GRC
GENDARMERIE ROYALE DU CANADA

Cybercriminalité :
SURVOL DES INCIDENTS ET DES ENJEUX AU CANADA

Gendarmerie royale du Canada
Royal Canadian Mounted Police

Canada

Cat. no.: PS64-116/2014F-PDF
ISBN: 978-0-660-22309-4

Résumé

Le présent rapport, *Cybercriminalité : survol des incidents et des enjeux au Canada*, est le premier de la GRC à traiter de la cybercriminalité. Il est axé sur les aspects de la cybercriminalité qui ont une incidence réelle et préjudiciable sur les organismes du secteur public, les entreprises et les citoyens du Canada.

Le rapport porte sur une vaste gamme d'infractions criminelles lors desquelles on a recours à Internet et à des technologies de l'information pour s'adonner à des activités illégales. On y fait la description d'actes criminels triés sur le volet qui sont commis dans le paysage numérique du Canada, et ce, afin de donner une idée de la complexité technique croissante, de la sophistication et de l'expansion de la criminalité. Biens qu'ils soient difficiles à évaluer, ces crimes ne montrent aucun signe de ralentissement au Canada.

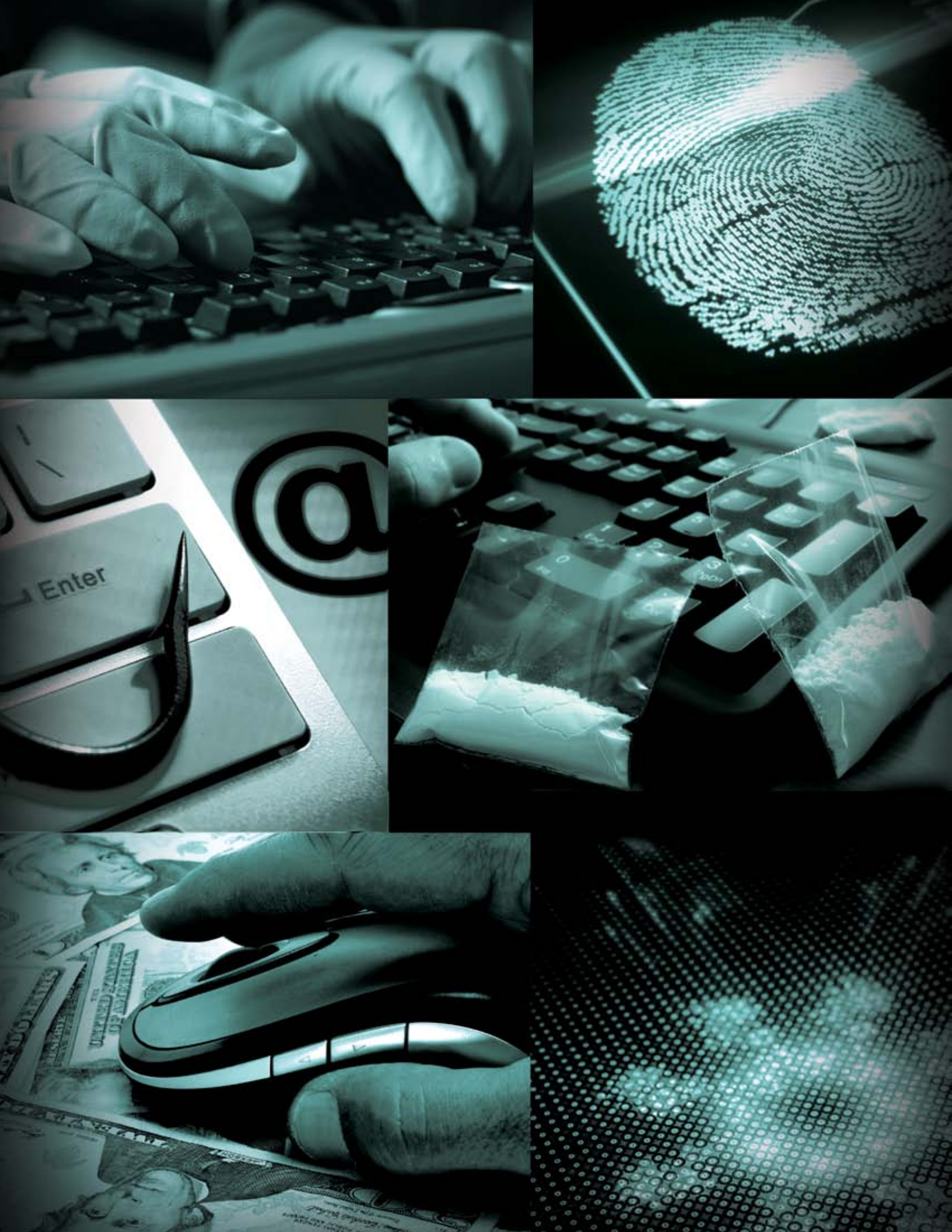
La GRC divise les actes de cybercriminalité en deux catégories :

- ***infractions où la technologie est la cible*** – actes criminels qui ciblent des ordinateurs et d'autres technologies de l'information, comme ceux qui concernent l'utilisation non autorisée d'ordinateurs ou les méfaits concernant des données;
- ***infractions où la technologie est l'instrument*** – actes criminels commis à l'aide d'Internet ou de technologies de l'information, comme la fraude, le vol d'identité, la violation de propriété intellectuelle, le blanchiment d'argent, le trafic de drogues, la traite de personnes, les activités du crime organisé, l'exploitation sexuelle des enfants ou la cyberintimidation.

Le rapport traite de ces catégories et il présente des exemples et des études de cas de l'application de la loi associés à des menaces récentes en matière de cybercriminalité. Le rapport se termine par trois principales observations :

- ***La technologie crée de nouvelles possibilités pour les criminels.*** Les marchés électroniques et les dispositifs reliés à Internet offrent les mêmes possibilités aux réseaux criminels organisés qu'aux entreprises légitimes.
- ***La cybercriminalité prend de l'ampleur.*** Autrefois considérée comme le domaine des criminels possédant des compétences spécialisées, la cybercriminalité est maintenant à la portée d'autres délinquants puisque le savoir requis est maintenant plus accessible.
- ***La cybercriminalité oblige la police à adopter de nouvelles méthodes.*** L'exploitation criminelle des nouvelles technologies – comme l'informatique en nuage, les médias sociaux, les réseaux anonymes en ligne et les fraudes liées à une devise virtuelle – exige de nouvelles mesures policières pour ne pas se laisser distancer à l'ère numérique.

Le présent rapport et les versions ultérieures informeront les Canadiens des menaces criminelles et des tendances dans le cyberespace, de même que des efforts faits par les organismes d'application de la loi pour les combattre.


Enter

Dans le rapport

DÉFINITION DE LA CYBERCRIMINALITÉ DU POINT DE VUE DE L'APPLICATION DE LA LOI

Selon la GRC, un cybercrime peut être n'importe quel type de crime commis en grande partie à l'aide d'Internet et des technologies de l'information, comme des ordinateurs, des assistants numériques personnels ou des appareils mobiles. On entend aussi par cybercrime les crimes sophistiqués sur le plan technique qui exploitent les failles des technologies numériques, tout comme les crimes plus traditionnels qui prennent de nouvelles formes dans le cyberespace. Le fait de considérer la cybercriminalité dans une perspective plus vaste est essentiel pour déterminer l'intervention qui convient le mieux, qu'il s'agisse de mettre en cause des organismes d'application de la loi ou d'autres mesures de cybersécurité.

La cybercriminalité peut être divisée en deux catégories :

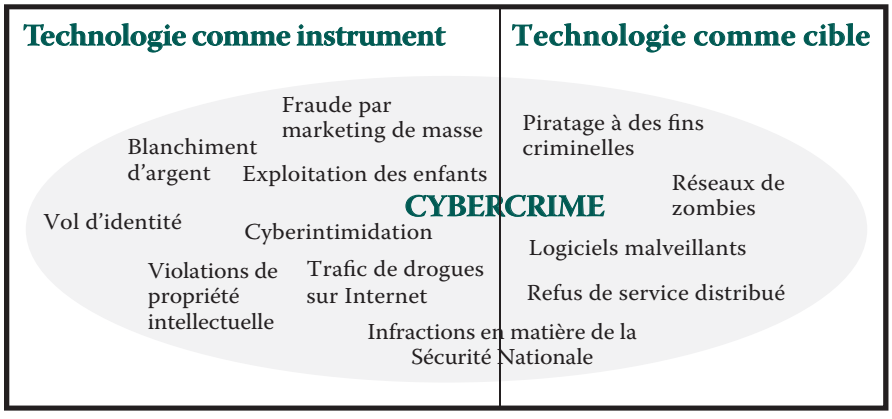
- ***infractions où la technologie est la cible*** – actes criminels qui ciblent des ordinateurs et d'autres technologies de l'information, comme ceux qui concernent l'utilisation non autorisée d'ordinateurs ou les méfaits concernant des données;

- ***infractions où la technologie est l'instrument*** – actes criminels commis à l'aide d'Internet ou de technologies de l'information, comme la fraude, le vol d'identité, la violation de propriété intellectuelle, le blanchiment d'argent, le trafic de drogues, la traite de personnes, les activités du crime organisé, l'exploitation sexuelle des enfants ou la cyberintimidation.

Ces catégories tiennent compte de l'exploitation répandue des nouvelles technologies à des fins criminelles. Elles permettent à la GRC de réprimer la criminalité organisée et les crimes graves commis par des délinquants qui se servent de la technologie pour élargir la portée de leurs activités traditionnelles et de repérer de nouvelles activités criminelles qui voient le jour en même temps que les progrès technologiques. Ces catégories sont distinctes des utilisations « accessoires » de la technologie pour commettre des crimes, c'est-à-dire les cas où Internet et les technologies connexes jouent un rôle secondaire et ne modifient pas l'activité criminelle de façon appréciable (p. ex. l'utilisation de la messagerie texte pour vendre de la drogue ou des recherches effectuées dans des sources ouvertes sur Internet pour planifier un vol).

Les infractions où la technologie est la cible et les infractions où la technologie

Figure 1 : catégories de cybercrimes

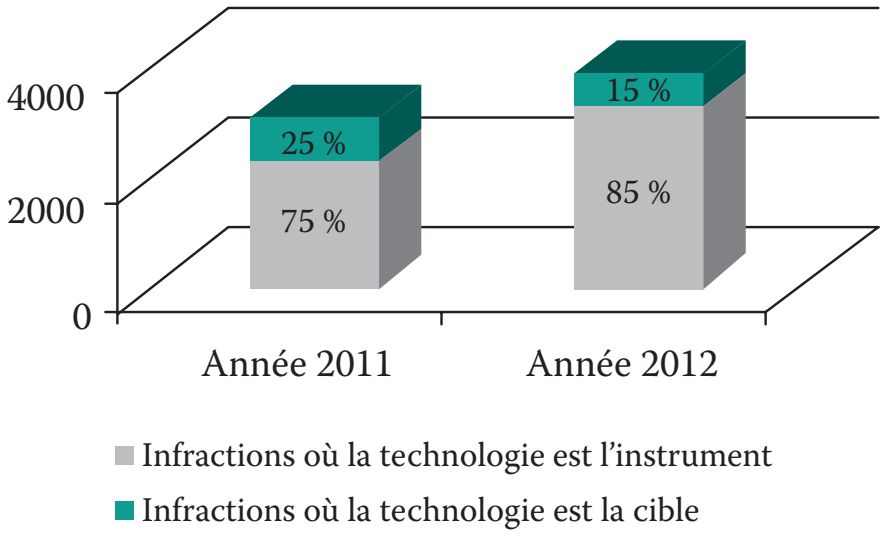


est l'instrument ne sont pas mutuellement exclusives. Dans de nombreux cas, les formes de cybercriminalité les plus avancées sur le plan technique (le piratage d'un ordinateur pour voler des données personnelles ou l'utilisation à distance d'un enregistreur de touches pour obtenir de l'information financière) peuvent servir à élargir la portée d'infractions criminelles plus traditionnelles (l'utilisation des mêmes renseignements personnels ou financiers pour faciliter la fraude par marketing de masse ou l'extorsion). Ces définitions sont élaborées plus bas au moyen d'exemples récents de mesures d'enquête et de répression.

Intensification de la cybercriminalité

Les incidents de cybercriminalité sont difficiles à évaluer et ils ne sont pas souvent signalés aux organismes d'application de la loi. Cependant, selon les statistiques de la GRC, la cybercriminalité continue de croître au Canada. En 2012, près de 4000 incidents de cybercriminalité ont été signalés à la GRC, une augmentation de plus de 800 cas par rapport à 2011. Au cours de ces deux années, ce sont les infractions où la technologie est l'instrument qui ont constitué la majorité

Tableau 1 : nombre d'incidents liés à la cybercriminalité signalés à la GRC en 2011 et en 2012



CENTRE ANTIFRAUDE DU CANADA

Le Centre antifraude du Canada (CAFC) constitue la référence canadienne pour le signalement et l'atténuation des fraudes en ligne par marketing de masse. Il s'agit d'un partenariat entre la GRC, la Police provinciale de l'Ontario (OPP) et le Bureau de la concurrence du Canada : **www.antifraudcentre-centreantifraude.ca**.

CENTRE NATIONAL DE COORDINATION CONTRE L'EXPLOITATION DES ENFANTS

Le Centre national de coordination contre l'exploitation des enfants (CNCEE) de la GRC collabore avec des partenaires de l'application de la loi de partout au Canada et à l'étranger pour lutter contre la cyberexploitation sexuelle des enfants. Le CNCEE collabore aussi étroitement avec le Centre canadien de protection de l'enfance, un organisme caritatif qui exploite la ligne nationale de signalement des cas d'exploitation sexuelle d'enfants sur Internet : **www.cyberaide.ca**.

des incidents signalés.

Ces statistiques ne donnent qu'une partie de l'information. D'autres études et rapports révèlent des augmentations dans certains aspects de la cybercriminalité au Canada. Par exemple, en 2013, le Centre antifraude du Canada (CAFC) a reçu plus de 16 000 plaintes de fraude informatique (escroqueries par courriel ou sur des sites Web), ce qui représente des pertes de plus de 29 millions de dollars. La cybercriminalité n'a cependant pas à être motivée par l'appât du gain pour avoir des conséquences dévastatrices sur les victimes. La cyberexploitation sexuelle d'enfants en est un parfait exemple. Pour la seule année 2013, le Centre national de coordination contre l'exploitation des enfants (CNCEE) de la GRC a reçu plus de 9000 signalements d'incidents et des demandes d'aide de la part d'organismes d'application de la loi et d'autres partenaires concernant la cyberexploitation sexuelle d'enfants.

MENACES POSÉES PAR LA CYBERCRIMINALITÉ ET ÉTUDES DE CAS

Les exemples et les études de cas qui suivent montrent les diverses infractions visées par la définition de cybercriminalité de la GRC et de quelles façons les gouvernements, les entreprises et les citoyens peuvent être victimes de cybercriminalité.

Infractions où la technologie est la cible

Les infractions où la technologie est la cible sont considérées comme des formes pures de cybercriminalité étant donné qu'elles n'existaient pas avant l'avènement d'Internet et des technologies connexes. Il s'agit d'infractions prévues dans le *Code criminel* et qui concernent l'utilisation non autorisée d'ordinateurs ainsi que les méfaits concernant des données. Ceux qui commettent ce type d'infractions cherchent à exploiter les vulnérabilités des logiciels ou d'autres technologies de l'information à des fins criminelles. Les criminels trouvent des moyens de compromettre ces technologies et d'obtenir, de modifier ou de détruire des renseignements personnels ou de nature délicate ou encore d'infiltrer des ordinateurs, des réseaux ou des appareils mobiles pour s'adonner à diverses activités illégales.

Refus de service distribué (DDoS)

Les attaques de refus de service distribué (DDoS) inondent les serveurs ou les sites Web ciblés de fausses demandes jusqu'à ce qu'un service en ligne soit perturbé et rendu inutilisable, privant ainsi des usagers d'utiliser le service ciblé. Les répercussions d'une attaque DDoS vont des désagréments temporaires à des effets plus perceptibles, notamment des occasions d'affaires manquées et des atteintes à la réputation découlant de l'interruption de service. Ces attaques peuvent être motivées par la politique, l'idéologie ou l'appât du gain ou être simplement utilisées pour faire obstacle à un organisme public ou privé ou perturber ses activités. Ces activités criminelles peuvent aussi être liées à des menaces internes

Menace électronique interne

Une menace interne est une menace malveillante et souvent criminelle contre un organisme public ou privé qui émane d'une personne œuvrant à l'intérieur de l'organisme, comme un

CAS 1 : ATTAQUE DDOS CONTRE UN SITE WEB DU GOUVERNEMENT

En 2012, la GRC a enquêté sur une attaque DDoS provenant de bureaux appartenant à la Chambre des communes contre le portail www.gouv.qc.ca du gouvernement du Québec, rendant le site Web inaccessible pendant plus de deux jours. Lors de l'enquête criminelle, la GRC s'est servie de noms de connexion, de dossiers sur l'accès aux immeubles, d'images de surveillance et de preuves numériques (matériel informatique saisi) pour identifier le suspect, un administrateur de réseau avec le gouvernement qui a obtenu des privilèges d'administrateur pour accéder au site www.gouv.qc.ca et qui en a profité pour y téléverser des maliciels. En 2013, le suspect a été reconnu coupable de deux accusations d'utilisation non autorisée d'ordinateurs et d'une accusation de méfait et il a été écopé d'une peine de détention à domicile.

employé ou un entrepreneur, qui tente d'en perturber les activités. Bien qu'elles ne touchent pas seulement la cybercriminalité, les menaces internes associées à l'utilisation non autorisée d'ordinateurs ou les méfaits concernant des données constituent un risque croissant pour les organisations qui dépendent d'Internet, de réseaux et de technologies connexes. Pour les personnes de l'intérieur, ces menaces constituent une autre façon de voler l'organisme ou de commettre un abus de confiance criminel. Les menaces électroniques internes sont une grande source de préoccupation pour les organismes d'infrastructures essentielles (comme ceux du gouvernement et des secteurs, du transport, de la finance, de la fabrication ou de l'énergie) et d'autres organismes qui utilisent des systèmes de technologie de l'information. Grâce à un accès interne et direct, les criminels peuvent contourner l'isolement du système (air gap) – mesure de sécurité consistant à isoler physiquement des réseaux pour les sécuriser – et compromettre directement un réseau informatique sécurisé, par exemple en installant un virus sur un réseau au moyen d'une clé USB.

La situation dans le *cas 1* constitue une attaque DDoS et une menace interne contre les réseaux informatiques du gouvernement et les systèmes de technologie de l'information connexes.

Réseaux de zombies

Un « réseau de zombies » est un réseau d'ordinateurs contrôlé à distance par un serveur de commande. Les réseaux de zombies peuvent servir à lancer des maliciels et à infecter des milliers voire des millions d'ordinateurs à diverses fins criminelles, comme la distribution d'un programme malveillant pour accéder à des données, à des saisies d'écran ou de mot de passe, ou encore à un enregistreur de touches pour obtenir de l'information personnelle ou financière.

Dans de nombreux cas, les victimes ne savent pas que les ordinateurs de leur entreprise ou leurs ordinateurs personnels font partie d'un réseau de zombie et que leurs données peuvent être subtilisées à des fins criminelles. Sans le savoir, une personne peut activer un maliciel sur un ordinateur en cliquant sur

un courriel ou un lien qui semble inoffensif, donnant ainsi une forme de contrôle codé à un réseau de zombies (le maliciel peut enregistrer les frappes et ainsi donner accès aux mots de passe d'un compte bancaire en ligne). Ces menaces ne mettent pas seulement en jeu des infractions « pures » relatives à la cybercriminalité, mais elles servent aussi à faciliter des crimes plus traditionnels, comme la fraude et le vol d'identité. L'Opération Clean Slate (*cas 2*) est un exemple d'une initiative récente d'application de la loi contre un réseau criminel international de zombies.

CAS 2 : OPÉRATION CLEAN SLATE

En 2013, le Federal Bureau of Investigation (FBI) des États-Unis a informé la GRC que des adresses IP canadiennes étaient soupçonnées d'être derrière des opérations de commande et de contrôle d'un réseau d'ordinateurs infectés (« réseau de zombies »). Connu sous le nom de Citadel, ce réseau de zombies a installé des logiciels malveillants dans des ordinateurs pour voler des données personnelles et financières et il a ciblé des institutions financières d'envergure au Canada et à l'étranger, entraînant des pertes économiques globales estimées à 500 millions de dollars. Ce type particulier de logiciel malveillant a permis à des criminels d'accéder à distance à des ordinateurs personnels et d'entreprises pour voler des données bancaires en ligne, des renseignements relatifs à des cartes de crédit et d'autres justificatifs d'identité. En conséquence, la GRC a saisi plus de 80 serveurs physiques pour ralentir la propagation de ce réseau de zombies. Le FBI et ses partenaires gouvernementaux et d'application de la loi à l'étranger ont collaboré étroitement avec l'industrie de la technologie de l'information et des institutions financières pour perturber les activités de plus de 1400 réseaux informatiques infectés par le logiciel malveillant Citadel, nettoyant ainsi plus de deux millions d'ordinateurs infectés à l'échelle de la planète.

Infractions où la technologie est l'instrument

La cybercriminalité pure met souvent en jeu le vol et l'échange de renseignements personnels ou financiers, ce qui s'applique aux *infractions où la technologie est l'instrument*. D'autres crimes impliquent l'utilisation d'Internet et des technologies de l'information de différentes façons et ils prennent une nouvelle dimension dans le cyberespace. Les exemples et les études de cas ci-dessous illustrent l'éventail des *infractions où la technologie est l'instrument*.

Fraude aux cartes bancaires

La fraude aux cartes bancaires est une infraction où on se sert d'Internet pour trafiquer et exploiter des données personnelles et financières et pour échanger des techniques liées à la cybercriminalité, comme l'achat et la vente en ligne de documents d'identité volés, de documents contrefaits, de renseignements sur des cartes de crédit et des comptes bancaires et d'outils de piratage. La fraude aux cartes bancaires et d'autres types de crimes semblables montrent à quel point la cybercriminalité

CAS 3 : OPÉRATION CARD SHOP

En 2010, la GRC a aidé le FBI et d'autres partenaires d'application de la loi étrangers à enquêter sur des infractions liées à la fraude aux cartes bancaires (p. ex. l'achat et la vente de données personnelles et financières) et à détecter les individus impliqués dans ce type de cybecriminalité. L'opération d'une durée de deux ans a débouché sur l'arrestation de suspects par des organismes internationaux d'application de la loi et elle a mis au jour des activités criminelles présumées au Canada. La GRC a apporté son aide en menant des opérations coordonnées en Colombie-Britannique, en Alberta et en Ontario, ce qui a permis l'arrestation d'un individu qui a renoncé à l'extradition aux États-Unis.

L'opération s'est étendue à huit pays, elle a donné lieu à 24 arrestations suivies d'autant de condamnations et elle a permis d'éviter des pertes économiques estimées à 205 millions de dollars parce que les fournisseurs de cartes de crédit ont pu être informés d'une fraude touchant plus de 400 000 cartes de crédit et de débit et que plus de 40 organismes des secteurs public et privé ont été mis au courant d'intrusions dans leurs réseaux.

pure peut jouer un rôle clé dans la facilitation de crimes plus traditionnels et dans la modification de leur portée. Par exemple, un criminel peut obtenir un accès non autorisé à une base de données informatique pour voler des renseignements permettant d'identifier une personne et des numéros de carte de crédit. Après coup, le criminel peut se rendre sur des forums anonymes en ligne, dont un grand nombre ne sont pas détectés par les moteurs de recherche, pour échanger cette information à des fins criminelles.

L'Opération Card Shop (*cas 3*) donne un aperçu d'une opération policière internationale contre la fraude aux cartes bancaires.

Fraude en ligne par marketing de masse et rançongiciel

Les liens entre la cybercriminalité pure et accessoire sont probablement les plus courants dans les cas de fraude. Internet a transformé cette infraction criminelle bien établie au point où le marketing de masse est maintenant lié à de nombreux types de fraude. La fraude par marketing de masse exploitant Internet, comme les courriels d'hameçonnage, les loteries frauduleuses, les fraudes 419 et les stratagèmes de rencontre, servent à tromper les victimes et à voler des identificateurs personnels à diverses fins criminelles motivées par l'appât du gain. Ces arnaques ciblent facilement de grandes populations dans divers pays, et ce, d'une manière beaucoup plus généralisée, anonyme et efficace que des crimes similaires commis hors ligne. Un de ces cybercrimes axé sur la fraude est illustré par les « rançongiciels ».

Les fraudes par rançongiciel impliquent un type de maliciel qui verrouille un ordinateur et les données qu'il contient et qui utilise des méthodes d'ingénierie sociale, comme des menaces,

CAS 4 : FRAUDES PAR RANÇONGICIEL

En 2012, le Centre antifraude du Canada (CAFC) a recueilli des plaintes de Canadiens qui recevaient des messages instantanés sur leur ordinateur mentionnant que leur système d'exploitation était verrouillé en raison d'une violation des lois du Canada, y compris de fausses accusations d'échange de fichiers contenant de la pornographie juvénile et d'envoi de pourriels aux motifs terroristes.

Les messages illégitimes étaient rédigés de façon à avoir l'air de messages de la GRC ou du Service canadien du renseignement de sécurité (SCRS) demandant aux personnes de payer 100 $ en argent électronique pour déverrouiller leur ordinateur. En 2012, la GRC et le CAFC ont reçu des centaines de signalement de Canadiens ayant reçu le message type du rançongiciel, qui était lié à un maliciel téléchargé sur des sites Web infectés ou à partir de courriels frauduleux. La GRC s'est servie de son site Web pour informer le public de la présence de ce maliciel et pour inciter les consommateurs canadiens à signaler toute possibilité d'incident au CAFC. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) de Sécurité publique Canada a aussi publié un bulletin de cybersécurité comprenant des procédures de récupération en cas d'infection par ce maliciel.

Ces menaces continuent d'avoir une incidence sur les Canadiens. En 2013, le CAFC a reçu 2 800 rapports de personnes qui sont tombées sur la plus récente variante d'un rançongiciel - Cryptolocker. En tout, certaines victimes ont versé plus de 15 000 $ pour tenter de recouvrer l'accès à leur ordinateur. Cryptolocker est un fichier exécutable qui prend la forme d'un fichier PDF et qui s'active lorsqu'une victime clique naïvement dessus. Le virus chiffre les fichiers et les dossiers de l'ordinateur et la victime peut seulement les déchiffrer et y accéder de nouveau après avoir effectué un paiement en ligne au fraudeur responsable (clé de déchiffrement). La GRC, le CAFC et les partenaires gouvernementaux continuent d'atténuer les menaces présentées par les rançongiciels en adoptant des tactiques de prévention et d'autres mesures de cybersécurité.

pour contraindre les victimes à débourser de l'argent pour recouvrer l'accès à leur ordinateur. Vous trouverez dans *cas 4* la description de récentes menaces impliquant des fraudes par rançongiciel.

Crime organisé et Internet

Internet et les technologies connexes ont créé de nouvelles possibilités, de nouveaux marchés et de nouvelles méthodes de livraison pour les transactions criminelles qui ne sont pas disponibles

dans le monde « réel ». En ce qui concerne les drogues, les produits de contrebande et d'autres types de trafic criminel, ces technologies ont créé une vitrine virtuelle où des groupes criminels peuvent efficacement, et dans l'anonymat,p acheter, vendre et échanger des produits et des services criminels à un niveau sans précédent.

Dans certains cas, ces types de cybercrimes sont aussi associés au blanchiment d'argent et aux activités du crime organisé. Grâce à des stratagèmes en ligne, les transferts criminels d'argent en provenance du Canada peuvent être acheminés électroniquement par l'intermédiaire de pays étrangers où les mesures de sécurité sont plus faibles afin de dissimuler plus efficacement les produits de la criminalité et de simplifier les opérations bancaires extraterritoriales. Les blanchisseurs d'argent peuvent aussi être de connivence et exploiter des services en ligne légitimes, comme des sites d'enchères ou de jeux en ligne, pour cacher les produits de la criminalité en achetant et en vendant des articles fictifs ou en faisant passer ces produits pour des profits générés par le jeu. Le *cas 5* illustre la menace croissante du blanchiment d'argent en ligne et ses liens avec le crime organisé.

CAS 5 : CRIME ORGANISÉ, BLANCHIMENT D'ARGENT ET INTERNET

En 2012, la GRC et des partenaires de l'Unité mixte d'enquête sur le crime organisé ont découvert un groupe du crime organisé soupçonné d'utiliser un site de jeux en ligne extraterritorial, Platinum Sports Book.com, pour blanchir les produits de la criminalité générés au Canada et faire des profits au moyen de paris illégaux. Après une opération d'une durée d'un an, la GRC a établi des liens entre des activités en provenance du Canada et le site de jeux en ligne. Le site Web accueillait des milliers de joueurs dont les mises auraient mené à des millions de dollars en profit pour le crime organisé.

L'opération a permis la fermeture et le démantèlement de l'entreprise de jeux en 2013. Plus de 30 personnes ont été arrêtées et accusées de nombreuses infractions liées au jeu (p. ex. participation ou contribution aux activités d'une organisation criminelle, tenue d'une maison de pari et conspiration) et on a saisi plus de trois millions de dollars.

Cyberexploitation sexuelle d'enfants

Internet a transformé et exacerbé les activités criminelles impliquant la cyberexploitation sexuelle d'enfants. Dans le cyberespace, les criminels cachent leur véritable identité au moyen de pseudonymes et ils échangent du matériel de pornographie juvénile par l'intermédiaire de sites Web privés et de babillards électroniques. L'Opération Snapshot (*cas 6*) donne une idée de la nature préjudiciable et omniprésente de la cyberexploitation sexuelle d'enfants et du rôle des organismes d'application de la loi.

CAS 6 : OPÉRATION SNAPSHOT

En 2012, la GRC a pris part à l'Opération Snapshot, une enquête multi-organismes axée sur l'identification de délinquants à risque élevé qui étaient en possession d'images de cyberexploitation d'enfants ou qui distribuaient ces images au moyen de réseaux de partage de fichiers poste à poste (P2P). Cette enquête exigeante a permis la saisie de plus de 100 ordinateurs et disques durs, qui ont été soumis à une analyse judiciaire, et de centaines de milliers d'images de cyberexploitation sexuelle d'enfants. L'enquête s'est soldée par le sauvetage d'un enfant et l'arrestation de plus de 15 individus en rapport avec des infractions à caractère sexuel (p. ex. l'accès à de la pornographie juvénile, la possession de pornographie juvénile, la distribution de pornographie juvénile, la production de pornographie juvénile et le leurre sur Internet).

L'opération multi-organismes s'est poursuivie en 2013 avec l'Opération Snapshot II, lors de laquelle les enquêteurs avaient deux priorités clés : identifier et délivrer des enfants victimes d'exploitation sexuelle, et repérer les délinquants à risque qui recueillent, possèdent ou diffusent du matériel de pornographie juvénile en ligne, et porter des accusations contre ces personnes. Ces enquêtes ont permis le sauvetage de deux enfants et l'arrestation de 22 individus dans les dans les provinces atlantiques qui étaient soupçonnées de recueillir, de posséder et de diffuser du matériel de pornographie juvénile en ligne.

ÉVOLUTION DES MENACES LIÉES À LA CYBERCRIMINALITÉ

Les menaces liées à la cybercriminalité deviennent de plus en plus sophistiquées étant donné que les criminels continuent d'exploiter les technologies de l'information, ce qui nuit passablement aux services de police pour détecter ces menaces et établir des liens. Voici quelques-uns des cybercrimes en évolution qui pourraient servir de fondement aux prochains rapports de la GRC.

Darknets
Les darknets sont des réseaux d'échange de fichiers en ligne qui assurent l'anonymat aux utilisateurs au moyen de technologies de chiffrement et de cybersécurité. Ils permettent aux criminels de négocier leurs produits et leurs services illégaux sur Internet et d'éviter d'être repérés sur des réseaux anonymes. Ces réseaux sont attrayants pour ceux qui se livrent à des activités criminelles parce qu'ils dissimulent les transactions en ligne, comme l'achat et la vente en ligne de drogues illégales, de fichiers piratés, de biens contrefaits et d'autres produits illicites.

Modèle CaaS (cybercrime-as-a-service)
Par l'intermédiaire de darknets et d'autres forums en ligne, les criminels

peuvent acheter ou louer des outils et des services de cybercriminalité ou une infrastructure connexe avec assez de facilité. Ce marché en ligne axé sur les services permet à un plus grand nombre de criminels de prendre part à des cybercrimes sophistiqués sur le plan technique, comme des opérations criminelles impliquant des attaques DDoS ou la distribution de maliciels au moyen de réseaux de zombies. La disponibilité en ligne de ces outils et services fait en sorte qu'un plus grand nombre de criminels peuvent sous-traiter leurs opérations de cybercriminalité, en tout ou en partie.

Ciblage des plates-formes mobiles par des maliciels

La popularité et l'interconnectivité des appareils mobiles, comme les téléphones intelligents et les tablettes, en font des cibles attrayantes pour les criminels. Des variantes de maliciels sont de plus en plus développées pour cibler les vulnérabilités des systèmes d'exploitation d'appareils mobiles. Les caractéristiques des appareils mobiles, comme la messagerie texte et les applications téléchargeables, sont utilisées pour déployer des maliciels et obtenir un accès à distance non autorisé aux plates-formes mobiles, et ce, à des fins illicites, p. ex. pour voler des données personnelles et obtenir des coordonnées GPS.

Fraudes liées à une devise virtuelle

Les fraudes liées à une devise virtuelle comme le Bitcoin sont commises par des criminels pour blanchir leurs profits en ligne (blanchiment d'argent). Ces stratagèmes fournissent à des réseaux criminels organisés de nouveaux moyens de dérober leurs gains aux regards des organismes d'application de la loi. L'utilisation de devises virtuelles à des fins criminelles est souvent associée aux darknets, ces endroits où des devises virtuelles et des réseaux anonymes en ligne sont utilisés pour obtenir des paiements en échange de biens et de services illégaux et pour blanchir les revenus associés à des transactions criminelles.

Manipulation du marché boursier facilitée par Internet

La cybercriminalité s'applique aux manipulations frauduleuses du marché boursier en ligne. Les criminels utilisent des techniques d'ingénierie sociale pour obtenir des justificatifs d'identité personnelle ou pour déployer des programmes malveillants comme des enregistreurs de touches, et ce, afin de pirater des comptes d'utilisateurs qui effectuent des transactions et de manipuler le cours du titre des valeurs ciblées. D'autres types de cybercrimes, comme les attaques DDoS, ont également des répercussions sur les marchés financiers parce qu'elles ébranlent la confiance envers les services en ligne et qu'elles modifient l'estimation des valeurs mobilières.

Menaces cybercriminelles contre les systèmes de contrôle industriels

Les systèmes de contrôle industriels, comme les systèmes d'acquisition et de contrôle des données (SCADA) sont utilisés pour la surveillance et les processus de contrôle industriels, comme ceux qu'on trouve dans les centrales ou les réseaux électriques. Ces systèmes peuvent comprendre des composants reliés à Internet, les rendant ainsi vulnérables à des attaques DDoS ou à d'autres types de cybercrimes impliquant des programmes malveillants. L'incidence de ces menaces aux infrastructures essentielles peut être variée : espionnage industriel; extraction de données; vol de propriété intellectuelle ou de secrets industriels, ou tactiques plus perturbatrices impliquant la compromission de systèmes.

Conclusion : principales observations

Le présent rapport donne un aperçu des menaces et des tendances en matière de cybercriminalité qui portent préjudice aux organismes publics, aux intérêts commerciaux et aux citoyens du Canada de façon réelle et concrète. Bien qu'incomplet, il met en lumière des enjeux liés à la cybercriminalité pour démontrer la gamme des infractions au *Code criminel* qui constituent des cas de cybercriminalité. Il se conclut par trois observations générales.

La technologie crée de nouvelles possibilités pour les criminels
Internet et les technologies connexes n'ont pas seulement transformé la société et l'économie canadiennes; ils ont aussi modifié le monde criminel du Canada. Les marchés électroniques et les dispositifs reliés à Internet offrent les mêmes possibilités aux réseaux criminels organisés qu'aux entreprises légitimes. Grâce aux technologies de l'information, les criminels étendent leurs activités pour commettre des crimes tout à fait nouveaux et commettre sous une nouvelle forme des crimes qui existaient déjà.

La cybercriminalité prend de l'ampleur
Autrefois considérée comme le domaine des criminels possédant des compétences spécialisées, la cybercriminalité est maintenant à la portée d'autres délinquants puisque le savoir requis est maintenant plus accessible. Des programmes malveillants facilement accessibles et prêts à utiliser – on peut les acheter, les vendre ou les échanger en ligne – offrent aux criminels de nouveaux moyens simplifiés de voler des renseignements personnels et de faire perdre de l'argent à des entreprises et à des citoyens du Canada. Certains individus ont aussi recours à la cybertechnologie pour se livrer à d'autres activités qui causent des préjudices, comme la cyberexploitation sexuelle des enfants et la cyberintimidation (en croissance constante).

La cybercriminalité oblige la police à adopter de nouvelles méthodes
L'exploitation criminelle des nouvelles technologies – comme l'informatique en nuage, les médias sociaux, les réseaux anonymes en ligne et les fraudes liées à une devise virtuelle – exige de nouvelles mesures policières pour ne pas se laisser distancer à l'ère numérique. Les activités criminelles qui se déroulent dans le cyberespace sont complexes et souvent internationales de nature – les éléments de preuve potentiels sont éphémères et ils se trouvent dans de nombreux pays. Afin de surmonter ces difficultés, il est nécessaire de pouvoir compter sur la collaboration des organismes d'application de la loi nationaux et internationaux, la mobilisation des organismes des secteurs public et privé et l'intégration de nouvelles compétences et de nouveaux outils techniques aux services de police traditionnels.

La GRC a un mandat étendu en ce qui a trait aux enquêtes et à l'arrestation de criminels dans le cyberespace; elle peut faire tout en son pouvoir pour contrer la cybercriminalité. Dans le but d'améliorer ses capacités dans le cyberespace, la GRC élabore une stratégie pour lutter contre la cybercriminalité en collaboration avec ses partenaires nationaux et internationaux. La stratégie devrait être prête en 2014 et elle complétera la Stratégie nationale de cybersécurité afin de contribuer à la sécurité des Canadiens en ligne.