GRC
GENDARMERIE ROYALE DU CANADA

Stratégie de lutte contre la cybercriminalité de la gendarmerie royale du Canada

Gendarmerie royale du Canada
Royal Canadian Mounted Police

Canada

CAT. NO.: PS64-128/2015F-PDF
ISBN: 978-0-660-03031-9

Sommaire

En 2010, le gouvernement du Canada a lancé la Stratégie de cybersécurité du Canada afin de protéger contre les cybermenaces les gouvernements et administrations, les entreprises, les infrastructures essentielles et les résidents du Canada. La stratégie a aidé le Canada à enrichir ses connaissances de la cybertechnologie et à orienter ses efforts visant à assurer la sécurité du gouvernement et d'autres systèmes névralgiques, de même qu'à protéger les Canadiens qui utilisent Internet.

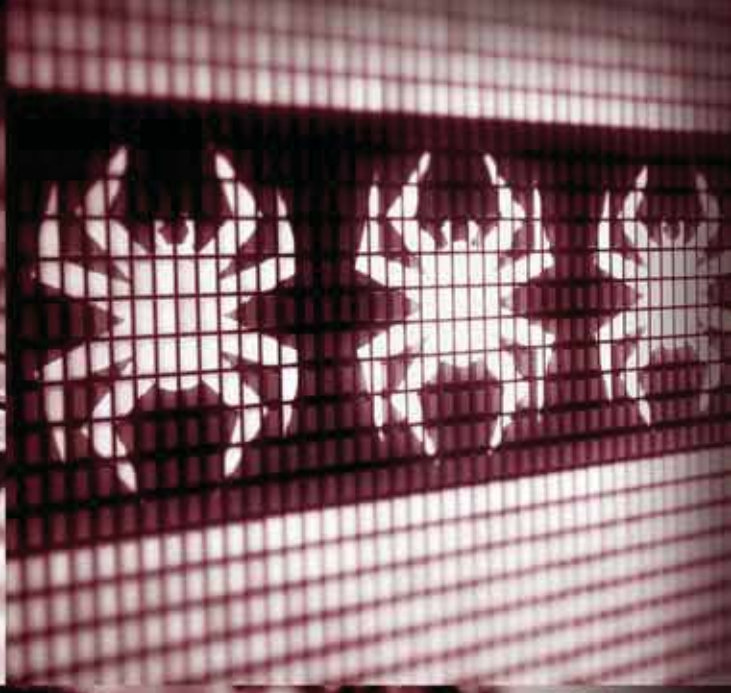
Conformément au travail réalisé par le gouvernement afin de rendre le cyberespace plus sécuritaire pour tous les Canadiens, la Stratégie de lutte contre la cybercriminalité de la GRC, fondée sur de longues consultations internes et externes, vise à trouver des façons d'améliorer les mesures prises par le service de police national du Canada afin de contrer l'augmentation et l'évolution de la menace que pose la cybercriminalité. Cette stratégie vient compléter la Stratégie de cybersécurité du Canada et s'inscrit dans les efforts visant à protéger les Canadiens lorsqu'ils utilisent Internet.

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 combattre la cybercriminalité. La Stratégie de lutte contre la cybercriminalité de la GRC a donc une grande portée et met en évidence le rôle de la cybernétique dans plusieurs secteurs de l'application de la loi. La stratégie a pour objectif de réduire la menace, les répercussions et la victimisation associées à la cybercriminalité au Canada grâce à des mesures policières. Elle comporte les trois piliers suivants, qui orientent le travail de la GRC afin d'endiguer ce type de crimes :

- Définir les menaces de cybercriminalité et en établir l'ordre de priorité au moyen de la collecte et de l'analyse de renseignements
- Cibler les cybercriminels grâce à des mesures de répression et d'enquête adaptées
- Soutenir les enquêtes sur la cybercriminalité grâce à des compétences, à de la formation et à des outils spécialisés.

La Stratégie de lutte contre la cybercriminalité de la GRC, dans un cadre opérationnel et un plan d'action, présente des objectifs, des catalyseurs stratégiques et 15 mesures de suivi que la GRC prendra au cours des cinq prochaines années et au-delà. Ensemble, ces initiatives permettront au service de police national du Canada de mieux lutter contre la cybercriminalité en collaboration avec ses partenaires de l'application de la loi au pays et à l'étranger et autres parties prenantes.


0,0003 14,29%
-0,0005 -12,50%




Enter

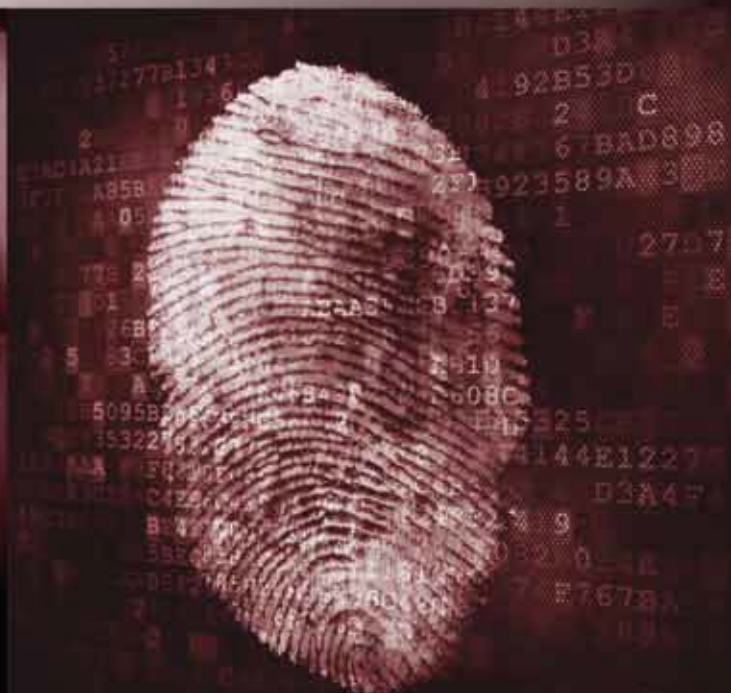


Table des matières

La cybercriminalité oblige la police à adopter de nouvelles méthodes

La cybercriminalité s'intensifie, tant au Canada qu'ailleurs dans le monde.

Autrefois considérée comme l'apanage d'initiés aux compétences spécialisées, la cybercriminalité est maintenant à la portée de bien d'autres individus puisque le savoir requis est aujourd'hui plus accessible. Des programmes malveillants facilement accessibles et prêts à utiliser et les services de cybercriminalité en ligne pour le compte d'autrui offrent aux criminels de nouveaux moyens simplifiés de voler des renseignements délicats et personnels. Ainsi, ils cherchent constamment de nouvelles failles dans les technologies qu'ils pourront exploiter à des fins illicites ainsi que de nouvelles façons de s'attaquer aux organisations publiques et privées et aux Canadiens qui se servent de ces technologies.

La portée et les répercussions des cybermenaces sont variées. Les cybercrimes peuvent cibler des personnes par le biais d'escroqueries en ligne ou d'autres techniques frauduleuses. Ils peuvent entraîner d'autres coûts sociaux et mener à d'autres crimes aux conséquences dévastatrices comme la cyberexploitation sexuelle des enfants et la cyberintimidation, qui est en croissance constante. Les réseaux du crime organisé posent également une menace sur le Web qui se solde par d'importantes pertes économiques pour les entreprises et les citoyens du Canada. Sur le plan commercial, les cybercriminels ciblent les institutions financières, les gros détaillants et d'autres organisations afin de voler des renseignements personnels de consommateurs (p. ex. des mots de passe de sites Web et des numéros de carte de crédit), de l'information confidentielle sur la propriété intellectuelle ou des secrets industriels. Au chapitre de la sécurité nationale, des individus parrainés par un État et d'autres criminels se servent de méthodes complexes et clandestines pour faire de l'espionnage, subtiliser des renseignements délicats ou mener des attaques contre des infrastructures essentielles et d'autres cybersystèmes essentiels du Canada.

L'exploitation criminelle des nouvelles technologies exige la prise de nouvelles mesures policières pour éviter que les organismes d'application de la loi se laissent distancer à l'ère numérique. Les mêmes technologies utilisées par des personnes et des organismes à des fins légitimes peuvent être exploitées par des criminels pour dissimuler leurs activités en ligne et éviter d'être détectés par les autorités. Souvent, la police doit trouver des solutions techniques pour déchiffrer, déverrouiller ou contourner des technologies de chiffrement, des adresses protocole Internet (IP) redirigées et d'autres obstacles techniques qu'exploitent des criminels pour brouiller les pistes et commettre des méfaits sur le Web. De plus, les activités criminelles menées dans le cyberespace sont complexes et souvent de nature internationale; les éléments de preuve potentiels sont éphémères et ils se trouvent dans de nombreux pays.

La cybercriminalité se répercute de façon réelle et préjudiciable sur les Canadiens, et ce, à divers degrés. Au chapitre de l'application de la loi, il est nécessaire de pouvoir compter sur la collaboration des forces de l'ordre nationales et internationales, la mobilisation des organismes des secteurs public et privé et de nouveaux outils techniques jumelés à des mesures policières habituelles. En tant que service de police national du Canada, la GRC doit s'efforcer de jouer un rôle de leader dans la lutte contre la cybercriminalité. La stratégie et le plan d'action exposés dans le présent document témoignent de l'engagement résolu de la GRC à cet égard.

Définition de la cybercriminalité

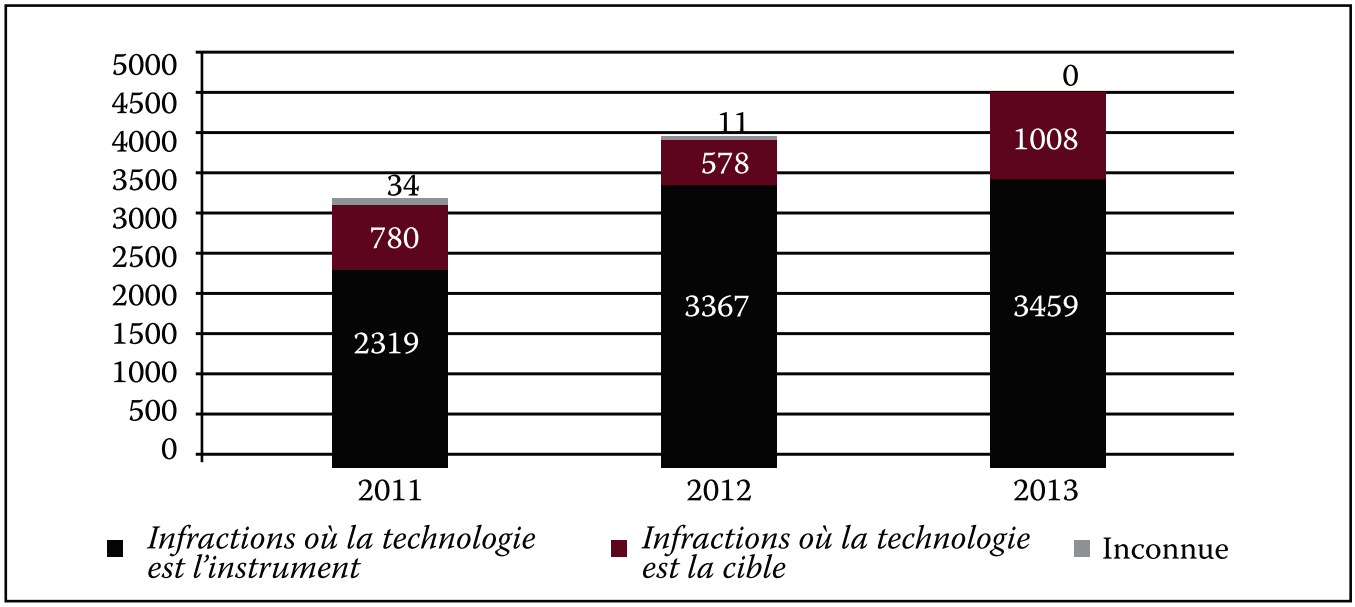
Selon la GRC, un cybercrime s'entend de n'importe quel type de crime commis en grande partie à l'aide d'Internet et des technologies de l'information comme des ordinateurs, des tablett=es, des assistants numériques personnels ou des appareils mobiles. La GRC divise les actes de cybercriminalité en deux catégories :

- *infractions où la technologie est la cible* – actes criminels qui ciblent des ordinateurs et d'autres technologies de l'information, notamment 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, notamment la fraude, le vol d'identité, la violation de propriété intellectuelle, le blanchiment d'argent, le trafic de drogue, la traite de personnes, les activités du crime organisé ou de terroristes, l'exploitation sexuelle des enfants et la cyberintimidation.

Fréquence des cybercrimes

Selon des statistiques compilées par la GRC, la cybercriminalité est en croissance au Canada. En 2013, la GRC a reçu plus de 4 400 signalements d'incidents liés à la cybercriminalité, ce qui représente une hausse de plus de 40 % (plus de 1 300 incidents signalés) par rapport à 2011. Dans un petit nombre de signalements d'incidents liés à la cybercriminalité, la nature de l'infraction n'a pu être identifiée soit comme une *infraction où la technologie est l'instrument* ou une *infraction où la technologie est la cible* (c'est-à-dire, inconnue.)

Tableau 1 : Nombre d'incidents liés à la cybercriminalité signalés à la GRC de 2011 à 2013



Autres renseignements sur la cybercriminalité

Plus d'information sur la cybercriminalité, y compris des définitions approfondies et des études de cas, figure dans le premier rapport public de la GRC sur la cybercriminalité intitulé *Cybercriminalité : survol des incidents et des enjeux au Canada* (en ligne à l'adresse http://www.rcmp-grc.gc.ca/pubs/cc-report-rapport-cc-fra.htm).

La stratégie de la GRC en matière de lutte contre la cybercriminalité

La GRC est la seule organisation fédérale ayant le mandat et le pouvoir d'enquêter sur des infractions liées à la cybercriminalité comme celles ciblant les systèmes et les réseaux du gouvernement ou d'autres secteurs des infrastructures essentielles. Les renseignements criminels permettent aux agences d'application de la loi de faire le lien entre les informations d'activités criminelles locales et nationales et internationales. En tant que service de police national du Canada, la GRC est chargée d'un vaste mandat en ce qui touche les enquêtes sur des individus ayant commis des crimes dans le cyberespace, ce qui mène à l'appréhension de criminels ou à la perturbation de leurs activités. Ce travail consiste entre autres à déceler les cybermenaces puis à les classer par ordre de priorité à partir de renseignements criminels, à mener des activités d'enquête et de perturbation de la cybercriminalité ainsi qu'à traiter les preuves numériques à l'appui des enquêtes en la matière.

Les rôles et les responsabilités de la GRC relativement à la cybercriminalité sont conformes au devoir de maintenir la paix et de prévenir le crime et d'autres infractions aux lois canadiennes comme il est énoncé dans la *Loi sur la Gendarmerie royale du Canada*. Dans les provinces, les territoires et les villes où la GRC est le service de police local engagé à contrat, cette dernière a aussi un mandat général d'application de la loi des services de police en matière de cybercriminalité étant donné que bon nombre de ces crimes sont perpétrés au moyen de technologies modernes.

De plus, la GRC joue un rôle déterminant dans la grande cybercommunauté du gouvernement. Dans le cadre de la Stratégie de cybersécurité du Canada, la GRC travaille de près avec ses partenaires gouvernementaux pour créer un cyberenvironnement sécuritaire au Canada.

La section qui suit traite des rôles et des responsabilités de la GRC relativement à la cybercriminalité qui se divisent en trois principaux domaines : les renseignements criminels, les enquêtes criminelles et les services spécialisés.

Renseignements criminels

La GRC a adopté une démarche policière axée sur les renseignements. Les renseignements criminels permettent aux agences d'application de la loi de faire le lien entre les informations d'activités criminelles locales et nationales et internationales. Qu'ils soient de nature tactique, opérationnelle ou stratégique, les renseignements criminels permettent à la GRC et à d'autres services de police canadiens d'établir leurs priorités et d'affecter leurs ressources en fonction des menaces criminelles les plus graves contre le Canada. Cette notion s'applique également à la cybercriminalité, plus particulièrement compte tenu de sa dimension transnationale et du besoin inhérent de dégager les tendances et de reconnaître les liens entre les données relatives à la cybercriminalité et d'autres sources de données pertinentes de multiples territoires de compétence.

La GRC peut enquêter sur la cybercriminalité à la suite d'une plainte ou de façon proactive après avoir eu accès à des renseignements criminels. Les renseignements sur la cybercriminalité tirés d'enquêtes, de bases de données policières, de recherches et d'analyses de sources ouvertes ou d'un travail de collaboration entre des organismes d'application de la loi et des intervenants des secteurs public et privé peuvent permettre le repérage de délinquants prolifiques et d'auteurs de crimes graves dans le cyberespace et peuvent amener, de façon objective, les policiers vers les principales cibles. La GRC analyse les renseignements criminels provenant d'un vaste éventail de sources, repère les nouvelles menaces de cybercriminalité et établit des liens entre la cybercriminalité et d'autres activités criminelles comme le crime organisé et la criminalité financière.

Centres d'intervention

Centre antifraude du Canada
Le Centre antifraude du Canada (CAFC) constitue la référence canadienne pour le signalement et la diminution 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. En 2014, le CAFC a reçu plus de 14 000 plaintes de fraude informatique (escroqueries par courriel ou sur des sites Web), ce qui représente des pertes de plus de 45 millions de dollars. On peut obtenir plus d'information au 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, des organismes gouvernementaux, des organisations non gouvernementales et des parties prenantes du secteur privé 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.cybertip.ca). En 2014, le CNCEE a reçu près de 8 500 signalements d'incidents et demandes d'intervention de la police et d'autres intervenants en la matière.

Enquêtes criminelles

Au fédéral, la GRC assure l'exécution des lois fédérales et mène des enquêtes sur des crimes graves et le crime organisé, des crimes économiques, ainsi que sur des menaces à la sécurité nationale. Ces enquêtes peuvent porter sur des infractions impliquant des activités de cybercriminalité soupçonnées comme le blanchiment d'argent et le financement des activités terroristes, les fraudes sur les marchés financiers, les menaces aux infrastructures essentielles du Canada, la violation de la propriété intellectuelle et le trafic de drogue. La GRC travaille avec des partenaires de l'application de la loi et d'autres parties prenantes au Canada et ailleurs dans le monde afin de lutter contre les menaces de cybercriminalité qui visent plusieurs territoires de compétence et nécessitent des opérations policières conjuguées.

La police internationale fait aussi partie intégrante de la stratégie d'intervention de la GRC en matière de cybercriminalité. La cybercriminalité est souvent transnationale, c'est-à-dire que l'auteur du crime dans un pays donné peut faire des victimes dans bien d'autres pays. Étant donné que les preuves d'activités criminelles peuvent facilement traverser les frontières dans le cyberespace, la GRC doit travailler avec des partenaires multilatéraux afin d'obtenir et d'analyser les éléments de preuve, ce qui est possible grâce à l'échange d'information entre les services de police et aux mécanismes juridiques officiels. La cybercriminalité ne connaissant aucune frontière, la GRC travaille en étroite collaboration avec ses partenaires de l'application de la loi au Canada et à l'étranger ainsi qu'avec d'autres parties prenantes des secteurs public et privé afin de contrer les menaces communes liées à la cybercriminalité au moyen de diverses mesures de répression qui mènent à des arrestations et à des accusations ou à d'autres perturbations.

Dans les provinces, les territoires et les municipalités où elle assure des services de police à contrat, la GRC joue également un rôle de premier plan dans la lutte contre la cybercriminalité. Les activités

policières dans ces provinces, territoires et municipalités ciblent un éventail de crimes dans lesquels Internet et des technologies connexes ont joué un rôle central, notamment la cyberexploitation sexuelle d'enfants, des fraudes locales et régionales et diverses infractions liées à la cyberintimidation.

Services spécialisés

Les services spécialisés et technologiques de la GRC jouent un rôle déterminant dans les enquêtes sur la cybercriminalité. La cybercriminalité implique souvent des activités clandestines en ligne, et on doit avoir recours aux compétences et aux outils policiers appropriés pour trouver la source d'une activité cybercriminelle, identifier les suspects potentiels et traiter les grandes quantités d'éléments de preuve numériques comme des téraoctets de données tirées d'ordinateurs, de disques durs et d'appareils mobiles saisis légalement. Les enquêtes sur la cybercriminalité diffèrent grandement des enquêtes criminelles habituelles en ce sens qu'elles doivent davantage être menées dans des environnements virtuels, comprennent l'analyse de sources ouvertes et l'utilisation de moyens secrets et supposent l'obtention et l'analyse de données – et d'éléments de preuve numériques potentiels – pour orienter les enquêtes. Ce travail revêt une importance cruciale pour les enquêtes criminelles qui comportent une dimension électronique et gagnera en complexité et en volume au fur et à mesure que les criminels continueront d'exploiter les nouvelles technologies.

Les Services d'enquêtes techniques (SET) de la GRC fait partie intégrante des services spécialisés dans les enquêtes sur la cybercriminalité de la GRC. Les SET offrent des conseils d'expert et des services numériques judiciaires aux services de police de toutes les compétences au Canada, en plus des services de police internationaux. Les membres des SET se tiennent à jour dans le domaine des enquêtes judiciaires concernant des ordinateurs et des réseaux et offrent d'autres services spécialisés, notamment des témoignages d'expert pendant des procédures au criminel liées à des enquêtes sur la cybercriminalité. Les groupes intégrés de la criminalité technologique (GICT) de la GRC fournissent également des services spécialisés en enquêtes sur la cybercriminalité. Les GICT sont situés dans des endroits stratégiques à l'échelle du Canada de manière à intervenir en cas d'incident de cybercriminalité en collaboration avec d'autres services de police au pays et à l'étranger et dirigent souvent, au nom du Canada, des enquêtes sur des cybercrimes qui sont d'envergure nationale ou internationale. Ces groupes s'occupent aussi de traiter et d'analyser des preuves numériques à l'appui des enquêtes sur des cybercrimes ou d'autres enquêtes criminelles, ce qui peut comprendre de l'informatique judiciaire, des analyses de systèmes en réseau, la récupération et l'extraction de données, la rétroingénierie de programmes malveillants et l'acquisition d'outils opérationnels à l'appui de techniques d'enquêtes sur la cybercriminalité.

Les services spécialisés de la GRC comprennent également la prestation de la formation appropriée et l'enseignement des compétences nécessaires pour lutter contre la cybercriminalité. Les enquêteurs sur des affaires de cybercriminalité doivent avoir suivi une formation de base et avancée pour être en mesure de suivre l'évolution des menaces criminelles dans le cyberespace. Par l'entremise des ses Services nationaux de police, la GRC, via le Collège canadien de police, offrent des occasions de formation policière sur les enquêtes et la collecte de renseignements dans le domaine de la cybercriminalité. Les Services nationaux de police comprennent des programmes et services coordonnés et intégrés auxquels les organismes canadiens de l'application de la loi ont accès ayant pour but d'appuyer les enquêtes portant sur les infractions criminelles, y compris la cybercriminalité.

Cadre opérationnel en matière de cybercriminalité de la GRC

Le cadre opérationnel en matière de cybercriminalité de la GRC présente la vision, les piliers, les objectifs et les catalyseurs stratégiques de la GRC aux fins de la lutte contre la cybercriminalité, qui se reflètent dans l'ensemble du plan d'action figurant à la section qui suit. Le cadre et le plan d'action sont centrés sur les opérations policières de base dans le cyberespace et visent à faire en sorte que la GRC ait à sa disposition le personnel, les compétences et les outils appropriés en cette ère numérique.

<table>
<tr><th colspan="4">Cadre opérationnel de la GRC en matière de cybercriminalité</th></tr>
<tr><th colspan="4">Vision – Réduire la menace, l'impact, et la victimisation de la cybercriminalité au Canada</th></tr>
<tr><td>(P) PILIERS</td><td>Définir les menaces de cybercriminalité et en établir l'ordre de priorité au moyen de la collecte et de l'analyse de renseignements (P1)</td><td>Cibler les cybercriminels grâce à des mesures de répression et d'enquête adaptées (P2)</td><td>Soutenir les enquêtes sur la cybercriminalité grâce à des compétences, à de la formation et à des outils spécialisés (P3)</td></tr>
<tr><td>(O) OBJECTIVES</td><td>• Renforcer la collecte et l'analyse de données relatives à la cybercriminalité afin de guider les enquêtes et d'autres mesures d'application de la loi (O1)
• Exploiter les renseignements criminels afin d'identifier les menaces de cybercriminalité sérieuses et nier aux cybercriminels leurs outils (O2)
• Travailler de concert avec les partenaires de l'application de la loi et en industrie privée pour perturber les menaces de cybercriminalité nationales et internationales (O3)</td><td>• Développer une équipe élite pour les enquêtes de cybercriminalité en priorité (O4)
• Accroître les capacités techniques afin de compléter les enquêtes dont l'aspect cyber fait partie de l'acte criminel présumé (O5)
• De concert avec les partenaires au plan national et international, viser les cybercrimes les plus sophistiqués et complexes (O6)</td><td>• Accroître les capacités de gestion des preuves numériques en appui des enquêtes de cybercriminalités (O7)
• Acquérir des outils opérationnels pour les enquêtes portant sur la cybercriminalité (O8)
• Élargir la formation à l'intention des organismes d'application de la loi pour enquêteurs en cybercriminalité et aux analystes de renseignements (O9)</td></tr>
<tr><td>(C) CATALYSEURS</td><td colspan="3">Connaissances – Développer un régime robuste et extensible de formation à l'intention des organismes d'application de la loi afin d'attaquer la cybercriminalité plus effectivement (C1)
Outils– Doter les organismes d'application de la loi avec les outils opérationnels dont ils ont besoin pour enquêter la cybercriminalité à tous les niveaux policiers (C2)
L'échange d'information – Faciliter le signalement de victimes de cybercriminalité, et améliorer l'échange d'information entre les partenaires (C3)
Coordination – Faciliter les opérations policières conjointes et résolution d'incompatibilité avec les partenaires en application de la loi lors des projets visant la cybercriminalité (C4)
Industrie – Engager le secteur privé afin d'adresser les problématiques de la cybercriminalité partagés et encourager des partenariats mutuellement avantageux (C5)
Sensibilisation communautaire – Informer les Canadiens et Canadiennes ainsi que le secteur privé des menaces nouvelles et émergentes pour prévenir la cybercriminalité dans ses premiers pas (C6)
Législation et politiques – Appuyer la modernisation des moyens légaux disponibles au Canada pour être à l'avant-garde des changements en technologie (C7)</td></tr>
</table>

Plan d'action de la GRC en matière de lutte contre la cybercriminalité

Le plan d'action de la GRC en matière de lutte contre la cybercriminalité s'inspire du cadre opérationnel. Il propose 15 mesures de suivi assorties d'indicateurs de réussite et d'échéanciers en vue de la mise en œuvre du cadre opérationnel en matière de cybercriminalité et de l'amélioration des mesures prises par la GRC pour contrer la cybercriminalité.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
1. Mettre sur pied une nouvelle équipe d'enquêteurs se consacrant à la lutte contre la cybercriminalité. Liens au cadre opérationnel : P2; O4; O5; O6; C4	- Mener plus d'enquêtes sur la cybercriminalité. - Appréhender plus de cybercriminels. - Perturber davantage d'activités cybercriminelles.	Période de mise en œuvre : 2015-2020 Mise en œuvre intégrale : 2020 et années subséquentes
Description : La GRC a besoin de ressources d'enquête dédiées à la lutte contre la cybercriminalité de manière à ce que de nouvelles capacités techniques soient intégrées aux mesures de répression habituelles. Afin de répondre à ce besoin, la GRC mettra sur pied une équipe à Ottawa, qui sera chargée d'enquêter sur les menaces les plus importantes pour l'intégrité politique, économique et sociale du Canada qui aurait une incidence négative sur la réputation et l'économie du Canada. L'équipe s'attaquera aux activités cybercriminelles d'envergure comme les intrusions dans les réseaux du gouvernement, les marchés criminels en ligne ou les cybercrimes impliquant l'utilisation non autorisée d'ordinateurs à grande échelle et des méfaits concernant des données entraînant des pertes économiques considérables. L'équipe tirera parti des groupes opérationnels de la GRC de partout au Canada qui offrent des services spécialisés et technologiques à l'appui des enquêtes sur la cybercriminalité et travaillera à des opérations policières conjuguées avec des partenaires du milieu de l'application de la loi au pays et à l'étranger. Grâce à cette nouvelle équipe d'enquêteurs, la GRC sera mieux outillée pour enquêter sur des cybercrimes soupçonnés ciblant des Canadiens au pays et ailleurs dans le monde, par exemple des menaces d'envergure aux réseaux, aux biens, aux infrastructures essentielles et à d'autres cybersystèmes essentiels du Canada.		
2. Mettre en place une structure de gouvernance en ce qui concerne les priorités et les opérations en matière de cybercriminalité. Liens au cadre opérationnel : P1; P2; P3; O3; O6; C3; C4; C5	- Assurer la gouvernance, la surveillance et la reddition de comptes pour l'équipe d'enquêteurs se consacrant à la lutte contre la cybercriminalité. - Offrir un soutien, des conseils et une orientation en matière d'opérations tactiques pour tous les gros projets d'enquête en matière de cybercriminalité.	Période de mise en œuvre : 2015-2017. Mise en œuvre intégrale : 2017 et années subséquentes
Description : La GRC a besoin d'une structure de gouvernance pour assurer la surveillance des priorités et des opérations d'enquête en matière de cybercriminalité.		

Afin de répondre à cette exigence, la GRC affectera du personnel à la gouvernance, à la surveillance et à la reddition de comptes pour la nouvelle équipe d'enquêteurs se consacrant à la lutte contre la cybercriminalité tout en veillant au respect de la structure de gouvernance de la GRC en ce qui concerne ses priorités en matière de crimes graves, de crime organisé, de sécurité nationale et de criminalité financière. La structure de gouvernance de la GRC en matière de cybercriminalité sera sous l'égide des Opérations criminelles de la Police fédérale de la Gendarmerie. D'autres mécanismes de surveillance seront en place pour les services spécialisés de la GRC qui appuient les enquêtes sur la cybercriminalité.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
3. Mettre sur pied un groupe du renseignement voué au repérage de menaces de cybercriminalité, nouvelles et émergentes. Liens au cadre opérationnel : P1; O1; O2; O3; C3; C4; C5	- Recueillir des renseignements sur les menaces et les tendances en matière de cybercriminalité et analyser les sources de données afin de cerner les vulnérabilités et les mesures de répression potentielles à l'intention des enquêteurs. - Produire des renseignements sur la cybercriminalité afin de trouver des pistes et d'établir des priorités opérationnelles afin que des mesures de répression soient prises.	Période de mise en œuvre : 2015-2017. Mise en œuvre intégrale : 2017 et années subséquentes
Description : La GRC a besoin de ressources affectées à l'analyse d'un plus grand nombre de sources de données et à la promotion d'une vision stratégique et nationale du renseignement en matière de cybercriminalité, et pour mieux repérer les cybercrimes d'envergure aux fins de répression. Afin de répondre à cette exigence, la GRC créera un groupe de renseignements sur la cybercriminalité dans son Centre national de coordination du renseignement (CNCR). Le CNCR recueillera et analysera des renseignements criminels sur des cybercrimes provenant de sources au pays et à l'étranger dans les cas où des présumées activités cybercriminelles ont été détectées et signalées à la GRC. Grâce au groupe de renseignements en matière de cybercriminalité, la GRC sera mieux à même d'analyser les menaces de cybercriminalité dans le cadre de ses opérations et d'affecter ses ressources de manière à cibler les auteurs des cybercrimes les plus graves et les criminels les plus prolifiques. De plus, en recourant au CNCR, la GRC aura plus de facilité à établir des liens entre les menaces de cybercriminalité et d'autres activités criminelles comme les délits financiers, les crimes graves ou le crime organisé.		
4. Renforcer les capacités de collecte d'éléments de preuve numérique pour les besoins des enquêtes en matière de cybercriminalité. Liens au cadre opérationnel : P3; O7; O8; C2	- Assurer un soutien en matière d'analyse judiciaire numérique dans le cadre d'enquêtes sur des cybercrimes, y compris celles menées par l'équipe d'enquêteurs se consacrant à la cybercriminalité. - Acquérir des outils opérationnels afin d'analyser les éléments de preuve numériques plus efficacement.	Période de mise en œuvre : 2015-2020 Mise en œuvre intégrale : 2020 et années subséquentes

Description : Les enquêtes sur des cybercrimes diffèrent grandement des enquêtes criminelles habituelles. En effet, elles doivent davantage être menées dans des environnements virtuels, par l'entremise de l'analyse de sources ouvertes et l'utilisation de moyens secrets, et l'obtention et l'analyse de données (éléments de preuve potentiels) pour orienter les enquêtes. On s'attend à ce que la nouvelle équipe d'enquêteurs affectés à la cybercriminalité traite des éléments de preuve numériques complexes et en grande quantité, notamment des éléments de preuve potentiels provenant de serveurs et d'appareils numériques saisis légalement.

Afin de répondre à cette exigence, la GRC fera l'acquisition d'outils opérationnels et affectera du nouveau personnel à l'appui direct des exigences en matière d'éléments de preuve numériques dans le cadre d'enquêtes sur des cybercrimes, y compris celles menées par la nouvelle équipe d'enquêteurs. Grâce à ces ressources, on pourra veiller à ce que des moyens et des outils à la fine pointe de la technologie soient en place pour appuyer les enquêtes prioritaires en matière de cybercriminalité. En outre, la GRC examinera les exigences de capacité pour apporter les compétences numériques légistes dans l'avant-plan de travail de policier.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
5. Accroître les occasions de formation en enquête sur la cybercriminalité pour les organismes canadiens d'application de la loi. Liens au cadre opérationnel : P3; O9; C1	- Élaborer et mettre en œuvre de nouveaux cours en enquête sur la cybercriminalité à l'intention des organismes d'application de la loi. - Élargir les compétences de base et avancées en matière d'enquête sur la cybercriminalité à l'échelle du pays.	Période de mise en œuvre : 2015-2017 Mise en œuvre intégrale : 2017 et années subséquentes

Description : Les enquêteurs criminels et les analystes de renseignements doivent suivre une formation de base et avancée sur les technologies nouvelles et émergentes pour suivre l'évolution des menaces criminelles dans le cyberespace. Afin de répondre à cette exigence, la GRC améliorera la formation sur la cybercriminalité à l'intention des organismes d'application de la loi en offrant à ses membres et à ses partenaires provinciaux et municipaux de nouvelles occasions de formation en renseignement et en enquêtes sur la cybercriminalité.

La GRC offre aux organismes d'application de la loi de la formation sur les techniques d'enquête et de collecte de renseignements en matière de cybercriminalité par l'entremise de l'Institut d'apprentissage en criminalité technologique (IACT) du Collège canadien de police. L'IACT est le seul établissement au Canada qui offre aux organismes d'application de la loi un programme de formation complet en cybercriminalité et sur les diverses techniques d'enquête dans ce domaine. Par l'entremise de l'IACT, la GRC élaborera et mettre en œuvre de nouveaux cours en enquête sur l'analyse d'appareils numériques mobiles et sur les sources ouvertes sur Internet et des techniques d'enquêtes secrètes en ligne, des domaines très prisés par les organismes canadiens d'application de la loi.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
6. Se pencher sur des façons de recruter plus efficacement des enquêteurs se consacrant à la cybercriminalité et d'autres personnes qui possèdent des compétences techniques pour lutter contre les cybercrimes. Liens au cadre opérationnel : P2; P3; O4; O5; O9; C1	- Élaborer une stratégie visant à recruter plus efficacement des enquêteurs en cybercriminalité, des analystes de renseignements et d'autres personnes qui possèdent des compétences techniques pour lutter contre les cybercrimes. - Prendre en considération les stratégies de recrutement d'autres organisations gouvernementales.	En cours.
Description : Les enquêtes sur des cybercrimes sont souvent complexes et longues et nécessitent le recours à des personnes qui possèdent des compétences hautement spécialisées et techniques, par exemple en sciences informatiques et en génie des réseaux. Afin de répondre à cette exigence, la GRC se penchera sur les stratégies actuelles de recrutement de policiers et de civils et prendra en considération de nouvelles techniques de recrutement et de maintien de l'effectif visant à attirer davantage d'experts en cybertechnologies. Parmi les stratégies de recrutement possibles, mentionnons l'examen de modèles de recrutement en vigueur à l'étranger et d'autres façons de réformer les mesures de recrutement d'experts en cybertechnologies, par exemple l'initiative des étudiants bénévoles en cybertechnologies (Cyber Student Volunteer Initiative) du département de la Sécurité intérieure des États-Unis et la réserve conjointe d'experts en cybertechnologies (Joint Cyber Reserve) du Royaume-Uni. La GRC envisage également de créer des campagnes de recrutement ciblées à l'intention des établissements universitaires spécialisés dans l'informatique ou des domaines connexes, de faire la promotion d'occasions de formation immédiates en enquête sur la cybercriminalité pour les cadets de la GRC ou de prendre part à de vastes initiatives de recrutement dans la communauté des cybertechnologies du gouvernement.		
7. Renforcer les partenariats public-privé et d'autres efforts de liaison afin de contrer la cybercriminalité. Liens au cadre opérationnel : P1; O3; C5	- Établir davantage de partenariats public-privé et faire appel à plus d'agents de liaison pour des opérations liées à la cybercriminalité. - Trouver plus de sources de données sur les menaces et les tendances en matière de cybercriminalité ayant des liens avec le Canada.	En cours.
Description : Aucune organisation ne détient à elle seule toute l'information requise pour bien comprendre la cybercriminalité, suivre son évolution et la combattre. La portée et l'envergure de la cybercriminalité sont vastes, et c'est pourquoi des organisations des secteurs public et privé doivent collaborer et échanger de l'information sur les menaces de cybercriminalité nouvelles et émergentes. Afin de répondre à cette exigence, la GRC continuera de renforcer ses partenariats public-privé et d'accroître ses efforts de liaison afin de lutter contre la cybercriminalité. Elle établira des partenariats plus solides avec des organisations qui se consacrent à lutter contre la cybercriminalité, notamment la National Cyber Forensics & Training Alliance (NCFTA) des États-Unis, la NCFTA Canada et des organismes des secteurs des infrastructures essentielles du Canada, afin de mieux comprendre les principales menaces de cybercriminalité et les façons de les déjouer.		

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
8. Se pencher sur des façons de renforcer la capacité du CAFC en tant que source fiable de données et de renseignements sur des cybercrimes motivés par l'appât du gain. Liens au cadre opérationnel : P1; O1; O2; O3; C3; C5	- Analyser et perturber un éventail plus vaste de menaces de cybercriminalité motivées par l'appât du gain. - Améliorer le signalement de victimes de cybercrimes motivés par l'appât du gain.	En cours.
Description : Le Centre antifraude du Canada (CAFC) joue un rôle important dans l'analyse et la réduction de la fraude en ligne en travaillant de concert avec les services de police et le secteur privé au Canada afin de perturber les activités criminelles dans le cyberespace. Cependant, les cybercrimes motivés par l'appât du gain ne se limitent pas à la fraude, et les organismes d'application de la loi doivent donc prendre en considération d'autres types d'infraction. Afin de répondre à cette exigence, le CAFC se penchera sur la nécessité de s'attaquer à un éventail plus vaste de menaces de cybercriminalité motivées par l'appât du gain comme les cybercrimes impliquant la violation de la propriété intellectuelle et le vol d'identité. Le CAFC examinera également des façons d'accroître la capacité d'enregistrement des signalements de victimes de présumés cybercrimes et d'améliorer l'échange d'information policière sur des activités cybercriminelles et des tendances en la matière. De plus, la GRC se penchera sur le rôle du CAFC dans le contexte de la gestion de l'information opérationelle de la Police fédérale, et sur ses liens potentiels avec les Services nationaux de police (SNP).		
9. Examiner des façons d'améliorer la collecte de renseignements sur des incidents suspects de cybersécurité touchant des infrastructures essentielles et d'autres cybersystèmes essentiels du Canada et d'améliorer l'analyse de tels incidents. Liens au cadre opérationnel : P1; O1; O2; O3; C3; C5	- Améliorer la collecte de renseignements sur des incidents suspects et présumés de cybersécurité touchant des infrastructures essentielles et d'autres cybersystèmes essentiels au Canada, et améliorer l'analyse de tels incidents. - Nouer le dialogue avec des représentants du secteur des infrastructures essentielles et des cybersystèmes essentiels pour les renseigner au sujet des présumés cybercrimes et des façons de les enrayer.	En cours.
Description : La cybercriminalité représente une importante menace pour les infrastructures essentielles du Canada et d'autres cybersystèmes essentiels, notamment dans les secteurs de l'énergie, des télécommunications et des finances. Les systèmes des infrastructures essentielles peuvent comprendre des composants liés à Internet, les rendant ainsi vulnérables aux logiciels malveillants et à d'autres menaces de cybercriminalité. Les répercussions de ces menaces peuvent être variées : espionnage industriel, extraction de données, vol de propriété intellectuelle ou de secrets industriels, ou tactiques plus perturbatrices impliquant la compromission de systèmes. Ces menaces sont de plus en plus complexes et nombreuses, et les organismes d'application de la loi et d'autres parties prenantes des secteurs public et privé doivent accroître leur travail de collaboration pour contrer ces menaces.		

Afin de répondre à cette exigence, la GRC se penchera sur des façons d'améliorer la collecte et l'analyse d'incidents suspects de cybersécurité touchant des infrastructures essentielles et d'autres cybersystèmes essentiels du Canada. On envisagera de recourir à l'Équipe nationale des infrastructures essentielles (ENIE) et à son analyse des menaces de cybersécurité aux infrastructures essentielles et à d'autres cybersystèmes essentiels. De plus, les organismes d'application de la loi collaboreront avec des représentants du secteur des infrastructures essentielles du Canada, notamment en participant au Forum national intersectoriel ou à des séances d'information dans le secteur. Par exemple, l'ENIE examine les menaces réelles et virtuelles aux infrastructures essentielles du Canada et collabore avec les organismes d'application de la loi et les intervenants du public et du privé afin que toutes les parties prenantes aient une notion commune des menaces criminelles et des risques touchant les infrastructures essentielles du Canada, y compris celles qui sont virtuelles.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
10. Améliorer l'enregistrement et le triage de signalements d'incidents de cybersécurité. Liens au cadre opérationnel : P1; O1; O2; O3; C3; C5	- Renforcer la capacité d'obtenir de l'information sur des incidents de cybersécurité et de communiquer cette information à des secteurs opérationnels. - Améliorer la connaissance de la situation relativement à de présumées activités cybercriminelles au Canada.	En cours.

Description : Compte tenu des incidents de cybersécurité qui surviennent au Canada et ailleurs dans le monde, la GRC prévoit qu'il faudra une plus grande capacité d'enregistrement et de triage des demandes d'aide aux autorités policières, améliorer la connaissance de la situation relativement aux activités cybercriminelles au Canada et communiquer l'information sur les incidents de cybersécurité à la GRC et aux autres services de police canadiens.

Afin de répondre à cette exigence, la GRC se penchera sur des façons d'améliorer les fonctions d'enregistrement et de triage de signalements d'incidents de cybersécurité. On se penchera surtout sur les secteurs opérationnels de la GRC qui facilitent les fonctions d'enregistrement et de triage pour les enquêtes criminelles menées au Canada et les demandes d'aide formulées par des organismes d'application de la loi de l'étranger, y compris le Groupe de l'enregistrement de la Gestion de l'information opérationnelle, Police fédérale, de la GRC et INTERPOL Ottawa.

La GRC s'intéressera également à ses réseaux internationaux touchés par des incidents de cybersécurité signalés et visés par des demandes d'aide de l'étranger aux autorités policières, y compris les réseaux 24/7 d'INTERPOL, du G7 et de la Convention sur la cybercriminalité du Conseil de l'Europe. De façon plus générale, par l'entremise des Services nationaux de police et les opérations de la Police fédérale, examinera comment celle-ci peu mieux aider tous les services canadiens de l'application de la loi dans l'enregistrement et le triage des nouvelles plaintes en matière de cybercriminalité et de coordonner les enquêtes liées à l'utilisation non autorisée d'ordinateurs à grande échelle ainsi que les méfaits concernant des données.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
11. Examiner les modèles intégrés d'application de la loi pour la lutte contre la cybercriminalité. Liens au cadre opérationnel : P1; P2; O3; O6; C4	- Assurer une meilleure coordination et harmonisation à l'échelle nationale et internationale en ce qui concerne les enquêtes d'envergure sur la cybercriminalité.	En cours.
Description : Les activités cybercriminelles sont souvent perpétrées sur de multiples territoires à la fois et leur perturbation requiert des efforts conjugués de services de police canadiens, incluant la coordination nationale et l'harmonisation. Afin de répondre à cette exigence, la GRC se penchera sur ses modèles actuels d'opérations policières conjuguées et prendra en considération des modèles qui conviendraient mieux aux enquêtes criminelles menées dans le cyberespace. On mettra l'accent sur l'examen de mesures de répression coordonnées et et les mesures d'harmonisation ciblant des cybercrimes complexes et perpétrés sur de multiples territoires, plus particulièrement ceux impliquant l'utilisation non autorisée d'ordinateurs à grande échelle et les méfaits concernant des données. Cet examen portera surtout sur les opérations à la Police fédérale, à la Police contractuelle et aux Services nationaux de police de la GRC, y compris les protocoles de collaboration entre la GRC et ses partenaires provinciaux et municipaux de l'application de la loi.		
12. Accroître la collaboration avec de proches partenaires de l'étranger afin de mieux comprendre les cybercrimes transnationaux et de les combattre. Liens au cadre opérationnel : P1; P2; O3; O6; C4	- Assurer une plus grande participation à des forums sur la cybercriminalité tenus par des organismes d'application de la loi de l'étranger. - Favoriser une meilleure compréhension des menaces de cybercriminalité transnationales. - Offrir aux agents de liaison et aux analystes affectés à l'étranger une formation de base sur la cybercriminalité dès qu'elle sera disponible.	En cours.
Description : La cybercriminalité est souvent une menace à l'échelle internationale qui exige une intervention concertée de parties prenantes de partout dans le monde. Afin de répondre à cette exigence, la GRC et ses partenaires de l'application de la loi de l'étranger collaborent de plus en plus afin d'établir une perception commune des menaces de cybercriminalité et de s'assurer que les activités opérationnelles préventives et concertées de lutte contre les menaces sont harmonisées. Par l'entremise d'organismes internationaux clés, notamment les groupes de travail d'INTERPOL, d'EUROPOL, du G8 ou du G7 et des Five Eyes, la GRC continuera de travailler avec ses partenaires de l'application de la loi de l'étranger pour repérer et contrer des menaces de cybercriminalité communes. Elle se penchera également sur des façons de renforcer le rôle qu'elle joue sur la scène internationale dans la lutte contre la cybercriminalité, par exemple en participant plus activement aux évaluations internationales des menaces communes et à l'établissement des activités de lutte en ordre de priorité, tout en faisant preuve de plus de leadership à cet égard.		

Ce travail peut comprendre des activités d'application de la loi organisées à l'échelle internationale auxquelles prend part la GRC, par exemple celles du Five Eyes Law Enforcement Group, du Groupe de travail sur la cyberdélinquance, du Cyber Crime Centre d'EUROPOL, du Joint Cybercrime Taskforce, du Groupe de Rome-Lyon du G7, du Sous-groupe chargé de la criminalité liée à la haute technologie, du groupe de travail international de la NCFTA et du Complexe mondial INTERPOL pour l'innovation.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
13. Examiner des façons de renseigner davantage les Canadiens et le secteur privé sur les menaces de cybercriminalité émergentes. Liens au cadre opérationnel : P1; O1; O2; O3; C3; C6	- Fournir, en temps voulu, aux Canadiens et au secteur privé plus d'information pertinente sur les menaces de cybercriminalité. - Encourager les Canadiens et le secteur privé à prendre des mesures préventives de lutte contre la cybercriminalité.	En cours.

Description : Dans le vaste contexte de la cybersécurité, les organisations des secteurs public et privé et les Canadiens eux-mêmes sont des acteurs importants dans la lutte contre les cybercrimes. Les entreprises privées jouent un rôle crucial dans ce contexte en assurant la protection de leurs réseaux et systèmes névralgiques, notamment dans les secteurs des télécommunications, des institutions bancaires et des infrastructures essentielles. Les Canadiens doivent quant à eux prendre des mesures de base pour se protéger lorsqu'ils utilisent Internet, par exemple en se servant de logiciels de sécurité et d'antivirus à jour, de noms d'utilisateurs uniques et de mots de passe sécurisés, et en téléchargeant des applications provenant de sources fiables seulement. Afin de prendre ces mesures et d'autres mesures préventives pour éliminer les menaces de cybercriminalité, les Canadiens et le secteur privé doivent être renseignés au sujet des cybercrimes qui présentent une menace pour le Canada.

Afin de répondre à cette exigence, la GRC continuera de travailler avec Sécurité publique Canada et d'autres organisations en renseignant les Canadiens et le secteur privé au sujet des menaces de cybercriminalité nouvelles et émergentes. Plus particulièrement, les Services nationaux de prévention du crime de la GRC contribuent aux stratégies de sensibilisation du public visant à prévenir la cyberintimidation, ce qui comprend les initiatives liées aux campagnes Pensez cybersécurité de Sécurité publique. La GRC continuera d'appuyer ces campagnes en organisant des activités de prévention du crime auprès des jeunes. Elle cherchera également des façons de sensibiliser le secteur privé au sujet des menaces de cybercriminalité émergentes par l'entremise de l'Association canadienne des chefs de police et du Comité de liaison avec le secteur privé et par l'amélioration de l'échange d'information entre l'Équipe nationale des infrastructures essentielles de la GRC et les propriétaires et exploitants d'infrastructures essentielles.

Mesure de suivi	Indicateurs de réussite	Échéancier prévu
14. Continuer d'appuyer la modernisation des outils juridiques et stratégiques afin de suivre le rythme des avancées technologiques. Liens au cadre opérationnel : P2; O6; C7	- Moderniser et ajouter des infractions au *Code criminel* et des outils d'enquêtes afin de mieux combattre la cybercriminalité au Canada. - Améliorer la capacité des organismes d'application de la loi à mener des enquêtes sur des cybercrimes au moyen d'outils juridiques harmonisés entre les États alliés.	En cours.
Description : À tous les échelons du gouvernement, la GRC et d'autres services de police canadiens prennent des mesures pour combattre la cybercriminalité à l'intérieur des limites du système juridique canadien, qui se compose de jurisprudence, de lois, de politiques publiques et d'autres instruments juridiques et stratégiques. Si la Stratégie de lutte contre la cybercriminalité de la GRC met l'accent sur le renforcement des mesures prises par la Gendarmerie pour contrer les cybercrimes dans le contexte juridique actuel, il est clair que le régime juridique et de politiques publiques du Canada devra suivre le rythme de l'évolution de la technologie afin que les enquêtes sur la cybercriminalité soient menées efficacement, tant au pays qu'ailleurs dans le monde. La GRC continuera de soutenir le travail du Canada visant à moderniser les infractions criminelles et les outils d'enquête modernisation afin de mieux lutter contre la criminalité à l'ère numérique. Elle engagera la communauté de justice pénale du Canada et identifiera les besoins pour l'éducation des procureurs sur les enquêtes sur la cybercriminalité et les nouveaux aspects juridiques de la cybercriminalité.		
15. Continuer de travailler avec la communauté canadienne de l'application de la loi afin de brosser un tableau national de la cybercriminalité et de prendre les mesures d'intervention nécessaires. Liens au cadre opérationnel : P2; O6; C4	- Assurer un leadership en ce qui concerne l'élaboration d'un cadre pour une stratégie nationale d'application de la loi afin de contrer la cybercriminalité. - Déterminer les mesures que tous les corps de police canadiens pourraient prendre pour lutter plus efficacement contre la cybercriminalité.	En cours.
Description : La cybercriminalité représente une menace commune à tous les niveaux de services de police au Canada, et la GRC et ses partenaires canadiens de l'application de la loi doivent s'unir pour éliminer cette menace. Afin de répondre à cette exigence, la GRC et ses partenaires canadiens de l'application de la loi, par l'intermédiaire de l'Association canadienne des chefs de police, du Comité des crimes électroniques et d'autres tribunes, continuent d'échanger et de créer des mesures coordonnées et nationales visant à lutter contre la cybercriminalité. Ainsi, la GRC s'appuiera sur sa Stratégie de lutte contre la cybercriminalité pour diriger l'élaboration de stratégies nationales d'application plus vaste afin de combattre les cybercrimes, ce qui comprend la prise de mesures visant à dresser un tableau général de la cybercriminalité en fonction de données policières compilées, et pour définir et améliorer les opérations et les mesures communes et concertées des multiples organismes d'application de la loi afin de lutter contre la cybercriminalité. De plus, la GRC fera appel à d'autres parties prenantes, notamment le Comité consultatif national des SNP, le Five Eyes Law Enforcement Group et le Groupe de travail sur la cybercriminalité, afin d'examiner toutes les exigences opérationnelles relatives à l'adoption d'une stratégie nationale de lutte contre la cybercriminalité.		

Conclusion

La cybercriminalité a des répercussions immédiates, concrètes et durables sur les Canadiens. À grande échelle, elle a une incidence préjudiciable sur le gouvernement et les infrastructures essentielles du Canada en plus de nuire à l'intégrité des secteurs économique et financier du pays. À une échelle individuelle, la cybercriminalité entraîne des pertes financières, implique la violation du droit à la vie privée et peut causer des préjudices graves découlant d'infractions comme l'exploitation sexuelle d'enfants et la cyberintimidation. Ces menaces évoluant constamment, un virage est nécessaire relativement à la façon de les comprendre et de les réprimer en cette ère numérique. En effet, les organismes d'application de la loi doivent prendre des mesures pour s'attaquer aux auteurs de crimes dans le cyberespace ainsi que des mesures de sécurité en complément de celles des gouvernements et du secteur privé.

La Stratégie de lutte contre la cybercriminalité de la GRC expose les principales mesures que le service de police national du Canada prendra pour surmonter les difficultés. Les mesures de suivi de la stratégie sont pertinentes sur le plan opérationnel et permettront à la GRC de mieux suivre le rythme de l'évolution des cybercrimes. Les résultats attendus de la GRC à cet égard seront évalués et communiqués dans la Stratégie de cybersécurité du Canada.

Grâce à la Stratégie de lutte contre la cybercriminalité, la GRC pourra davantage collaborer avec ses partenaires nationaux et internationaux de l'application de la loi afin de lutter contre la cybercriminalité.


RCMP
POLICE
GRC