# Études Internationales ACCP 2015

## Un guide pour l'action policière contre le cybercrime au Canada

CACP EXECUTIVE GLOBAL STUDIES PROGRAM

PROGRAMME D'ÉTUDES INTERNATIONALES POUR CADRES SUPÉRIEURS ACCP

## TROIS VÉRITÉS SUR LA CYBERCRIMINALITÉ

### LA CYBERCRIMINALITÉ EST UN ACTE CRIMINEL

- Elle fait des victimes réelles, qui subissent des effets dévastateurs.
- Elle est souvent liée au crime organisé ou à d'autres formes de criminalité.
- Elle est une menace pour la primauté du droit.

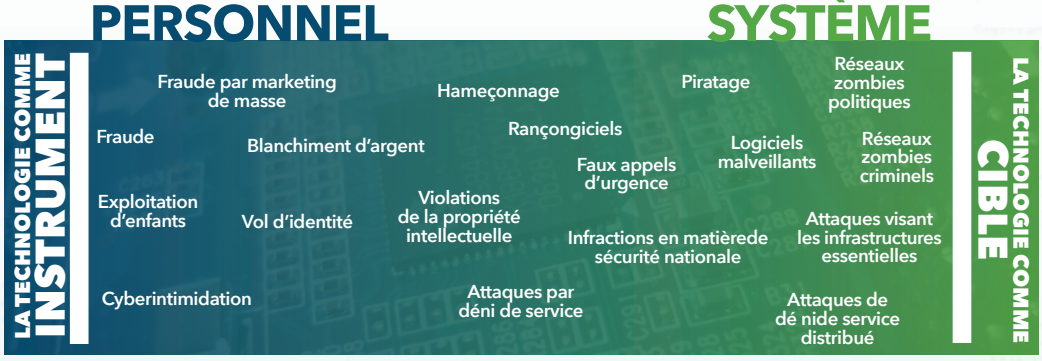
### LA CYBERCRIMINALITÉ EST UNE PRIORITÉ POUR LA SÉCURITÉ DES COLLECTIVITÉS:

- Elle n'est pas toujours déclarée et fait trop rarement l'objet d'enquêtes.
- Elle cause un tort véritable à nos collectivités.
- Son intensité augmente rapidement.
- Les avancées technologiques ne feront que l'aggraver.

### LES SERVICES DE POLICE DE TOUS LES NIVEAUX PEUVENT ENGAGER DES ACTIONS EN JUSTICE

- Quand il y a une démarche de collaboration;
- Quand il y a de la coordination
- Quand la police possède les connaissances et les aptitudes nécessaires

## LE CHAMP D'ACTION DE LA POLICE FACE AU CYBERCRIME




Problèmes mieux compris de la police
Interventions de généralistes requises

Problèmes moins compris de la police
Interventions de spécialistes requises

**Le cybercrime prend bien des formes. Toutes sont criminelles.**

## GLOSSAIRE

### RÉSEAU ZOMBIE
Un ensemble d'ordinateurs compromis (zombies) exécutant des applications malicieuses à l'insu de l'utilisateur, par le biais d'une infrastructure de commandement et de contrôle.

### HARMONISATION
Dans le contexte de la cybercriminalité, chercher à éliminer le double emploi, l'interférence ou les conflits entre les enquêtes, les interventions et les systèmes de différents organismes d'application de la loi.

### ATTAQUE PAR DÉNI DE SERVICE
Type de cyberattaque visant à causer une surcharge ou autrement entraver la capacité du système visé de recevoir de l'information et de communiquer avec d'autres systèmes.

### ATTAQUE DE DÉNI DE SERVICE DISTRIBUÉ
Type d'attaque où un ordinateur et une connexion Internet sont utilisés pour submerger un serveur de données afin de surcharger sa bande passante et ses ressources. Une telle attaque recourt simultanément à un grand nombre d'ordinateurs et de connexions Internet, souvent réparties dans le monde entier, et souvent détournés par un réseau zombie (voir réseau zombie).

### PIRATE INFORMATIQUE
Personne qui utilise des ordinateurs et Internet pour accéder à d'autres ordinateurs et des serveurs sans permission.

### LOGICIELS MALVEILLANTS
Logiciels conçus pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Exemples : virus informatique, ver informatique, cheval de Troie, logiciel espion, publiciel.

### RANÇONGICIELS
Logiciel qui empêche un utilisateur d'accéder à ses fichiers avant qu'il ne paie une rançon.

### FAUX APPELS D'URGENCE
Mauvais tour/crime où une personne trouve votre adresse au moyen de votre protocole Internet ou connaît votre nom et votre adresse, et fait un appel anonyme au 911 pour faussement signaler une urgence.

## NOUS POUVONS TOUS EN FAIRE PLUS – UN CHANGEMENT DE FOND S'IMPOSE POUR LA POLICE AU CANADA

### INTERVENTION À L'ÉCHELLE LOCALE OU PROVINCIALE

### INTERVENTION À L'ÉCHELLE NATIONALE

#### CYBERCRIMINALITÉ COURANTE

- Accroître les capacités d'enquête des unités de première ligne
- Former les policiers en contact avec le public pour qu'ils fassent comprendre à la population que la cybercriminalité est un crime et pour qu'ils l'encouragent à déclarer ces actes criminels

- L'ACCP devrait participer davantage et de façon plus visible au Mois national de la sensibilisation à la cybersécurité au Canada (en octobre de chaque année), comme elle le fait lors de la Journée nationale de retour des médicaments.

#### ACCROÎTRE LA SENSIBILISATION ET LE SOUTIEN AUX VICTIMES

- Lancer une campagne d'information dans votre territoire de compétence sur votre rôle face au cybercrime
- Veiller à ce que les agents de première ligne sachent diriger les victimes vers des outils et des ressources de soutien.
- Faire en sorte que les outils de déclaration en ligne permettent de signaler les actes de cybercriminalité.
- Promouvoir la prudence en ligne chez les jeunes (de la même façon que la prudence sur la route)
- Créer des liens avec des initiatives comme pensezcybersecurite.ca et cyberaide.ca

- Créer un modèle de collaboration intersectorielle et avec le secteur privé (PPP – partenariats public-privé) fondé sur la confiance
- Idéal: regroupement dans un cadre intégré doté de protocoles officiels et appropriés d'échange d'information
- Faire fond sur les structures et initiatives actuelles (p. ex., Centre national de coordination contre l'exploitation des enfants, Programme de gestion conjointe de la résilience opérationnelle, National Cyber Forensics Training Alliance (Canada), Centre canadien de réponse aux incidents cybernétiques), en tirer parti, les restructurer et les réorienter en vue d'une consolidation

#### ACCROÎTRE LA COLLABORATION DES PARTENAIRES NON POLICIERS

- Créer des cadres d'échange raisonnable de renseignements entre intervenants clés et établir la confiance entre eux
- Mettre en place des mécanismes nationaux ou régionaux de collaboration et y participerr

#### ASSURER LA COORDINATION POLICIÈRE

- Fournir des ressources, de l'expertise, de l'expérience locale et des données à des structures nationales ou régionales de lutte contre le cybercrime

- Créer des mécanismes et des structures pour assurer la coordination et l'échange d'information à tous les paliers
- Clarifier les rôles et responsabilités des corps de police locaux, provinciaux et fédéraux face aux actes de cybercriminalité qui touchent plusieurs territoires de compétence

#### REHAUSSER LES CAPACITÉS DU SYSTÈME DANS SON ENSEMBLE

- Créer des équipes d'enquête régionales pour les cybercrimes « purs » complexes (échelle provinciale)
- Doter les unités d'enquête locales d'une cybercapacité
- Intégrer les rudiments du cybercrime dans la formation de toutes les recrues
- Demander des outils de criminalistique numérique pour les agents de première ligne
- Lancer des modèles non traditionnels de recrutement, de fidélisation du personnel et de prestation de services
- Tirer parti de l'expertise locale de bénévole dans le cadre de forces auxiliaires

- Créer des séances de formation continue spécialisée
- Lancer des modèles non traditionnels de recrutement, de fidélisation du personnel et de prestation de services
- Sensibiliser les avocats de la Couronne et encourager la spécialisation des procureurs

#### DEMANDER DES CHANGEMENTS DANS LES POLITIQUES ET LES LOIS

- Discuter avec les dirigeants locaux et provinciaux des répercussions de la cybercriminalité sur les collectivités qui font partie de votre territoire de compétence

- Demander des normes de préservation des données (1 an au minimum)
- Demander des ordonnances de communication visant des données étrangères
- Demander des exigences de déclaration des actes de cybercriminalité
- Demander l'applicabilité de l'extraterritorialité pour les attaques criminelles visant des cybersystèmes vitaux
- Continuer de demander l'accès légal
- Continuer de demander une réforme des traités d'entraide juridique

**Chaque corps de police canadien devrait faire la promotion de ces ressources dans chaque collectivité: www.pensezcybersecurite.gc.ca**

# CACP RÉSOLUTION #07-2015

## CYBERCRIMINALITÉ : RÔLES ET RESPONSABILITÉS DE LA POLICE DANS UN CADRE NATIONAL DE COLLABORATION

Présentée par: Norm Taylor, directeur, Programme d'études internationales pour cadres supérieurs de l'ACCP

**ATTENDU QUE** comme le proposait la résolution 03 2012, et par le travail soutenu du Comité sur la cybercriminalité, l'ACCP a demandé au gouvernement du Canada ainsi qu'à ses partenaires du secteur public et du secteur privé d'élaborer une Stratégie nationale de lutte contre la cybercriminalité pour entraver la cybercriminalité;

**ET ATTENDU QU'**en août 2014, le conseil d'administration de l'ACCP a insisté sur l'importance croissante de la cybercriminalité, affirmant que le phénomène remet en cause les compétences, les aptitudes, les rôles et les modes d'intervention traditionnels de la police, et que la nécessité d'une action nationale cohérente devient une priorité pour les dirigeants policiers;

**ET ATTENDU QUE** les données empiriques actuelles indiquent que pour parer à la victimisation causée par la cybercriminalité, il faut une collaboration efficace entre de nombreux acteurs, et les services de police à tous les niveaux partagent des responsabilités qui leur sont propres en ce qui concerne la protection des citoyens et la défense de la primauté du droit;

**ET ATTENDU QUE** le conseil d'administration a déterminé que le Programme 2015 d'études internationales pour cadres supérieurs de l'ACCP devrait se pencher sur les moyens à prévoir au Canada contre la cybercriminalité et sur la façon dont certains pays choisis ont abordé la question afin de discerner les rôles les plus efficaces que peut jouer la police au sein d'un cadre de collaboration;

**ET ATTENDU QU'**en mai 2015, à l'issue de travaux de recherche et d'entrevues sur le terrain dans neuf pays avec presque 100 spécialistes des milieux policier, gouvernemental et universitaire et du secteur privé, la cohorte des études internationales a conclu que la voie la plus prometteuse pour l'action des forces de l'ordre face à la cybercriminalité comprend les aspects suivants :

(1) Aborder la cybercriminalité comme une question policière fondamentale,
(2) Désigner la cybercriminalité comme une priorité actuelle en matière de sécurité des collectivités,
(3) Reconnaître que malgré sa complexité, la cybercriminalité peut être attaquée dans une certaine mesure par tous les paliers des services policiers;

**ET ATTENDU QUE** l'expérience d'autres pays et l'analyse émergente de la situation au Canada confirment que les tendances de la victimisation, le tort croissant causé aux collectivités et les menaces à l'endroit de la primauté du droit, qui sont tous alimentés par les progrès constants et rapides de la technologie, justifient une action réfléchie, cohérente et soutenue de la part de tous les paliers des services policiers au Canada;

**ET ATTENDU QUE** l'ACCP et ses membres, en adoptant la présente résolution, reconnaissent que toute « cybercriminalité », quelles que soient ses motivations sous-jacentes, ses sources ou les formes qu'elle prend, est effectivement un crime et que, comme tout crime, elle fait des victimes qui méritent notre attention. Malgré la complexité en jeu et la nécessité de vastes stratégies de collaboration qui doivent projeter les capacités d'action nationale bien au-delà des seuls services policiers, **les corps policiers à tous les niveaux continuent d'avoir le devoir, dans la mesure de leurs capacités, de poursuivre les cybercriminels et de protéger leurs collectivités,**

**IL EST DONC RÉSOLU QUE…**

**L'Association canadienne des chefs de police demande à ses partenaires, à leurs associations et aux intervenants fédéraux-provinciaux-territoriaux** de travailler avec elle afin d'accélérer l'élaboration et l'adoption d'une Stratégie nationale de lutte contre la cybercriminalité, comme le prévoyait la résolution 03 2012, y compris des cadres de référence, des mécanismes et une structure qui mèneront à une meilleure coordination nationale parmi les organismes d'application de la loi ainsi qu'entre eux et les gouvernements, le milieu universitaire et le secteur privé;

**IL EST EN OUTRE RÉSOLU QUE…**

**L'Association canadienne des chefs de police demande au gouvernement fédéral de mettre davantage l'accent sur la cybercriminalité,** conformément aux principes énoncés ci-dessus, la prochaine fois qu'il mettra à jour la Stratégie de cybersécurité du Canada (2010);

**IL EST EN OUTRE RÉSOLU QUE…**

**L'Association canadienne des chefs de police demande à ses partenaires à leurs associations et aux intervenants fédéraux-provinciaux-territoriaux de militer collectivement en faveur de changements** dans les lois, la réglementation et les politiques qui accroîtront l'efficacité et l'efficience des enquêtes, augmenteront les risques et les conséquences pour les délinquants, et faciliteront le travail de la police dans divers domaines, y compris en ce qui concerne : les exigences de déclaration; les normes sur la préservation des données; l'entraide judiciaire internationale; les ordonnances de communication visant des données étrangères; la modernisation de l'accès légal; et la capacité d'action extraterritoriale à l'égard de certains cybersystèmes vitaux.