exiger la production de données biométriques en vertu d'un mandat relatif à l'obtention d'empreintes (art. 487.092) ou d'un mandat général (art. 487.01), mais pas la communication de mots de passe ou de clés de chiffrement. D'autres pays ont examiné ou mis en place des mesures législatives permettant d'exiger cette communication :

- Au Royaume-Uni, la *Regulation of Investigatory Powers Act 2000* habilite le tribunal à ordonner qu'une personne fournisse des renseignements non chiffrés ou des clés de chiffrement. La loi a été contestée au nom de la protection contre l'auto-incrimination, mais sans succès.

- La *Cybercrime Act 2001* de l'Australie autorise un magistrat à ordonner qu'une personne, y compris un suspect ou une personne accusée, fournisse toute information ou toute aide raisonnables et nécessaires pour que les forces de l'ordre puissent accéder à des données électroniques, les copier et les convertir. Elle prévoit une pénalité pour défaut d'obtempérer.

- Des dispositions sur la communication de clés sont en vigueur en Afrique du Sud (*Regulation of Interception of Communications and Provision of Communication-Related Information Act*), en France (*Loi sur la sécurité quotidienne*) et en Finlande (*Pakkokeinolaki (loi sur les mesures coercitives)*).

- La Suède a récemment proposé des mesures législatives sur la communication de clés de chiffrement.

- Les Douanes de Nouvelle-Zélande ont publié en 2015 un document de discussion proposant de prévoir dans la *Customs and Excise Act* de nouveaux pouvoirs permettant d'exiger les mots de passe de personnes franchissant la frontière.

- Les États-Unis n'ont pas encore souscrit pleinement au principe de la communication des clés, mais il y a eu des cas où des juges ont ordonné à des personnes accusées de fournir leurs mots de passe aux forces de l'ordre. Les tribunaux américains n'ont pas statué de façon définitive sur la mesure dans laquelle l'obligation de fournir une clé ou une copie non chiffrée de données chiffrées viole la protection contre l'auto-incrimination assurée par le Cinquième Amendement de la Constitution.

  Cependant, le 13 avril 2016, le président du Comité du Sénat américain sur le renseignement Richard Burr et la sénatrice Dianne Feinstein ont publié un projet de loi préliminaire (*Compliance with Court Orders Act of 2016*) qui traiterait de la question des appareils chiffrés ou protégés par mot de passe en exigeant que l'entreprise pertinente déchiffre les données ou fournisse une assistance technique aux forces de l'ordre. La proposition est soutenue par la National District Attorneys Association et l'Association internationale des chefs de police.

Précisions sur les mesures législatives du Royaume-Uni

Les mesures législatives du Royaume-Uni méritent une attention particulière parce qu'elles comprennent des dispositions bien établies sur la communication de clés de chiffrement/mots de passe et que nous partageons des principes juridiques et constitutionnels communs. Un résumé des données des rapports annuels de l'Office of Surveillance Commissioners (OSC) permet de jauger l'efficacité de ces mesures législatives. L'OSC est un organisme public qui, sous l'égide du Home Office, supervise le recours à la surveillance secrète et à des sources secrètes de

renseignement humain par des autorités publiques, en vertu de la *Regulation of Investigatory Powers Act 2000* (RIPA).

L'article 49 de la RIPA, activé par décret ministériel en octobre 2007, exige que des personnes fournissent des renseignements non chiffrés ou des clés de chiffrement aux représentants de l'État sur réception d'une ordonnance d'un tribunal. Dans la pratique, une demande en ce sens comporte les étapes suivantes :

- Le National Technical Assistance Centre (NTAC) du Home Office doit approuver une demande de signification d'un avis au titre de l'article 49.
- Une fois l'approbation du NTAC acquise, une permission peut être demandée à un juge.
- Une fois la permission d'un juge acquise, l'avis au titre de l'article 49 est signifié.
- Si une personne refuse de se conformer à l'avis au titre de l'article 49, une accusation criminelle peut être déposée.

L'OSC fait état du recours à l'article 49 dans chacun de ses rapports annuels depuis 2008-2009. Le plus récent rapport est celui de 2014-2015. Selon les données de 2008 à 2015 :

- 160 avis ont été signifiés en vertu de l'article 49 de la RIPA.
    - Les enquêtes concernent généralement des affaires de terrorisme, d'extrémisme au pays, d'images indécentes d'enfants, de délits d'initié, de fraude, d'évasion de droits d'accise et de drogues.
    - Les enquêtes sur la traite des personnes et l'enlèvement d'enfants semblent être en hausse.
- Entre 38 et 42 individus (~24 % à ~26 %) se sont conformés à l'avis[1].
- 93 individus (~58 %) ne se sont pas conformés à l'avis[2].
- 68 de ces personnes ont fait l'objet d'accusations.
- 46 de ces personnes ont été poursuivies.
- 14 poursuites ont mené à des condamnations.

[1] Le rapport 2008-2009 ne précise pas le nombre d'avis qui ont été respectés ou qui restent en instance. Comme le rapport indique que 15 avis ont été signifiés et que 11 avis n'ont pas été respectés, cette estimation tient compte du nombre minimum (0) et du nombre maximum (4) de personnes qui pourraient avoir obtempéré.

[2] Ce pourcentage ne tient pas compte des avis qui restent en instance. Les pourcentages annuels d'avis non respectés ont une valeur explicative incertaine, compte tenu du chevauchement des données entre les années. Dans la mesure où elles sont utiles à titre indicatif, elles se présentent comme suit :

- 2008-2009 (~73 %);
- 2009-2010 (~41 %);
- 2010-2011 (~17 %);
- 2011-2012 (~75 %);
- 2012-2013 (~73 %);
- 2013-2014 (~52 %);
- 2014-2015 (~59 %).

Résolution #04 - 2016

ACCROÎTRE LES MESURES VISANT À LIMITER L'ACCÈS À DES CIBLES RÉACTIVES ET LEUR UTILISATION AU CANADA

Présentée par le Comité sur les amendements législatifs

ATTENDU QUE les cibles réactives, aussi appelées cibles explosives, sont expressément conçues pour exploser lorsqu'elles sont atteintes par un projectile d'une carabine de grande puissance ou de puissance normale et sont utilisées dans le tir à la cible à grande distance;

ET ATTENDU QU'une cible réactive est un mélange binaire vendu au Canada sous forme de trousses multi-ingrédients. Lorsque les ingrédients sont mélangés, ils produisent une puissante explosion. En l'occurrence, une cible réactive a une puissance explosive d'environ 0,82, en équivalence TNT[3];

ET ATTENDU QUE les cibles réactives sont soumises au *Règlement de 2013 sur les explosifs* et peuvent être vendues en ligne ainsi que par des établissements de commerce de détail à des personnes possédant un permis de possession et d'acquisition d'armes à feu ou un certificat de technicien en pyrotechnie en règle;

ET ATTENDU QUE selon la réglementation actuelle, une personne peut acheter, transporter et stocker jusqu'à 20 kg de cibles réactives à la fois sans autre permis ou licence;

ET ATTENDU QUE même si les cibles réactives sont destinées au tir à la cible à grande distance, il se trouve sur Internet et les médias sociaux de nombreux exemples d'utilisations abusives, au Canada et dans d'autres pays;

ET ATTENDU QUE la police, au Canada, a fait enquête sur de nombreux cas d'utilisation abusive ou criminelle de cibles réactives, y compris comme engins explosifs improvisés (EEI);

ET ATTENDU QUE selon des recherches et des essais effectués au Canada par la police et des partenaires en matière de sécurité, les cibles réactives peuvent aisément être transformées en armes et intégrées à des EEI puissants et destructeurs à des fins criminelles et terroristes;

[3] L'équivalence TNT est une mesure conventionnelle de l'énergie libérée par une explosion.

ET ATTENDU QUE les cibles réactives posent une menace directe pour la sécurité du public et des premiers intervenants du fait qu'elles fournissent un moyen sûr de fabriquer des explosifs artisanaux,

IL EST DONC RÉSOLU QUE l'Association canadienne des chefs de police incite les gouvernements fédéral, provinciaux et territoriaux à prévenir l'utilisation abusive, criminelle et terroriste de cibles réactives en resserrant les mesures afin d'y limiter l'accès et d'en limiter l'utilisation au Canada.

Résolution #04 - 2016

ACCROÎTRE LES MESURES VISANT À LIMITER L'ACCÈS À DES CIBLES RÉACTIVES ET LEUR UTILISATION AU CANADA

Contexte

Les cibles réactives, ou cibles explosives, sont expressément conçues pour exploser lorsqu'elles sont atteintes par un projectile d'une carabine de grande puissance ou de puissance normale et sont utilisées dans le tir à la cible à grande distance. Les cibles réactives permettent ainsi au tireur pratiquant le tir à la cible à grande distance de constater qu'il a bien atteint sa cible.

Une cible réactive est un mélange binaire vendu au Canada sous forme de trousses multi-ingrédients, sous diverses marques de commerce telles que Tannerite, Thundershot, Sure Shot, KaBoom et Shockwave. Un explosif binaire est composé de deux éléments, dont ni l'un ni l'autre n'est explosif en soi. Dans les cibles réactives, les deux éléments sont du nitrate d'ammonium ou un mélange de nitrate d'ammonium et de perchlorate potassique (partie A) et une poudre d'aluminium ou d'alliage de magnalium (partie B). Lorsque les parties A et B sont combinées, une forte explosion est produite. En l'occurrence, une cible réactive a une puissance explosive d'environ 0,82, en équivalence TNT.

Au Canada, l'acquisition, le transport, le stockage et l'utilisation de cibles réactives est soumise au *Règlement de 2013 sur les explosifs*. En octobre 2014, la Direction de la sécurité et de la sûreté des explosifs de Ressources naturelles Canada (RNCan), a publié des lignes directrices sur la vente de cibles réactives[4]. Une personne possédant un permis de possession et d'acquisition d'armes à feu ou un certificat de technicien en pyrotechnie en règle peut acheter, transporter, stocker et utiliser jusqu'à 20 kg de cibles réactives. Des quantités dépassant la limite de 20 kg peuvent être achetées et stockées par le détenteur d'une licence de poudrière, délivrée par RNCan et assortie de droits annuels de 70 $.

Même si les cibles réactives sont destinées au tir à la cible à grande distance, il se trouve sur Internet et les médias sociaux de nombreux exemples d'utilisations abusives, au Canada et dans d'autres pays. Bien que ce soit contraire aux indications des fabricants et aux lignes directrices réglementaires, des cibles réactives sont combinées pour produire des explosions suffisamment puissantes pour détruire des immeubles et des véhicules, et de blesser gravement des personnes et des animaux. Des vidéos accessibles au public, au Canada et aux États-Unis, démontrent le potentiel destructeur de cibles réactives utilisées abusivement.

- Des échos de coups de feu et de cibles explosives suscitent la peur chez les résidents (Canada) – http://globalnews.ca/video/2655114/echoes-of-gunfire-and-exploding-targets-trigger-residents-fears

[4] www.rncan.gc.ca/explosifs/publications/lignes-directrices/16730

- 4 lb de cibles explosives Thundershot (Canada) – https://www.youtube.com/watch?v=_hZRbLBn2K8

- 164 lb de Tannerite détruisent une grange (États-Unis) – https://www.youtube.com/watch?v=edRbcTXAijY

- 250 lb de cibles explosives (États-Unis) – https://www.youtube.com/watch?v=osrWmQtyatw

- Pulvériser une voiture avec 50 lb de Tannerite (États-Unis) – https://www.youtube.com/watch?v=7DK_pw2tq2Q

- 40 lb de Tannerite contre une Jetta (États-Unis) – https://www.youtube.com/watch?v=-oyoY_5Vp64

Face au risque de déclencher des feux de forêt et aux menaces pour la sécurité publique, le Service des forêts des États-Unis a interdit l'utilisation de cibles réactives sur les terres forestières nationales. Sur une période de deux ans (2012 à 2014), les cibles réactives ont été liées à de nombreux feux dans les forêts nationales des États-Unis, et à des frais de quelque 30 millions de dollars en lutte contre l'incendie[5].

Les cibles réactives préoccupent les organismes américains d'application de la loi. En mars 2013, le FBI a publié un bulletin mettant en garde contre le risque d'utilisation illicite de cibles réactives par des criminels et des extrémistes[6]. Les forces de l'ordre américaines ont d'ailleurs découvert des cas d'utilisation de cibles réactives dans des EEI tels que mines Claymore et bombes tuyaux.

En plus d'utilisations abusives de cibles réactives rapportées par les médias[7, 8], les organismes canadiens d'application de la loi ont aussi constaté des utilisations abusives et criminelles :

- **Avril 2016 :** À la suite d'une interception routière et de la perquisition ultérieure d'une résidence, deux EEI ont été saisis et des mélanges de cibles réactives ont été découverts[9].
- **Depuis 2014 :** L'utilisation criminelle de cibles réactives a été mise en cause dans quatre enquêtes de la GRC sur la destruction de biens, par suite de l'examen de restes d'explosif[10].
- **Mai 2012 :** La GRC a porté des accusations contre deux personnes qui avaient tiré des coups de feu sur 6 lb de cibles réactives dans une laveuse. Le feu qui en a résulté a

[5] http://gazette.com/u.s.-forest-service-to-ban-exploding-targets-in-colorado/article/1504412
[6] https://publicintelligence.net/fbi-exploding-targets/
[7] www.cbc.ca/news/canada/manitoba/neighbours-tackle-trash-at-seddons-corner-cleanup-1.3100513
[8] http://globalnews.ca/news/2655045/litter-vandalism-in-ghost-valley-are-growing-concern/
[9] www.cbc.ca/news/canada/edmonton/speeding-driver-in-edmonton-caught-with-drugs-guns-and-explosives-1.3552490
[10] www.wltribune.com/news/284005611.html?mobile=true

> occasionné des dommages de 30 000 $ à des biens, et il en a coûté 60 000 $ pour l'éteindre[11].

Fait important, selon des recherches et des essais effectués au Canada par la police et des partenaires en matière de sécurité, les cibles réactives peuvent aisément être transformées en armes et intégrées à des EEI puissants et destructeurs à des fins criminelles et terroristes.

Malgré la réglementation canadienne, l'Association canadienne des chefs de police croit que les cibles réactives posent une menace directe pour la sécurité du public et des premiers intervenants du fait qu'elles fournissent un moyen sûr de fabriquer des explosifs artisanaux. Compte tenu de ces préoccupations, l'Association canadienne des chefs de police incite les gouvernements fédéral, provinciaux et territoriaux à prévenir l'utilisation abusive, criminelle et terroriste de cibles réactives en resserrant les mesures afin d'y limiter l'accès et d'en limiter l'utilisation au Canada.

[11] www.comoxvalleyrecord.com/news/160620805.html?mobile=true