Rapports de la vérificatrice générale du Canada
au Parlement du Canada

Rapport 7

La lutte contre la cybercriminalité

Rapport de l'auditeur indépendant | 2024

Bureau du vérificateur général du Canada
Office of the Auditor General of Canada

Rapport d'audit de performance

Le présent rapport fait état des résultats d'un audit de performance réalisé par le Bureau du vérificateur général du Canada (BVG) en vertu de la *Loi sur le vérificateur général*.

Un audit de performance est une évaluation indépendante, objective et systématique de la façon dont le gouvernement gère ses activités et ses ressources et assume ses responsabilités. Les sujets des audits sont choisis en fonction de leur importance. Dans le cadre d'un audit de performance, le BVG peut faire des observations sur le mode de mise en œuvre d'une politique, mais pas sur le bien-fondé de celle-ci.

Les audits de performance sont planifiés, réalisés et présentés conformément aux normes professionnelles d'audit et aux politiques du BVG. Ils sont effectués par des auditrices compétentes et des auditeurs compétents qui :

- établissent les objectifs de l'audit et les critères d'évaluation de la performance;
- recueillent les éléments probants nécessaires pour évaluer la performance en fonction des critères;
- communiquent les constatations positives et négatives;
- tirent une conclusion en regard des objectifs de l'audit;
- formulent des recommandations en vue d'apporter des améliorations s'il y a des écarts importants entre les critères et la performance évaluée.

Les audits de performance favorisent une fonction publique soucieuse de l'éthique et efficace, et un gouvernement responsable qui rend des comptes au Parlement et à la population canadienne.

La publication est également diffusée sur notre site Web à l'adresse www.oag-bvg.gc.ca.

This publication is also available in English.

Nº de catalogue FA1-27/2024-1-7F-PDF

ISBN 978-0-660-71869-9

ISSN 2561-3456

Photo de la page couverture : iStock.com/gorodenkoff

Survol

Message général

Dans l'ensemble, la Gendarmerie royale du Canada (GRC), le Centre de la sécurité des télécommunications Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) n'avaient ni la capacité ni les outils requis pour appliquer efficacement les lois visant à protéger la population canadienne contre les cyberattaques ou pour s'attaquer à la quantité croissante de cybercrimes, qui deviennent de plus en plus sophistiqués. Nous avons constaté des lacunes dans les interventions, la coordination, les mesures d'application de la loi, le suivi et l'analyse au sein des organisations chargées de protéger la population canadienne contre les cybercrimes, et entre ces organisations.

En 2022, des victimes de fraude ont signalé des pertes financières totalisant 531 millions de dollars au Centre antifraude du Canada. Les trois quarts de ces signalements étaient liés à la cybercriminalité. Le Centre estime que seulement 5 % à 10 % des cybercrimes sont signalés. Sans intervention rapide, les pertes financières et de renseignements personnels ne feront que croître à mesure que la cybercriminalité et les cyberattaques continueront d'augmenter.

Pour lutter efficacement contre la cybercriminalité, il faut veiller à ce que les signalements soient acheminés aux organisations les mieux placées pour les recevoir. Ces organisations doivent donner suite aux signalements reçus pour aider à protéger la population canadienne contre les risques de pertes financières et d'autres préjudices. Même si la GRC, le Centre de la sécurité des télécommunications Canada et Sécurité publique Canada ont discuté de la mise en place d'un guichet unique où les particuliers canadiens pourraient signaler les incidents de cybercriminalité, un tel guichet n'a pas encore été mis en place. Selon le système actuel, les personnes sont laissées à elles-mêmes pour déterminer où faire un signalement, ou elles peuvent se faire demander de signaler ce même incident à une autre organisation. Par exemple, entre 2021 et 2023, le Centre de la sécurité des télécommunications Canada a jugé que près de la moitié des 10 850 signalements reçus ne relevaient pas de son mandat puisqu'ils visaient des particuliers et non des organisations canadiennes. Toutefois, il n'avait pas répondu à bon nombre de ces particuliers pour leur dire de signaler l'incident à une autre organisation.

En général, nous avons constaté que la main-d'œuvre en cybersécurité du Canada devait être renforcée au sein de toutes les organisations. Par exemple, la GRC a eu de la difficulté à pourvoir les postes au sein de ses équipes d'enquête en cybercriminalité. Nous avons estimé qu'en date de janvier 2024, près du tiers des postes au sein de l'ensemble des équipes étaient vacants. À notre avis, avoir un plan pour réduire les lacunes en ressources humaines dans l'ensemble des organisations responsables est une composante importante d'une Stratégie nationale de cybersécurité renouvelée.

La GRC avait aussi accusé des retards dans la mise en place de sa Solution nationale en matière de cybercriminalité, un système de technologie de l'information visant à faciliter le signalement des cybercrimes par les victimes, à fournir une base de données commune sur la cybercriminalité à l'intention des organismes d'application de la loi canadiens et à permettre la vérification du recoupement entre des échantillons de logiciels malveillants nationaux et internationaux.

LES CYBERCRIMES AU CANADA

Hameçonnage

Logiciels malveillants et rançongiciels

Cyberfraudes

Vols d'identité

Principales constatations et données clés

- La GRC, par l'entremise de son Centre national de coordination en cybercriminalité, a établi des partenariats entre les forces de l'ordre canadiennes et internationales pour comprendre les besoins de ses organismes et assurer la coordination des efforts. Toutefois, elle n'avait pas toujours acheminé aux services policiers nationaux les demandes d'information qu'elle recevait de partenaires internationaux.
- La GRC et le Centre de la sécurité des télécommunications Canada coordonnaient souvent bien leurs interventions à l'égard de cas hautement prioritaires, comme les attaques sur des systèmes du gouvernement du Canada ou des infrastructures essentielles.
- Dans un signalement concernant une offre de vente de matériel d'exploitation sexuelle d'enfants, le CRTC n'a pas transféré le signalement aux forces de l'ordre; il a plutôt dit à la personne ayant signalé l'incident de communiquer directement avec les forces de l'ordre.
- Dans un cas, afin d'éviter de faire l'objet d'un mandat de perquisition par un organisme d'application de la loi, le CRTC a supprimé des éléments probants et a retourné des appareils électroniques dans des délais accélérés à une personne faisant l'objet d'une enquête pour infraction à la loi anti-pourriel.
- La Stratégie nationale de cybersécurité établie par Sécurité publique Canada comportait de graves lacunes, notamment l'absence du CRTC à titre d'acteur clé, malgré le mandat de cet organisme consistant à faire appliquer la *Loi canadienne anti-pourriel*, qui est directement lié à la cybercriminalité.

Les **Recommandations et réponses** se trouvent à la fin du présent rapport.

Table des matières

Introduction

Contexte

La cybercriminalité et la menace qu'elle représente pour la population canadienne

7.1 La cybercriminalité représente pour la population canadienne une menace dont la nature évolue rapidement et qui ne cesse de croître. Elle peut viser les actifs financiers, les renseignements personnels et même la sécurité des personnes. La cybercriminalité menace aussi de perturber les activités des entreprises et des institutions et peut comprendre des attaques touchant des infrastructures et des services essentiels, comme les réseaux électriques et les hôpitaux.

7.2 Selon la Gendarmerie royale du Canada (GRC), la cybercriminalité s'entend de tout crime commis dans lequel les technologies de l'information, y compris Internet, jouent un rôle important. Certains cybercrimes ciblent directement les systèmes informatiques, par exemple une intrusion par piratage dans une base de données pour voler ou corrompre des renseignements protégés. Pour d'autres cybercrimes, les technologies de l'information servent d'instrument pour commettre des délits. De nombreux cybercrimes reposent sur l'utilisation de pourriels, ou de courriels envoyés à grande échelle qui visent à persuader les gens de cliquer sur des liens qui pourraient mener à des logiciels malveillants.

7.3 Jusque dans les années 1990, la cybercriminalité mettait habituellement en cause des particuliers ciblant de grandes institutions ou entreprises. Toutefois, la cybercriminalité devient de plus en plus sophistiquée et cible davantage les particuliers. Les cybercriminelles et cybercriminels peuvent agir en solo ou faire partie d'un groupe sophistiqué du crime organisé.

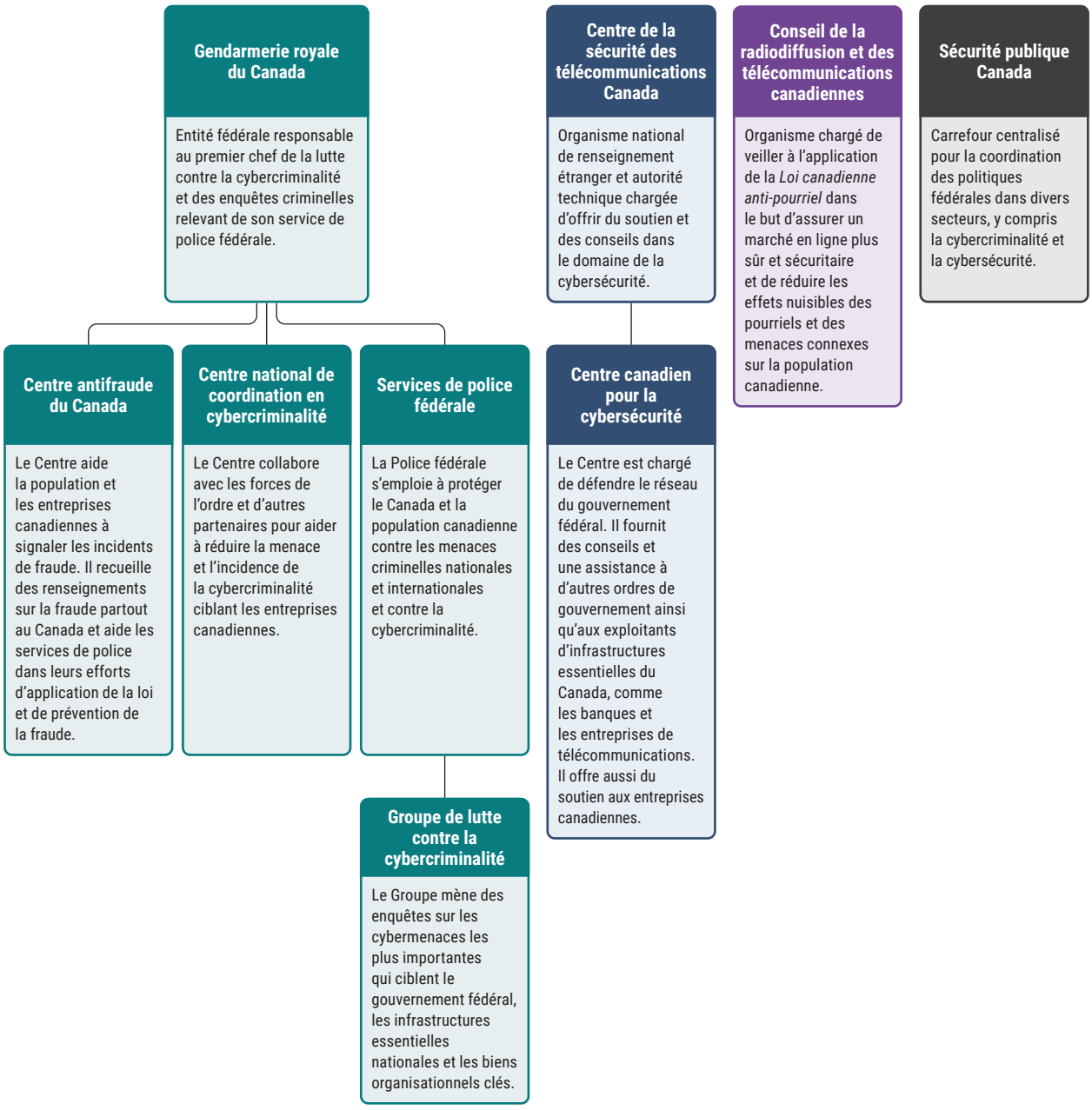
7.4 Année après année, la cybercriminalité prend de l'ampleur, aussi bien du point de vue du nombre d'attaques que de la somme totale des vols. En 2022, le Centre antifraude du Canada, un service national de police exploité conjointement par la GRC, le Bureau de la concurrence du Canada et la Police provinciale de l'Ontario, a reçu des signalements de pertes financières subies par des victimes de fraude totalisant 531 millions de dollars. Les trois quarts de ces signalements étaient liés à des cybercrimes. Ce montant représente plus du triple du montant signalé en 2020. Selon les projections du Centre, cette hausse

se poursuivra, et les pertes signalées atteindront plus d'un milliard de dollars d'ici 2028. Le Centre estime aussi que seulement 5 % à 10 % des cybercrimes lui sont signalés.

Rôles et responsabilités

7.5 Plusieurs organisations fédérales ont des responsabilités en matière de cybercriminalité (voir la pièce 7.1).

Pièce 7.1 — Les organisations fédérales dotées de responsabilités en matière de cybercriminalité



Source : D'après des renseignements fournis par la Gendarmerie royale du Canada, le Centre de la sécurité des télécommunications Canada, le Conseil de la radiodiffusion et des télécommunications canadiennes et Sécurité publique Canada

7.6 **Gendarmerie royale du Canada (GRC)** — La GRC est l'entité fédérale responsable au premier chef de la lutte contre la cybercriminalité. Elle est chargée d'enquêter sur les crimes relevant de la Police fédérale. Cette dernière a comme mandat d'enquêter sur les menaces criminelles les plus importantes qui pèsent sur le Canada, notamment les cybercrimes, le crime organisé grave et transnational et les menaces pour la sécurité nationale. L'une des principales responsabilités de la GRC consiste aussi à fournir des programmes pour appuyer d'autres services de police canadiens. Cela comprend notamment une expertise spécialisée en cybercriminalité et un soutien aux enquêtes. La GRC assure aussi la coordination des enquêtes multiorganisationnelle sur la cybercriminalité.

7.7 **Centre de la sécurité des télécommunications Canada** — Le Centre est l'organisme national du renseignement électromagnétique étranger du Canada. C'est-à-dire qu'il est chargé d'intercepter, de décoder et d'analyser les communications électroniques. Il est aussi l'autorité technique du gouvernement en matière de cybersécurité et fournit une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, notamment la GRC. Il héberge le Centre canadien pour la cybersécurité, qui est chargé de fournir des conseils, une orientation, des services et du soutien en matière de cybersécurité à l'égard des entreprises canadiennes, des infrastructures essentielles, comme les transports et les communications, ainsi que des systèmes du gouvernement fédéral.

7.8 **Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)** — Le CRTC réglemente et supervise la radiodiffusion et les télécommunications. Il assure aussi l'application de la *Loi canadienne anti-pourriel*. Même si les infractions à cette loi ne sont pas criminelles en soi, elles peuvent faciliter l'activité criminelle.

7.9 **Sécurité publique Canada** — Ce Ministère sert de carrefour centralisé pour la coordination des travaux effectués par les ministères et organismes fédéraux dans divers secteurs, dont la cybersécurité. Ce Ministère est aussi chargé d'élaborer des politiques et de fournir des conseils au ministre de la Sécurité publique.

7.10 **Autres organismes** — Les enquêtes criminelles en matière de cybercriminalité peuvent exiger l'intervention de plusieurs des organisations fédérales susmentionnées, ainsi que d'autres organismes d'application de la loi provinciaux, territoriaux et municipaux, de services de police des Premières Nations, ainsi que de partenaires internationaux comme l'Agence de l'Union européenne pour la coopération des services répressifs (Europol).

Initiatives fédérales de lutte contre la cybercriminalité

7.11 Au cours des dernières années, le Canada a entrepris plusieurs initiatives de lutte contre la cybercriminalité :

- **Stratégie nationale de cybersécurité de Sécurité publique Canada** — Lancée en 2018 sous la direction de Sécurité publique Canada, cette stratégie est assortie d'objectifs de lutte contre la cybercriminalité et d'initiatives comme le financement du Centre canadien pour la cybersécurité, la création du Centre national de coordination en cybercriminalité de la GRC et le financement pour développer l'expertise canadienne en cybersécurité. Au moment de notre audit, une nouvelle stratégie était en cours d'élaboration.
- **Centre national de coordination en cybercriminalité de la GRC** — En 2018, le gouvernement du Canada a mis sur pied le centre pour agir à titre de fournisseur de services aux forces de l'ordre canadiennes. Le Centre assure la coordination des enquêtes, offre une orientation et des conseils techniques et produit des renseignements exploitables sur la cybercriminalité. Il a aussi mis en place un système national de signalement des incidents de cybercriminalité. Le Centre s'intéresse principalement à la cybercriminalité dont la cible est la technologie, ce qui comprend les rançongiciels, les cybercrimes axés sur les logiciels malveillants, les atteintes à la sécurité des données et d'autres intrusions ciblant les sociétés et les entreprises canadiennes.
- **Centre antifraude du Canada de la GRC** — Le Centre s'intéresse à la cybercriminalité ciblant les particuliers, par exemple, la fraude, les crimes liés à l'identité, les stratagèmes de rencontre, les menaces à la sécurité des courriels professionnels, la fraude sur les paiements d'avance, l'hameçonnage (attaques visant à amener des particuliers à révéler des renseignements personnels sur des sites qui semblent légitimes) et le harponnage (campagne d'hameçonnage ciblant une personne ou un groupe en particulier). La GRC prend en charge la gestion du Centre, qui est exploité conjointement par la GRC, le Bureau de la concurrence du Canada et la Police provinciale de l'Ontario.
- **Police fédérale de la GRC** — La Police fédérale s'emploie à protéger le Canada et la population canadienne contre les menaces criminelles nationales et internationales et contre la cybercriminalité.
- **Groupe de lutte contre la cybercriminalité de la Police fédérale** — Au moment de la production du rapport, le Groupe comptait cinq équipes d'enquête sur les cybercrimes dans l'ensemble du pays. Ces équipes ont comme mandat de mener des enquêtes sur

les cybermenaces les plus importantes qui ciblent le gouvernement fédéral, les infrastructures essentielles nationales et les biens organisationnels clés.

Objet de l'audit

7.12 Cet audit visait à déterminer si la GRC et les entités fédérales sélectionnées avaient la capacité et les compétences requises pour appliquer efficacement les lois visant à lutter contre les activités de cybercriminalité afin d'assurer la sécurité et la sûreté de la population canadienne.

7.13 Cet audit est important parce que les particuliers, les entreprises, les institutions et les infrastructures du Canada continueront d'être la cible de cybercriminelles et de cybercriminels. En raison de la nature de plus en plus sophistiquée des tentatives de cybercrimes, du faible taux de signalement et du fait que la cybercriminalité traverse les frontières nationales et internationales, il devient plus important que jamais de collaborer et d'intervenir de manière stratégique.

7.14 La section intitulée **À propos de l'audit**, à la fin du présent rapport, donne des précisions sur l'objectif, l'étendue, la méthode et les critères de l'audit.

Constatations et recommandations

Une mauvaise gestion des cas a limité la capacité de la GRC à répondre aux incidents de cybercriminalité

Importance de cette constatation

7.15 Cette constatation est importante parce que les organisations fédérales interviennent dans les cas de cybercriminalité en menant des enquêtes, en avisant les victimes potentielles, comme des entreprises et des organisations, et en fournissant des conseils et une assistance aux victimes pour atténuer les effets des cybercrimes. Une intervention efficace permet de prendre des mesures, notamment d'éviter les rançongiciels, qui préviennent ou réduisent les effets de la cybercriminalité.

Contexte

7.16 Les avis aux victimes découlent souvent de la communication de renseignements par des partenaires internationaux d'application de loi visant à informer la GRC au sujet de cyberattaques criminelles imminentes, en temps réel ou récentes visant des entreprises ou des organisations canadiennes. Les avis peuvent aussi porter sur des cas où, dans le cadre de ses travaux de renseignements, la GRC prend connaissance du fait qu'une organisation a été victime d'une cyberattaque, par exemple, en constatant que des données d'une organisation ont été divulguées et téléversées sur le Web clandestin. Le Centre national de coordination en cybercriminalité de la GRC envoie un avis au service de police municipal, provincial, territorial ou des Premières Nations compétent pour l'informer de la situation afin que la police locale puisse communiquer avec l'organisation victime.

L'absence de procédures et de normes de service de la GRC pour gérer les avis aux victimes

Constatations

7.17 Nous avons constaté que la GRC n'avait pas de norme officielle en ce qui concerne la rapidité avec laquelle son Centre national de coordination en cybercriminalité devait envoyer un avis aux victimes. Des personnes responsables au sein de la GRC ont confirmé qu'elles estimaient que les avis aux victimes étaient hautement prioritaires et que les attentes en général étaient de gérer ces avis dans un délai d'une journée. Nous avons appliqué ce délai d'un jour aux 37 cas que nous avons examinés. Nous avons constaté que la majorité des avis aux victimes étaient envoyés dans le respect de cette cible informelle d'une journée (voir la pièce 7.2). Parmi les 9 cas pour lesquels l'avis a été envoyé dans un délai se situant entre 2 et 27 jours, les personnes responsables ont indiqué qu'elles estimaient que ces cas étaient moins urgents parce qu'ils visaient des activités criminelles survenues dans le passé et qu'ils ne nécessitaient pas une attention immédiate.

Pièce 7.2 — Le Centre national de coordination en cybercriminalité de la GRC a envoyé la majorité de ses avis aux victimes dans un délai d'une journée dans les 37 cas que nous avons examinés.

Délai	Nombre d'avis aux victimes	Pourcentage d'avis aux victimes
1 jour	26 sur 37	70 %
Entre 2 et 27 jours	9 sur 37	24 %
Autre*	2 sur 37	6 %

* Dans un cas, nous n'avons pas pu déterminer le résultat de la demande d'avis aux victimes en raison de lacunes dans le dossier. Dans un deuxième cas, aucun avis aux victimes n'avait été envoyé.

7.18 Nous avons aussi constaté que le Centre de la GRC n'avait pas de procédures normalisées pour trier les demandes d'avis aux victimes selon leur niveau d'urgence, par exemple en accordant la priorité aux cyberattaques visant d'importantes cibles économiques, comme une grande banque ou une importante société de télécommunications. Par conséquent, lorsque le nombre d'avis devant être envoyés aux victimes était élevé et que les demandes s'accumulaient, le Centre n'avait pas de procédures pour s'assurer que les cas les plus urgents étaient recensés et traités en premier.

7.19 L'avis ne se rend pas en effet jusqu'à la victime à moins que le service de police avec lequel la GRC a communiqué avise la victime. Le Centre demande régulièrement aux services de police de confirmer qu'ils ont avisé les victimes. Nous avons constaté que le Centre avait reçu de telles confirmations de la part des services de police pour 24 des 34 cas que nous avons examinés (ce qui représente 71 % des cas). Toutefois, en ce qui concerne les 10 cas restants, les organismes d'application de la loi n'avaient pas répondu. Sans réponse, il était impossible pour le Centre de déterminer si la police locale avait avisé à temps les victimes et si les avis aux victimes avaient aidé à prévenir des cybercrimes.

Recommandation

7.20 Le Centre national de coordination en cybercriminalité de la GRC devrait établir des procédures pour cerner les avis aux victimes les plus urgents et s'assurer qu'ils sont envoyés en premier. Le Centre devrait définir des attentes officielles sur la rapidité avec laquelle les avis aux victimes doivent être envoyés, évaluer le rendement par rapport à ces normes et veiller au respect de celles-ci.

***Réponse de la GRC** — Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Les réponses incomplètes de la GRC aux demandes de coordination des cas avec les partenaires policiers

Constatations

7.21 Le Centre national de coordination en cybercriminalité de la GRC répond aux demandes d'assistance dans le cadre d'enquêtes sur des incidents de cybercriminalité provenant des organismes d'application de la loi partenaires. Chacune de ces demandes comporte deux éléments :

- la réalisation de recherches pour déterminer si un incident précis est lié à d'autres cas de cybercriminalité;
- la communication d'éléments probants et la coordination avec les organismes d'application de la loi partenaires chargés des enquêtes en cours.

7.22 Nous avons constaté que les réponses du Centre à ces demandes n'étaient pas toujours bien documentées. Pour 39 % des demandes (soit 17 demandes sur 44), le dossier ne contenait pas tous les documents requis, comme la demande d'assistance initiale provenant de l'organisation partenaire. Malgré cela, dans certains cas, la superviseure ou le superviseur avait tout de même approuvé et fermé le dossier. De plus, dans certains cas, les examens obligatoires par la superviseure ou le superviseur n'avaient pas été achevés.

7.23 Nous avons constaté que le Centre n'avait pas transmis aux services de police nationaux 7 des 26 demandes (soit 27 % des demandes) provenant de partenaires internationaux que nous avons examinées pour voir si elles comportaient des éléments probants pertinents pour l'enquête. Nous n'avons pas pu déterminer clairement pourquoi le Centre n'avait pas transmis ces demandes. Il n'y avait pas d'explications de ces décisions dans les dossiers. Il était donc impossible de confirmer si l'information n'avait pas été communiquée par erreur ou pour une raison légitime. Par exemple, le partenaire international aurait pu demander que la demande ne soit pas communiquée à l'extérieur de la GRC.

Recommandation

7.24 Le Centre national de coordination en cybercriminalité de la GRC devrait veiller à ce que toutes les demandes d'assistance provenant de partenaires nationaux et internationaux soient dûment documentées et achevées, de sorte que toute l'information nécessaire soit transmise dans le cadre de la réponse. Le Centre devrait communiquer les demandes, s'il y a lieu, à toutes les organisations concernées par la demande.

Réponse de la GRC — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

L’insuffisance du suivi et de l’évaluation des incidents de cybercriminalité par la GRC

Constatations

7.25 Nous avons constaté que l’approche énoncée par la Police fédérale de la GRC consistait à gérer les cybercrimes au moyen d’une gouvernance centralisée pour veiller à ce que les ressources soient affectées aux cas les plus importants. La Police fédérale a un Groupe de lutte contre la cybercriminalité qui compte cinq équipes d’enquête réparties dans l’ensemble du pays. Les équipes se concentrent sur la tenue d’enquêtes sur des cas représentant une menace grave pour le Canada. Le Groupe a quatre secteurs prioritaires visant les activités criminelles qui :

- constituent une menace pour le gouvernement fédéral;
- ciblent les infrastructures essentielles, comme les hôpitaux ou les services publics;
- menacent d’importants biens organisationnels;
- ciblent des institutions canadiennes au nom d’un État étranger.

Toutefois, nous avons constaté que les priorités n’avaient pas été établies. Des enquêtes pouvaient donc être lancées sans que le Groupe de lutte contre la cybercriminalité ait établi l’ordre de priorité et ait assigné des cas potentiels à ses équipes aux fins d’enquête.

7.26 Un contrôle clé utilisé pour veiller à accorder la priorité aux cas les plus importants est un formulaire, nommé l’outil de triage des incidents. Le formulaire comprend des critères d’évaluation, comme l’applicabilité au mandat de la Police fédérale de la GRC, la disponibilité des ressources et les solutions de rechange à une intervention de la Police fédérale. Toutefois, dans le cadre de notre examen d’un échantillon de 36 cas assignés au Groupe de lutte contre la cybercriminalité de la Police fédérale, nous avons constaté que l’outil de triage des incidents n’avait été utilisé que dans 3 des 36 cas (8 %). Nous avons aussi constaté que 5 des 36 cas (14 %) que nous avons examinés ne s’inscrivaient dans aucun des quatre secteurs prioritaires du Groupe, tels que nous les avons présentés au paragraphe 7.25. Par conséquent, les ressources spécialisées n’étaient pas affectées aux cas les plus importants.

7.27 Par ailleurs, nous avons constaté que la gestion des dossiers de la GRC était mauvaise et que la qualité de ses données était faible. Cela a entravé la capacité de la Police fédérale de la GRC à avoir une vue d’ensemble des cas de cybercriminalité signalés à son Groupe de lutte contre la cybercriminalité et à assurer un suivi à l’égard de cas particuliers assignés au Groupe aux fins d’enquête. Par conséquent, la Police fédérale était incapable de dénombrer avec exactitude tous les cybercrimes potentiels qui lui avaient été signalés, et elle ne pouvait pas suivre avec précision les cas assignés à son Groupe de lutte contre la cybercriminalité. Par exemple, nous avons constaté que le système de

gestion des dossiers de la GRC s'appuyait sur des champs de données générés manuellement pour relever les cybercrimes possibles. Ces champs pouvaient être laissés vides ou être remplis incorrectement. Il était donc impossible de recenser avec fiabilité les éventuels cybercrimes.

7.28 En 2018, la GRC a reçu un financement de 78,9 millions de dollars sur 5 ans pour accroître la capacité du Groupe de lutte contre la cybercriminalité. De cette somme, 55,2 millions de dollars avaient été dépensés en date du 31 mars 2023. Étant donné les problèmes que nous avons observés en ce qui concerne les données sur les cybercrimes de la Police fédérale, les résultats publiés pour cette dernière concernant les indicateurs de rendement, comme le nombre d'enquêtes sur les cybercrimes fermées, n'étaient ni exacts ni exhaustifs. En raison de ces données inexactes et incomplètes, la GRC n'a pas pu démontrer si la population canadienne avait reçu des services optimaux pour le financement accordé au Groupe de lutte contre la cybercriminalité.

7.29 Nous avons aussi constaté que la Police fédérale de la GRC avait défini des mesures de rendement internes qui visaient à faciliter la gestion de programme. En raison de données inexactes et incomplètes, la Police fédérale avait été incapable de produire ces mesures pendant la période visée par l'audit. C'est donc dire qu'il manquait à la Police fédérale une source d'information importante pour gérer le Groupe de lutte contre la cybercriminalité.

Recommandation

7.30 La Police fédérale de la GRC devrait adopter un processus de triage uniforme géré de manière centralisée de sorte que les ressources spécialisées dans les enquêtes sur la cybercriminalité soient affectées aux enquêtes sur les cybercrimes les plus graves.

Réponse de la GRC — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Recommandation

7.31 La GRC devrait s'assurer que ses systèmes de gestion de l'information recueillent des données exactes et complètes qui permettent d'évaluer le rendement, d'améliorer la prise de décisions et de démontrer l'optimisation des ressources en ce qui concerne les travaux effectués par le Groupe de lutte contre la cybercriminalité de la Police fédérale.

Réponse de la GRC — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Le Centre de la sécurité des télécommunications Canada répondait efficacement aux incidents de cybercriminalité

Importance de cette constatation

7.32 Cette constatation est importante parce qu'en aidant les organisations canadiennes victimes de cyberattaques, le Centre de la sécurité des télécommunications Canada prévient ou réduit les préjudices causés par ces cyberattaques. En coopérant efficacement avec la GRC, le Centre aide à assurer une réponse fédérale mieux coordonnée et plus efficace à la cybercriminalité.

Le respect par le Centre de la sécurité des télécommunications Canada des normes en ce qui concerne les interventions en temps voulu et les avis aux victimes

Constatations

7.33 Le Centre de la sécurité des télécommunications Canada héberge le Centre canadien pour la cybersécurité. Ce dernier est chargé de fournir des conseils, une orientation, des services et du soutien en matière de cybersécurité à l'égard des entreprises canadiennes, des infrastructures essentielles, comme les transports et les communications, ainsi que des systèmes du gouvernement fédéral. Nous avons constaté que ce Centre canadien pour la cybersécurité avait respecté ses normes en matière d'intervention à la suite de signalements d'incidents de cybercriminalité dans 80 % des cas, y compris en ce qui concerne le suivi auprès des victimes potentielles et l'envoi d'avis à celles-ci. Les organisations qui sont victimes d'incidents de cybercriminalité peuvent communiquer avec le Centre de la sécurité des télécommunications Canada pour obtenir une assistance. Celui-ci n'est pas un organisme d'application de la loi, et il ne peut donc prendre aucune mesure en ce sens. En revanche, il peut fournir des conseils et une orientation aux organisations pour les aider à intervenir à la suite d'une cyberattaque. Le Centre de la sécurité des télécommunications Canada collabore avec d'autres organisations qui devraient participer à l'intervention, comme la GRC ou d'autres organismes d'application de la loi.

7.34 Nous avons examiné un échantillon de 51 incidents de cybercriminalité au cours des exercices 2021-2022 et 2022-2023. Nous les avons sélectionnés parmi un total de 5 341 incidents auxquels le

Centre de la sécurité des télécommunications Canada a donné suite après avoir obtenu un signalement de la part des organisations. Nous avons constaté ce qui suit :

- Le Centre de la sécurité des télécommunications Canada était intervenu en temps opportun dans 80 % des cas. Ses agentes et agents avaient analysé la priorité à accorder aux incidents en fonction des critères de triage présentés dans les procédures opérationnelles normalisées et les avaient assignés à des agentes et à des agents qui y avaient donné suite dans les délais prescrits, soit dans l'heure suivant le signalement pour les incidents les plus graves et dans les deux jours ouvrables pour les incidents les moins graves.
- Les agentes et agents avaient effectué un suivi auprès de l'organisation ayant fait le signalement dans 80 % des cas pour s'assurer que leurs cas avaient été traités de manière appropriée.
- Dans les cas où l'incident signalé touchait une ou plusieurs tierces parties, le Centre de la sécurité des télécommunications Canada avait avisé les tierces parties victimes dans 95 % des cas. Cette pratique était conforme à sa politique selon laquelle les victimes ou parties concernées doivent être avisées pour qu'elles puissent prendre des mesures pour se protéger.

La collaboration efficace entre le Centre de la sécurité des télécommunications Canada et la GRC

Constatations

7.35 Nous avons constaté que le Centre de la sécurité des télécommunications Canada et la GRC avaient coordonné leurs interventions à l'égard d'incidents de cybersécurité. Les deux entités avaient échangé des renseignements sur les cas et coordonné leurs interventions liées aux incidents potentiels de cybercriminalité hautement prioritaires, c'est-à-dire les incidents qui pouvaient toucher les systèmes du gouvernement du Canada ou d'autres systèmes d'importance au Canada.

7.36 Nous avons examiné 41 cas dans lesquels la GRC avait demandé au Centre de la sécurité des télécommunications Canada de collaborer à l'envoi d'un avis aux victimes. Dans 33 cas sur 41 (soit 80 % des dossiers), le Centre national de coordination en cybercriminalité de la GRC avait reçu une réponse du Centre de la sécurité des télécommunications Canada le jour même ou le lendemain.

Le CRTC et le Centre de la sécurité des télécommunications Canada n'avaient pas donné suite à des milliers de signalements de cybercrimes

Importance de cette constatation

7.37 Cette constatation est importante parce que pour lutter efficacement contre la cybercriminalité, il faut que les signalements d'incidents soient transmis aux organisations les mieux outillées pour les recevoir et que ces organisations donnent suite aux signalements, pour ainsi protéger la population canadienne contre le risque de perte financière et d'autres préjudices.

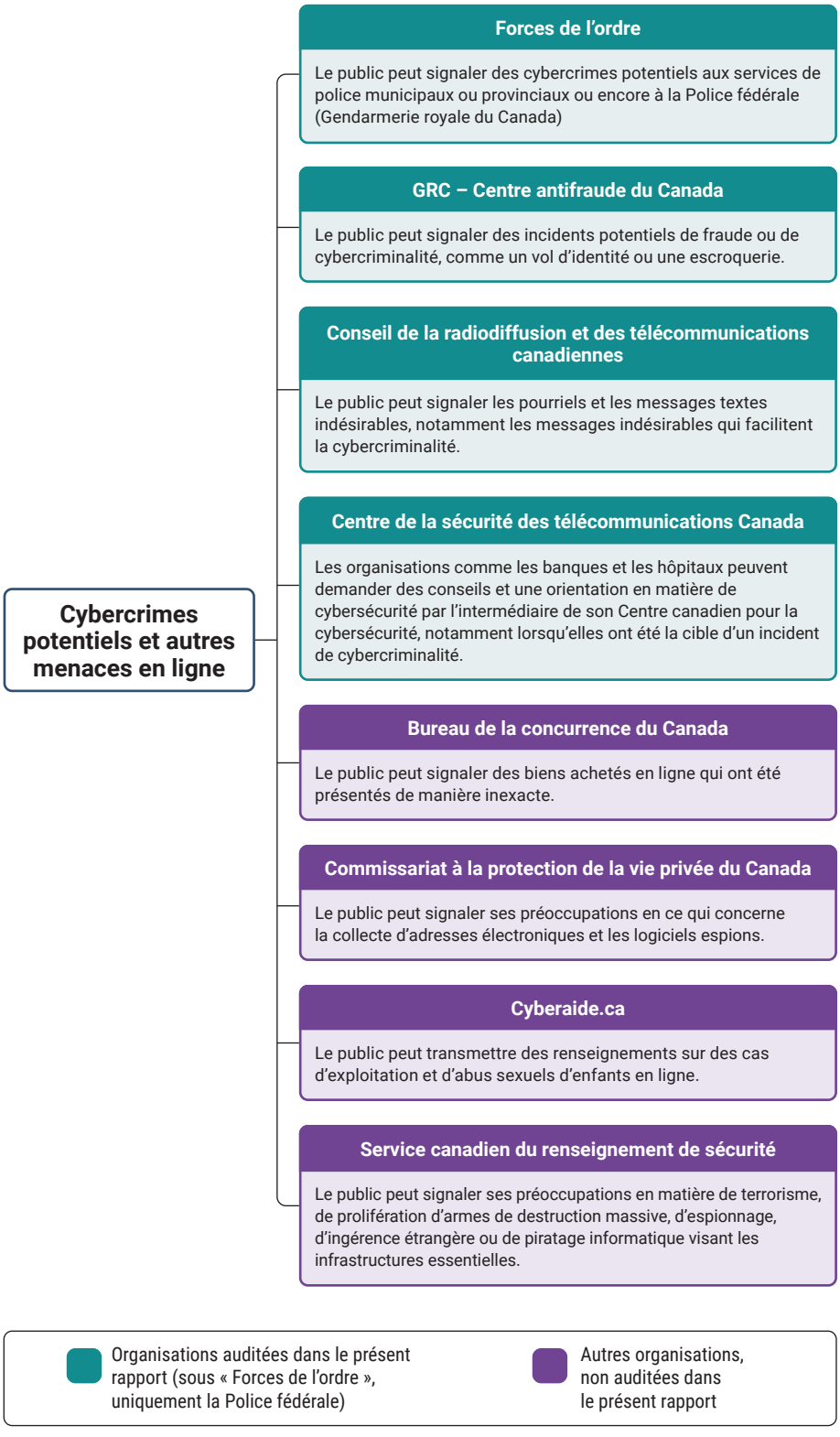
Contexte

7.38 Au Canada, le public peut signaler les cybercrimes potentiels et d'autres menaces en ligne à diverses organisations dotées de mandats différents (voir la pièce 7.3).

7.39 Le mandat du Centre de la sécurité des télécommunications Canada est de fournir des conseils et une assistance technique aux organisations canadiennes confrontées à un cybercrime potentiel. Sa clientèle comprend les propriétaires d'infrastructures essentielles (comme les réseaux électriques et les réseaux de télécommunications), les organisations du gouvernement du Canada et des entreprises du secteur privé. Son mandat ne s'étend pas aux particuliers ayant été victimes de cybercrime. Le Centre doit aussi collaborer avec les organismes d'application de la loi, comme la GRC et le CRTC.

7.40 En 2014, la *Loi canadienne anti-pourriel* est entrée en vigueur. Cette loi vise à protéger la population canadienne contre les pourriels, notamment l'hameçonnage, les logiciels malveillants, le vol d'identité et les escroqueries en ligne. Le Centre de notification des pourriels a été mis en place pour permettre aux membres du public de présenter des plaintes liées à des infractions à la *Loi canadienne anti-pourriel*. Parfois, le CRTC reçoit d'autres types de plaintes qui peuvent justifier une enquête par un autre organisme parce que les menaces peuvent être à la fois une infraction à la *Loi canadienne anti-pourriel* et au *Code criminel*.

Pièce 7.3 — Signalement public de cybercrimes potentiels et d'autres menaces en ligne au Canada



Source : D'après des renseignements fournis par le Centre canadien pour la cybersécurité et le Commissariat à la protection de la vie privée du Canada

7.41 La *Loi canadienne anti-pourriel* est un cadre réglementaire civil. Le CRTC a des pouvoirs d'exécution civile qui sont distincts des pouvoirs des organismes d'application de la loi. Dans le cadre de ses pouvoirs d'enquête, le CRTC peut demander que tous les renseignements pertinents pour une enquête qu'il mène lui soient transmis ou qu'ils soient conservés, et il peut exécuter des mandats de perquisition pour vérifier la conformité. Le CRTC peut aussi prendre des mesures pour traiter les cas de non-conformité, notamment envoyer des avis à des personnes soupçonnées d'avoir enfreint la *Loi canadienne anti-pourriel* et négocier des ententes pour corriger la non-conformité. Ces deux cas peuvent nécessiter le versement d'une somme d'argent précise.

Le peu de mesures prises par le CRTC pour protéger la population canadienne contre les menaces en ligne

Constatations

7.42 Nous avons constaté qu'au cours de l'exercice 2022-2023, le CRTC avait reçu 335 751 signalements par l'entremise de son Centre de notification des pourriels concernant des infractions possibles à la *Loi canadienne anti-pourriel*. Nous avons estimé qu'environ 75 000 signalements, soit 22 % des signalements, étaient des **incidents liés à la cybercriminalité**[1]. Les incidents signalés n'auraient pas tous donné lieu à une enquête. Certains signalements auraient été semblables et auraient pu être regroupés, alors que d'autres auraient pu ne pas contenir suffisamment d'information pour qu'un suivi soit assuré. Toutefois, il reste un gros écart entre le nombre de signalements reçus par le Centre de notification des pourriels et le nombre d'enquêtes menées par le CRTC.

7.43 Nous avons constaté que la plupart des signalements liés à des incidents de cybercriminalité n'avaient pas fait l'objet d'une enquête par le CRTC. Au cours des trois ans de notre période d'audit, nous avons constaté que le CRTC n'avait mené que six enquêtes sur des infractions à la *Loi canadienne anti-pourriel* se rapportant à des incidents liés à la cybercriminalité. Sur ces enquêtes :

- trois avaient entraîné des mesures d'application de la loi à l'égard de particuliers, notamment l'évaluation d'une sanction pécuniaire;
- deux étaient en cours au moment de notre audit;
- une était fermée parce que le CRTC avait déterminé qu'aucune autre mesure n'était nécessaire.

7.44 Nous avons constaté que les procédures opérationnelles du CRTC permettaient l'échange d'information avec les forces de l'ordre dans des circonstances restreintes, notamment au moment d'exécuter ses propres mandats de perquisition pour assurer la sécurité de son

1 **Incident lié à la cybercriminalité** — Un incident visé par la *Loi canadienne anti-pourriel*, mais qui peut aussi constituer une infraction criminelle.

personnel ou en réponse à des ordonnances judiciaires, comme une ordonnance de communication ou un mandat. Toutefois, le CRTC nous a indiqué que sa capacité de communiquer de l'information aux organismes d'application de la loi était limitée parce que la *Loi canadienne anti-pourriel* relevait d'un régime administratif civil et que la divulgation de renseignements aux organismes d'application du droit pénal pourrait porter atteinte aux droits à la vie privée des Canadiennes et des Canadiens.

7.45 Les procédures opérationnelles du CRTC indiquent que l'information devrait toujours être communiquée aux forces de l'ordre lorsqu'une victime signale une situation posant un danger imminent pour la vie ou la sécurité, des menaces au bien-être d'un enfant ou toute activité liée à du matériel d'exploitation sexuelle des enfants ou à la vente de tel matériel. Ces procédures décrivent aussi les étapes additionnelles à prendre lorsque le risque encouru par une personne est particulièrement élevé. En décembre 2021, le CRTC a reçu un signalement provenant d'un particulier, envoyé par l'intermédiaire du Centre de notification des pourriels, qui portait sur une offre d'achat de matériel d'exploitation sexuelle des enfants. Au lieu de transférer le signalement aux forces de l'ordre, le CRTC a communiqué avec le particulier et lui a demandé de signaler l'incident aux forces de l'ordre. Nous ne savons pas si le particulier a procédé de la sorte. Nous avons fait part au CRTC de nos préoccupations quant au fait qu'il n'avait pas transféré ce signalement à un organisme d'application de la loi, comme l'exigeaient ses procédures opérationnelles. Le CRTC a exprimé son désaccord et a indiqué que ses procédures opérationnelles n'exigeaient pas qu'il informe les forces de l'ordre puisque la personne ayant fait le signalement au Centre de notification des pourriels n'était pas la victime potentielle et qu'elle n'était pas à risque de préjudice immédiat. Par conséquent, nous avons signalé l'incident à la GRC en avril 2024.

7.46 Nous avons constaté que pour une des six enquêtes menées dans le cadre de la *Loi canadienne anti-pourriel*, le CRTC avait fourni des renseignements incorrects à un organisme d'application de la loi en réponse à la possibilité de faire l'objet d'un mandat de perquisition. En 2019, le CRTC a lancé une enquête visant plusieurs particuliers pour des infractions liées à la cybercriminalité au titre de la *Loi canadienne anti-pourriel*. Dans le cadre de cette enquête, le CRTC a saisi plusieurs appareils électroniques de particuliers aux fins d'utilisation à titre d'éléments probants. Le CRTC a pris connaissance du fait qu'une des personnes faisait aussi l'objet d'une enquête par un organisme d'application de la loi en raison d'accusations criminelles possibles connexes. Le CRTC a informé l'organisme d'application de la loi qu'il menait sa propre enquête. L'organisme d'application de la loi a émis une ordonnance de communication pour demander au CRTC de lui fournir les éléments probants électroniques stockés sur les appareils, ce qu'il a fait.

7.47 En plus de l'ordonnance de communication, le CRTC a aussi été informé qu'il allait faire l'objet d'un mandat de perquisition pour la saisie des appareils en question. Le CRTC a pris la décision de supprimer les

données sur les appareils de manière accélérée après avoir obtenu le consentement de la personne à qui appartenaient les appareils. Le CRTC a par la suite communiqué avec l'organisme d'application de la loi pour indiquer que les données sur les appareils avaient été supprimées et que le mandat n'était donc plus valable. Toutefois, nous avons constaté que la déclaration faite à l'organisme d'application de la loi était incorrecte, puisque les données sur les appareils avaient été supprimées à une date ultérieure. En octobre 2023, nous avons signalé à la direction et aux cadres supérieurs du CRTC nos préoccupations quant à la façon dont cette question avait été gérée.

7.48 En outre, nous avons constaté d'autres pratiques préoccupantes au CRTC en ce qui concerne la prise de décisions sur les mesures d'application de la loi. Selon la *Loi canadienne anti-pourriel*, une « personne désignée » a le pouvoir de prendre des mesures d'application de la loi, comme émettre des avis de communication ou de préservation de l'information ou des avis d'infractions à la loi. Les membres de la Division de la mise en application du commerce électronique du CRTC sont considérés « des personnes désignées ». Toutefois, nous avons constaté que les services juridiques prenaient souvent des décisions quant à la prise de mesures d'application de la loi, même si les membres des services juridiques ne sont pas des « personnes désignées ».

7.49 Les constatations ci-dessus illustrent certains aspects de la culture du CRTC que nous avons observés au cours de l'audit. Nous avons constaté que le CRTC avait une aversion au risque. Nous avons observé une relation tendue entre les services juridiques et les responsables de la Division de la mise en application du commerce électronique au sein du CRTC. Parfois, cela entraînait des retards et des occasions ratées de réagir aux cybermenaces les plus graves dans le cadre de l'administration par le CRTC de la *Loi canadienne anti-pourriel*. Nous avons observé un manque de confiance et de civilité manifeste entre ces deux équipes. À notre avis, la culture au CRTC a nui à la capacité du personnel de sa Division de la mise en application du commerce électronique d'agir dans l'intérêt public au moment d'exécuter ses tâches.

Recommandation

7.50 Le Conseil de la radiodiffusion et des télécommunications canadiennes devrait s'assurer d'avoir des politiques et des procédures claires décrivant quand et dans quelles circonstances les renseignements qu'il acquiert doivent être communiqués aux forces de l'ordre.

Réponse du Conseil de la radiodiffusion et des télécommunications canadiennes — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Recommandation

7.51 Le Conseil de la radiodiffusion et des télécommunications canadiennes devrait s'assurer que les rôles et responsabilités des personnes responsables de l'application de la loi soient conformes aux exigences de la loi. En outre, il devrait veiller à ce que seules les « personnes désignées » aux termes de la *Loi canadienne anti-pourriel* prennent les décisions clés dans le cadre de leur rôle consistant à faire appliquer la loi.

Réponse du Conseil de la radiodiffusion et des télécommunications canadiennes — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Aucun accusé de réception de la part du Centre de la sécurité des télécommunications Canada lorsque des particuliers signalaient des incidents en ligne

Constatations

7.52 Nous avons constaté que le centre de contact avec le public du Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications Canada avait reçu 10 850 appels téléphoniques, courriels et signalement en ligne au cours des exercices 2021-2022 et 2022-2023. Le Centre de la sécurité des télécommunications Canada a jugé que 5 766 de ces signalements s'inscrivaient dans son mandat puisqu'ils se rapportaient à des entreprises et à des organisations et non à des particuliers. Ces signalements ont été soumis à son protocole d'intervention en cas d'incidents. Ces travaux nous ont permis de confirmer que les cas qui avaient été désignés comme relevant du mandat du Centre avaient été classés correctement et que ce dernier n'avait pas donné suite à des signalements qui ne relevaient pas de son mandat. Les autres signalements reçus, soit 5 084 signalements, avaient été jugés comme ne relevant pas de son mandat puisqu'ils concernaient des particuliers et non des organisations. Le Centre a déterminé que 27 % de ces signalements (1 366 sur 5 084) étaient des cybercrimes potentiels.

7.53 Nous avons constaté que le Centre de la sécurité des télécommunications Canada aiguillait les particuliers canadiens vers les organisations compétentes, comme le Centre antifraude du Canada de la GRC, seulement lorsqu'ils signalaient des incidents par téléphone ou par courriel. Ces signalements représentaient 3 212 (63 %) des 5 084 incidents hors mandat.

7.54 Nous avons constaté que le Centre de la sécurité des télécommunications Canada ne répondait pas aux particuliers canadiens qui signalaient des incidents à partir de son portail de signalement

en ligne (Web). Les signalements en ligne représentaient 1 870 (37 %) des 5 084 incidents hors mandat. En raison de politiques sur la protection des renseignements personnels, le Centre ne transmettait pas non plus ces signalements aux autorités compétentes, comme le Centre national de coordination en cybercriminalité de la GRC, aux fins de suivi. Le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications Canada supprimait presque immédiatement tous les renseignements fournis dans les signalements ne relevant pas de son mandat. Toutefois, nous avons constaté que le Centre de la sécurité des télécommunications Canada ne disposait pas des contrôles requis pour veiller à ce que les signalements aient été correctement évalués comme étant hors mandat avant d'être supprimés. Il en résulte un risque que certains signalements jugés hors mandat puissent avoir été évalués incorrectement, et le Centre aurait dû les traiter.

7.55 Notre recommandation à cet égard est présentée au paragraphe 7.78.

Les limites des données de suivi sur les signalements de cybercrimes hautement prioritaires

Constatations

7.56 Nous avons constaté que le Centre antifraude du Canada de la GRC avait consigné plus de 87 000 signalements de fraude potentielle provenant du public canadien au cours de l'exercice 2022-2023. Le Centre a évalué que plus de 28 000 de ces signalements concernaient des cybercrimes potentiels. Sur ces 28 000 signalements, 3 257 signalements concernaient des victimes canadiennes ayant subi des pertes de 10 000 $ ou plus à la suite d'un cybercrime. Il s'agit du seuil à partir duquel un incident est jugé hautement prioritaire et nécessite la prise de mesures.

7.57 Nous avons constaté que, dans son système interne de gestion de l'information, le Centre antifraude faisait rarement le lien entre les plaintes reçues dans sa base de données et les mesures de suivi correspondantes. Il en est ainsi parce que les plaintes étaient reçues et consignées dans un système, alors que les mesures de suivi étaient consignées dans un autre système. Les signalements dans les deux systèmes devaient être reliés manuellement, et nous avons constaté que le personnel ne l'avait pas fait. Par conséquent, nous avons pu relier aux mesures de suivi correspondantes seulement 6 % des dossiers de plainte hautement prioritaires (soit 196 dossiers sur 3 257). Par conséquent, le Centre antifraude du Canada ratait des occasions de mieux comprendre les méthodes efficaces de règlement des plaintes et de mieux rendre compte des progrès réalisés. L'incapacité d'assurer un suivi à l'égard des incidents signalés avait aussi entraîné un risque que certains cas hautement prioritaires ne soient pas traités.

Recommandation

7.58 La GRC devrait améliorer ses systèmes et pratiques de gestion de l'information afin d'associer systématiquement les signalements reçus par le Centre antifraude du Canada aux mesures prises. La GRC pourra ainsi suivre les progrès réalisés par rapport aux cas hautement prioritaires et cerner les approches efficaces utilisées.

Réponse de la GRC *— Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

La GRC ne s'était pas dotée des capacités requises pour lutter contre le problème croissant que représente la cybercriminalité

Importance de cette constatation

7.59 Cette constatation est importante parce que pour être efficace dans ses efforts de lutte contre la cybercriminalité, la GRC doit avoir un nombre suffisant de personnes ayant les compétences nécessaires pour mener des enquêtes sur la cybercriminalité ainsi que de l'information et des systèmes de TI complets et adaptatifs.

Contexte

7.60 En 2018, la GRC a soumis une analyse de rentabilisation qui a fait ressortir la nécessité de mettre en place des systèmes de TI pouvant stocker de grandes quantités de données nécessaires pour assurer un suivi des données liées à la cybercriminalité et en faire une analyse efficace. L'analyse de rentabilisation a fait ressortir que de tels systèmes étaient nécessaires pour permettre au Centre national de coordination en cybercriminalité d'atteindre sa pleine capacité opérationnelle. En juin 2020, la GRC a reçu 69,5 millions de dollars pour l'élaboration d'un système de TI qui l'aiderait dans la lutte contre la cybercriminalité, soit la Solution nationale en matière de cybercriminalité. Celle-ci devait être pleinement mise en œuvre au 31 mars 2023, mais sa mise en œuvre a été retardée. La Solution devrait maintenant être lancée en mars 2025.

7.61 La Solution nationale en matière de cybercriminalité devrait comprendre trois composantes :

- un portail public actualisé permettant aux victimes de signaler des cybercrimes;
- une base de données renfermant des indicateurs de cybercrimes, des renseignements sur les cas et d'autres données dans laquelle les organismes d'application de la loi canadiens peuvent faire des

recherches en vue de relever des cas communs et de faciliter la coordination des enquêtes;

- un système qui permet la vérification du recoupement entre des échantillons de logiciels malveillants nationaux et internationaux pour aider à relever des éléments comme des adresses IP malveillantes associées à une activité criminelle connue.

L'insuffisance des ressources humaines

Constatations

7.62 Nous avons constaté que les équipes d'enquête sur les cybercrimes de la GRC éprouvaient des difficultés persistantes à recruter et à maintenir en poste du personnel ayant les compétences techniques nécessaires, ce qui avait une incidence sur la capacité de la GRC à lutter contre la cybercriminalité. La Police fédérale de la GRC n'avait pas de suivi fiable du nombre de postes vacants au sein de son Groupe de lutte contre la cybercriminalité. En janvier 2024, nous avons estimé que 30 % des postes étaient vacants.

7.63 Toutefois, nous avons relevé des lacunes dans l'analyse de la GRC concernant ses problèmes de dotation. Plus particulièrement, même si la GRC avait recueilli des données sur les motifs de départ, ainsi que sur le mieux-être et la diversité du personnel dans le cadre de son analyse, cette analyse ne visait pas précisément les postes liés à la cybercriminalité. De plus, la GRC n'avait pas effectué une analyse de sa main-d'œuvre interne, c'est-à-dire de son effectif actuel, de ses besoins en effectif et de la progression du personnel au sein de l'organisation. Une telle analyse aiderait la GRC à recruter et à maintenir en poste du personnel chargé de la lutte contre la cybercriminalité. Des responsables au sein de la GRC nous ont indiqué que ces difficultés étaient principalement attribuables à la rémunération offerte. Ces responsables nous ont aussi dit que les personnes effectuant le même travail technique en cybercriminalité dans le secteur privé étaient généralement mieux payées.

Recommandation

7.64 La GRC devrait mener une analyse pour comprendre ses difficultés à recruter et à maintenir en poste du personnel pour les postes spécialisés en cybercriminalité. Elle devrait ensuite se servir des résultats de cette analyse pour orienter ses futurs efforts de recrutement et de maintien en poste en vue d'accroître sa capacité de lutte contre la cybercriminalité.

Réponse de la GRC *— Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Le retard dans la mise en œuvre de la Solution nationale en matière de cybercriminalité de la GRC

Constatations

7.65 La GRC a commencé le déploiement de composantes de la Solution nationale en matière de cybercriminalité aux fins d'essais par des utilisatrices et utilisateurs et aux fins d'utilisation opérationnelle restreinte en avril 2023. Toutefois, les responsables nous ont indiqué que la pleine mise en œuvre de la solution avait été retardée jusqu'en mars 2025, soit plus de deux ans après la date prévue à l'origine.

7.66 Nous avons constaté que diverses raisons expliquaient ce retard, notamment le fait que la GRC avait sous-estimé la complexité de la migration des données existantes vers le nouveau système. En outre, des problèmes étaient survenus en ce qui concerne la mise en adéquation des fonctionnalités du système avec les besoins des utilisatrices et des utilisateurs.

7.67 Au cours de la période d'audit, le Centre national de coordination en cybercriminalité de la GRC s'appuyait sur divers systèmes de TI qui devaient être renforcés par des processus manuels. Nous avons constaté que ces systèmes étaient limités dans leur capacité à recevoir et à relier les incidents de cybercriminalité signalés dans les différentes bases de données des services de police du Canada et des sources internationales.

7.68 Nous avons constaté qu'au 31 décembre 2023, la GRC avait dépensé 29,7 millions sur les 69,5 millions de dollars qu'elle avait obtenus en 2020 au titre du projet. Des responsables au sein de la GRC nous ont indiqué s'attendre à ce que le projet soit réalisé selon le budget établi, en dépit de ce retard. Toutefois, nous avons constaté que les coûts liés au personnel associé au projet n'avaient pas tous été inclus dans les rapports financiers. À notre avis, les retards constants dans le calendrier de projet constituent un risque croissant que les fonds investis dans le projet ne produisent pas tous les avantages escomptés et qu'il y ait des dépassements de coûts de projet.

Recommandation

7.69 La GRC devrait veiller à régler les problèmes associés à la mise en adéquation des fonctionnalités de la Solution nationale en matière de cybercriminalité avec les besoins des utilisatrices et des utilisateurs afin que le projet respecte l'ensemble des exigences énoncées. Elle devrait aussi mettre en œuvre des réponses efficaces aux risques et des plans d'urgence pour que le projet soit réalisé dans le respect du budget et du calendrier révisé.

Réponse de la GRC — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Les partenariats établis par la GRC avec les forces de l'ordre canadiennes et internationales

Constatations

7.70 Nous avons constaté que le Centre national de coordination en cybercriminalité de la GRC avait établi des partenariats avec les organismes d'application de la loi canadiens et internationaux. Les partenariats ont aidé le Centre à comprendre les besoins de ces organismes en matière de programmes de la GRC appuyant leurs efforts de lutte contre la cybercriminalité et à communiquer de l'information générale sur les tendances en matière de cybercriminalité. Par exemple, à l'échelle nationale, certains membres du personnel du Centre siégeaient au Comité sur la cybercriminalité des Services nationaux de police. Par l'entremise de ce comité, divers services de police canadiens et d'autres partenaires clés échangent des renseignements sur les tendances en matière de cybercriminalité.

La stratégie pangouvernementale comportait des lacunes en ce qui concerne certains aspects clés de la lutte du Canada contre la cybercriminalité

Importance de cette constatation

7.71 Cette constatation est importante parce que, pour lutter contre la cybercriminalité, il faut une approche coordonnée entre les entités fédérales, les gouvernements provinciaux, les administrations municipales et le secteur privé.

Contexte

7.72 Sécurité publique Canada est le ministère responsable des politiques chargé d'élaborer et de mettre en œuvre la Stratégie nationale de cybersécurité. La Stratégie a été lancée en 2018. Au moment de notre audit, elle faisait l'objet d'un renouvellement, et la stratégie renouvelée devait être publiée en 2024.

7.73 Sécurité publique Canada assure la présidence (ou la coprésidence avec le Centre de la sécurité des télécommunications Canada) de divers groupes de travail sur la cybersécurité. Il s'agit notamment des comités de gouvernance des sous-ministres, des sous-ministres adjointes et sous-ministres adjoints et des directrices générales et directeurs généraux ainsi que de divers groupes de travail

interministériels ciblant des enjeux particuliers liés à la cybersécurité. Les membres de ces comités de gouvernance proviennent de diverses organisations fédérales, comme la GRC, mais pas du CRTC.

Les faiblesses de la Stratégie nationale de cybersécurité

Constatations

7.74 Nous avons constaté que le CRTC n'était pas inclus dans la Stratégie nationale de cybersécurité originale ni dans la stratégie faisant l'objet d'un renouvellement au moment de notre audit. Le CRTC était exclu même si, compte tenu de son mandat consistant à veiller à l'application de la *Loi canadienne anti-pourriel*, il pourrait jouer un rôle important dans les cas liés à la cybercriminalité.

7.75 La GRC, le Centre de la sécurité des télécommunications Canada et Sécurité publique Canada ont tous examiné la possibilité de mettre en place un guichet unique où le public canadien pourrait signaler des cybercrimes. Les signalements faits par le public pourraient ensuite être acheminés aux organisations ayant la compétence d'y donner suite. Nous avons cependant constaté que ce guichet unique n'avait pas encore été mis en place. À notre avis, une intervention coordonnée en matière de cybercriminalité comprenant un guichet unique où le public canadien signalerait les cybercrimes pourrait simplifier le processus et éliminer la nécessité pour les Canadiennes et les Canadiens de signaler le même incident à de multiples organisations.

7.76 Dans le cadre des efforts déployés pour mettre en œuvre la nouvelle Stratégie nationale de cybersécurité, diverses options étaient envisagées en ce qui concerne la mise en place d'une main-d'œuvre canadienne spécialisée en cybersécurité. À notre avis, avoir un plan pour réduire les lacunes en matière de ressources humaines dans toutes les organisations responsables est une composante importante d'une stratégie renouvelée.

Recommandation

7.77 Puisque les infractions à la *Loi canadienne anti-pourriel* peuvent être liées aux cybercrimes, Sécurité publique Canada devrait inclure le Conseil de la radiodiffusion et des télécommunications canadiennes dans l'élaboration des initiatives de lutte contre la cybercriminalité du gouvernement du Canada.

Réponse de Sécurité publique Canada — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Recommandation

7.78 Sécurité publique Canada, la GRC, le Centre de la sécurité des télécommunications Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes devraient collaborer pour veiller à ce que les cybercrimes signalés par les particuliers et les entreprises canadiennes soient acheminés à l'organisation dotée du mandat en la matière.

Réponse de chaque entité — *Recommandation acceptée.*

Les réponses détaillées se trouvent dans les **Recommandations et réponses** à la fin du présent rapport.

Conclusion

7.79 Nous avons conclu que la GRC et les entités fédérales sélectionnées n'avaient ni la capacité ni les compétences requises pour appliquer efficacement les lois visant à lutter contre les activités de cybercriminalité afin d'assurer la sécurité et la sûreté de la population canadienne.

À propos de l'audit

Le présent rapport de certification indépendant sur la lutte contre la cybercriminalité a été préparé par le Bureau du vérificateur général du Canada. Notre responsabilité était de donner de l'information, une assurance et des avis objectifs au Parlement en vue de l'aider à examiner soigneusement la gestion que fait le gouvernement des ressources et des programmes et d'exprimer une conclusion quant à la conformité de la GRC et des entités fédérales sélectionnées, dans tous ses aspects importants, aux critères applicables.

Tous les travaux effectués dans le cadre du présent audit ont été réalisés à un niveau d'assurance raisonnable conformément à la Norme canadienne de missions de certification (NCMC) 3001 — Missions d'appréciation directe de Comptables professionnels agréés du Canada (CPA Canada), qui est présentée dans le Manuel de CPA Canada — Certification.

Le Bureau du vérificateur général du Canada (BVG) applique la Norme canadienne de gestion de la qualité (NCGQ) 1, *Gestion de la qualité par les cabinets qui réalisent des audits ou des examens d'états financiers, ou d'autres missions de certification ou de services connexes.* Cette norme exige que le BVG conçoive, mette en place et fasse fonctionner un système de gestion de la qualité qui comprend des politiques ou des procédures conformes aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables.

Lors de la réalisation de nos travaux d'audit, nous avons respecté les règles sur l'indépendance et les autres règles de déontologie définies dans les codes de déontologie pertinents applicables à l'exercice de l'expertise comptable au Canada, qui reposent sur les principes fondamentaux

d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

Conformément à notre processus d'audit habituel, nous avons obtenu ce qui suit de la direction de l'entité :

- la confirmation de sa responsabilité à l'égard de l'objet considéré;
- la confirmation que les critères étaient valables pour la mission;
- la confirmation qu'elle nous a fourni tous les renseignements dont elle a connaissance et qui lui ont été demandés ou qui pourraient avoir une incidence importante sur les constatations ou la conclusion contenues dans le présent rapport;
- la confirmation que les faits présentés dans le rapport sont exacts, sauf en ce qui concerne le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). Ce dernier n'a pas confirmé que les constatations présentées dans le présent rapport sont exactes.

Objectif de l'audit

L'objectif de l'audit consistait à déterminer si la GRC et les entités fédérales sélectionnées avaient la capacité et les compétences requises pour appliquer efficacement les lois visant à lutter contre les activités de cybercriminalité afin d'assurer la sécurité et la sûreté de la population canadienne.

Étendue et méthode

L'audit a porté sur les efforts déployés par la GRC (par l'entremise du Centre national de coordination en cybercriminalité et des équipes d'enquête du Groupe de lutte contre la cybercriminalité de la Police fédérale) ainsi que les efforts déployés par le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications Canada et le CRTC pour lutter contre la cybercriminalité et les infractions connexes qui ont une incidence sur les particuliers, les entreprises et d'autres institutions.

En particulier, nous avons examiné si la GRC avait réussi à acquérir les compétences et les capacités nécessaires pour contrer la menace grandissante de la cybercriminalité qui évolue rapidement, et si elle avait assuré le soutien et la collaboration nécessaires pour aider les forces de l'ordre partout au Canada à répondre à cette menace. Nous avons également examiné les rôles joués par Sécurité publique Canada, le Centre de la sécurité des télécommunications Canada et le CRTC en matière de lutte contre la cybercriminalité dans le cadre de leurs mandats respectifs.

Nous avons examiné les données provenant des systèmes des entités afin de comprendre :

- le volume de cas potentiels de cybercriminalité signalés par les particuliers et les entreprises canadiennes aux entités visées, de façon à évaluer si tous les cas signalés avaient été examinés et transmis aux forces de l'ordre concernées, au besoin;
- le volume de demandes d'assistance présentées par les partenaires nationaux et internationaux d'application de la loi, en vue de prévenir ou de réduire l'incidence des cybercrimes sur les entreprises canadiennes et d'évaluer si ces demandes avaient été correctement gérées dans le cadre d'une mesure d'application de la loi ou d'une assistance offerte aux victimes.

Notre audit a compris un examen des dossiers de cybercrimes pour déterminer si les cas de cybercriminalité relevés avaient été traités en temps opportun et conformément aux normes concernant le délai d'intervention de l'organisation même. Nous avons examiné des dossiers de cybercriminalité gérés par les groupes suivants :

- le Centre national de coordination en cybercriminalité (GRC);
- les équipes d'enquête sur les cybercrimes du Groupe de lutte contre la cybercriminalité de la Police fédérale (GRC);
- le Centre canadien pour la cybersécurité (Centre de la sécurité des télécommunications Canada);
- le Secteur de la conformité et des enquêtes (CRTC).

Dans les cas où un échantillonnage représentatif a été utilisé, la taille de l'échantillon était suffisante pour tirer une conclusion sur la population échantillonnée avec un degré de confiance d'au moins 90 % et une marge d'erreur de tout au plus 10 %. Plus particulièrement :

- pour le Centre national de coordination en cybercriminalité de la GRC, nous avons sélectionné un échantillon représentatif de 46 dossiers d'avis aux victimes sur 384 dossiers clos et un échantillon représentatif de 44 dossiers sur 274 dossiers clos dans lesquels une demande de coordination des dossiers avec des partenaires policiers avait été présentée;
- pour le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications Canada nous avons sélectionné un échantillon de 51 incidents sur les 5 341 incidents qu'il avait gérés.

Dans le cadre de notre audit, nous avons aussi examiné si la GRC avait été en mesure de recruter des personnes ayant les compétences et les connaissances spécialisées requises pour lutter efficacement contre la cybercriminalité. Nous avons interrogé des membres de la GRC responsables de la gestion des ressources humaines des groupes de lutte contre la cybercriminalité. Nous avons passé en revue les politiques de la GRC en matière de ressources humaines et avons analysé les données sur les niveaux de dotation en personnel pour les postes de lutte contre la cybercriminalité.

Nous avons aussi examiné si Sécurité publique Canada avait exercé un leadership à l'échelle fédérale pour coordonner les interventions au moyen de politiques dans le cadre de la lutte contre la cybercriminalité. Nous avons interrogé des responsables au sein de l'entité et avons examiné si et comment Sécurité publique Canada avait coordonné les efforts déployés pour mettre en place la Stratégie nationale de cybersécurité. Nous avons également examiné les efforts déployés par Sécurité publique Canada pour coordonner l'évaluation et le renouvellement de la stratégie.

Nous n'avons pas examiné les secteurs liés à la collecte de renseignements étrangers par le Canada ni les travaux du Centre national contre l'exploitation d'enfants de la GRC.

Critères

Pour tirer une conclusion par rapport à l'objectif de notre audit, nous avons utilisé les critères suivants :

Critères	Sources
Les entités fédérales reçoivent les signalements de cybercrimes et de cybercrimes potentiels, en font le tri et les transmettent aux forces de l'ordre en temps opportun afin de gérer les incidents déclarés d'activités présumées de cybercriminalité.	• Normes de traitement des entités sélectionnées qui sont fondées sur les procédures opérationnelles normalisées • GRC, Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada, 2015 • Centre national de coordination en cybercriminalité de la GRC, Modalités d'accès à titre de service national de police, 2020 • *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*
La Police fédérale de la GRC détermine les incidents de cybercriminalité qui relèvent de son mandat, en établit l'ordre de priorité et y donne suite.	• GRC, Plan stratégique de la Police fédérale de la GRC (2020-2023)
Le Centre national de coordination en cybercriminalité de la GRC fournit des services nationaux de police afin de soutenir les organismes canadiens et internationaux d'application de la loi dans la lutte contre la cybercriminalité.	• Modalités du CNC3, 2020 • *Règlement de la Gendarmerie royale du Canada*, 2014
Le CRTC et le Centre canadien pour la cybersécurité collaborent avec les partenaires d'application de la loi pour appuyer les enquêtes liées à la cybercriminalité.	• Mandat du Centre canadien pour la cybersécurité • Protocole d'entente entre la GRC et le CRTC, 2018 • CRTC, Plan stratégique de la Division de la mise en application du commerce électronique (2020-2022) • *Loi sur le Centre de la sécurité des télécommunications*

Critères	Sources
Le CRTC relève les infractions à la *Loi canadienne anti-pourriel* qui pourraient faciliter la cybercriminalité, en établit l'ordre de priorité et y donne suite.	• *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications* • CRTC, Plan stratégique de la Division de la mise en application du commerce électronique (2020-2022)
Sécurité publique Canada dirige les efforts déployés par les entités fédérales chargées de la sécurité publique visant à établir des priorités stratégiques pour lutter contre la cybercriminalité et à évaluer les progrès par rapport à ces priorités.	• *Loi sur le ministère de la Sécurité publique et de la Protection civile* • Conseil du Trésor, Politique sur la sécurité du gouvernement, 2019 • Sécurité publique Canada, Stratégie nationale de cybersécurité, 2018 • Sécurité publique Canada, Plan d'action national en matière de cybersécurité (2019-2024), 2019

Critères	Sources
Les entités sélectionnées utilisent des renseignements transparents, clairs et utiles pour évaluer et démontrer la mesure dans laquelle elles déterminent les incidents de cybercriminalité et y donnent suite.	• *Loi sur le ministère de la Sécurité publique et de la Protection civile* • *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications* • Modalités du CNC3, 2020 • GRC, Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada, 2015 • *Loi sur le Centre de la sécurité des télécommunications* • *Loi sur la protection des renseignements personnels* • Conseil du Trésor, Politique sur la sécurité du gouvernement, 2019 • *Loi sur la communication d'information ayant trait à la sécurité du Canada* • Sécurité publique Canada, Stratégie nationale de cybersécurité, 2018 • Conseil du Trésor, Politique sur les résultats, 2016 • Secrétariat du Conseil du Trésor du Canada, Guide à l'intention des ministères sur la gestion des initiatives horizontales et l'établissement de rapports connexes, 2018 • Nations Unies, Transformer notre monde : le Programme de développement durable à l'horizon 2030, 2015
Les entités sélectionnées mènent des activités de planification stratégique des ressources humaines pour s'assurer d'avoir les bonnes personnes possédant les bonnes compétences au bon endroit et au bon moment afin de lutter contre la cybercriminalité.	• *Loi sur la gestion des finances publiques* • *Loi sur l'emploi dans la fonction publique* • Bureau du Conseil privé, Guide du sous-ministre, 2017 • Plans, politiques et procédures des entités en matière de ressources humaines

Critères	Sources
Les entités sélectionnées recrutent et maintiennent en poste des personnes diversifiées possédant les compétences et les connaissances nécessaires pour mener et soutenir des enquêtes liées à la cybercriminalité.	• *Loi sur l'emploi dans la fonction publique* • *Loi sur la Gendarmerie royale du Canada* • Conseil du Trésor, Politique sur la gestion des personnes, 2021 • Plans, politiques et procédures des entités en matière de recrutement et de maintien en poste
Les entités sélectionnées tiennent compte de critères liés à la diversité et à l'inclusion dans leurs activités de planification des ressources humaines, de recrutement, d'embauche et de maintien de poste, et atteignent leurs objectifs respectifs.	• *Loi sur l'équité en matière d'emploi* • Conseil du Trésor, Politique sur la gestion des personnes, 2021 • Plans, politiques et procédures des entités en matière de recrutement et de maintien en poste
Les entités sélectionnées font la promotion d'activités de sensibilisation pour informer la population canadienne des risques liés à la cybercriminalité, déterminent le public cible de ces activités et les mettent en œuvre.	• *Loi sur le ministère de la Sécurité publique et de la Protection civile* • Sécurité publique Canada, Stratégie nationale de cybersécurité 2019-2024 : Rapport sur l'examen de mi-parcours • GRC, Stratégie de lutte contre la cybercriminalité de la Gendarmerie royale du Canada, 2015 • GRC, Plan stratégique de la Police fédérale de la GRC (2020-2023) • Modalités du CNC3, 2020 • Innovation, Sciences et Développement économique Canada, Évaluation horizontale de la *Loi canadienne anti-pourriel*, 2018 • Secrétariat du Conseil du Trésor du Canada, Intégration de l'analyse comparative entre les sexes plus dans l'évaluation : un guide d'introduction, 2019 • ONU Femmes, Déclaration et Programme d'action de Beijing, 1995 • Conseil du Trésor, Politique sur les communications et l'image de marque, 2019 • Conseil du Trésor, Politique sur les résultats, 2016

Critères	Sources
Les entités fédérales fournissent des mécanismes axés sur la clientèle pour encourager le signalement public des incidents de cybercriminalité.	• Modalités du CNC3, 2020 • Mandat du Centre canadien pour la cybersécurité • Conseil du Trésor, Politique sur les services et le numérique, 2019 • Conseil du Trésor, Directive sur les services et le numérique, 2020

Période visée par l'audit

L'audit a porté sur la période allant du 1er avril 2020 au 31 mars 2023. Il s'agit de la période à laquelle s'applique la conclusion de l'audit. Toutefois, afin de mieux comprendre l'objet considéré de l'audit, nous avons aussi examiné certains dossiers ultérieurs à cette période.

Date du rapport

Nous avons fini de rassembler les éléments probants suffisants et appropriés à partir desquels nous avons fondé notre conclusion le 24 mai 2024, à Ottawa, au Canada.

Équipe d'audit

L'audit a été réalisé par une équipe multidisciplinaire du Bureau du vérificateur général du Canada (BVG) dirigée par Sami Hannoush, directeur principal. Le directeur principal est responsable de la qualité de l'audit dans son ensemble; il doit s'assurer notamment que les travaux d'audit sont exécutés conformément aux normes professionnelles, aux exigences des textes légaux et réglementaires applicables ainsi qu'aux politiques et au système de gestion de la qualité du BVG.

Recommandations et réponses

Les réponses figurent telles qu'elles ont été reçues par le Bureau du vérificateur général du Canada.

Dans ce tableau, le numéro du paragraphe qui précède la recommandation indique l'emplacement de la recommandation dans le rapport.

Recommandation	Réponse
7.20 Le Centre national de coordination en cybercriminalité de la GRC devrait établir des procédures pour cerner les avis aux victimes les plus urgents et s'assurer qu'ils sont envoyés en premier. Le Centre devrait définir des attentes officielles sur la rapidité avec laquelle les avis aux victimes doivent être envoyés, évaluer le rendement par rapport à ces normes et veiller au respect de celles-ci.	**Réponse de la GRC** — Recommandation acceptée. Bien que la plupart des avis aux victimes hautement prioritaires soient suivis dans les 24 heures, le Centre national de coordination de la cybercriminalité (CNC3) de la GRC établira et officialisera des procédures normalisées pour définir le niveau de priorité pour les avis aux victimes. Le CNC3 appliquera une norme de service officielle et un processus d'établissement des priorités pour les avis aux victimes d'ici septembre 2024. Ce calendrier s'aligne sur la mise en œuvre complète prévue de la Solution nationale en matière de cybercriminalité, qui comprendra de nouvelles capacités pour mesurer systématiquement les activités opérationnelles du CNC3. Les procédures de notification aux victimes du CNC3 continuent d'évoluer depuis sa capacité opérationnelle initiale en 2020. Ces avis sont maintenant un élément essentiel des efforts du CNC3 et des organismes canadiens d'application de la loi visant à réduire les préjudices de la cybercriminalité pour les organisations canadiennes. Les partenaires du CNC3 et des organismes canadiens d'application de la loi ont participé aux opérations internationales d'application de la loi visant à envoyer des avis aux cybervictimes, comme le démantèlement de l'infrastructure de rançongiciel du groupe Hive en 2023. Ces efforts ont permis d'empêcher des paiements relatifs à des rançongiels ou de les atténuer, et contribuent à protéger l'économie du Canada contre les rançongiciels et autres cyberintrusions.

Recommandation	Réponse
7.24 Le Centre national de coordination en cybercriminalité de la GRC devrait veiller à ce que toutes les demandes d'assistance provenant de partenaires nationaux et internationaux soient dûment documentées et achevées, de sorte que toute l'information nécessaire soit transmise dans le cadre de la réponse. Le Centre devrait communiquer les demandes, s'il y a lieu, à toutes les organisations concernées par la demande.	**Réponse de la GRC** — Recommandation acceptée. Le Centre national de coordination contre la cybercriminalité (CNC3) de la GRC veillera à ce que toutes les demandes d'aide reçues des partenaires nationaux et internationaux de l'application de la loi soient entièrement consignées et complétées, et à ce que le CNC3 communique l'information, au besoin, aux organisations concernées. Depuis sa capacité opérationnelle initiale en 2020, le CNC3 a amélioré sa capacité à coordonner et à communiquer l'information avec les partenaires, tout en respectant le consentement de l'auteur et d'autres exigences en matière de communication de renseignements. Le CNC3 demande également à ses partenaires de lui faire part de leurs commentaires sur ses services, notamment dans le cadre de sondages annuels. D'après les résultats des sondages, la plupart des partenaires actifs sont satisfaits ou très satisfaits des services du CNC3. D'ici septembre 2024 et après la mise en œuvre intégrale de la Solution nationale en matière de cybercriminalité (SNC), le CNC3 sera mieux outillé pour répondre pleinement aux besoins de ses partenaires nationaux et internationaux de l'application de la loi, notamment grâce à des capacités de suivi des audits plus complètes pour donner suite aux demandes opérationnelles et à des capacités de communication d'informations renforcées.
7.30 La Police fédérale de la GRC devrait adopter un processus de triage uniforme géré de manière centralisée de sorte que les ressources spécialisées dans les enquêtes sur la cybercriminalité soient affectées aux enquêtes sur les cybercrimes les plus graves.	**Réponse de la GRC** — Recommandation acceptée. La GRC reconnaît qu'il faut redoubler d'efforts à cette fin. L'équipe de la Police fédérale chargée de la Cybercriminalité (EC) a commencé la mise en œuvre d'un processus de surveillance du respect de l'utilisation de l'Outil de triage des incidents (OTI) pour tous les nouveaux dossiers. L'OTI, lancé dans l'ensemble de la Police fédérale en 2020, est conçu pour guider les enquêteurs au fil d'un processus d'évaluation normalisé et complet, tout en repérant les obstacles possibles tels que le manque de ressources ou d'expertise. Un processus de surveillance structuré au sein des secteurs de programme permettra de veiller à la conformité et à ce que les ressources soient concentrées sur les enquêtes les plus importantes, tout en recueillant des données clés pour éclairer la prise de décision et la responsabilisation. En outre, l'EC a élaboré un plan d'action qui sera mis en œuvre par les équipes d'enquête sur la cybercriminalité partout au Canada afin de garantir le respect du mandat de la Police fédérale. Elle est convaincue qu'avec un mandat clair, un modèle de gouvernance défini et une meilleure coordination des activités de ces équipes, les résultats correspondront au mandat de la Police fédérale et se concentreront sur les menaces les plus graves.

Recommandation	Réponse
7.31 La GRC devrait s'assurer que ses systèmes de gestion de l'information recueillent des données exactes et complètes qui permettent d'évaluer le rendement, d'améliorer la prise de décisions et de démontrer l'optimisation des ressources en ce qui concerne les travaux effectués par le Groupe de lutte contre la cybercriminalité de la Police fédérale.	**Réponse de la GRC** — Recommandation acceptée. La Police fédérale de la GRC s'engage à collaborer avec le centre de décision chargé du Système de gestion des dossiers opérationnels (SGDO) de la GRC, connu sous le nom de Système d'incidents et de rapports de police, afin d'élaborer des façons d'accroître l'exactitude et l'exhaustivité des données concernant les enquêtes en matière de cybercriminalité. Elle a également débuté à discuter avec le centre de décision afin d'explorer des façons d'améliorer les rapports au sein du SGDO. Le délai de mise en œuvre des solutions choisies dépendra de leur complexité. En plus des efforts visant à améliorer les données du SGDO, la Police fédérale continuera d'élaborer des façons d'améliorer les rapports opérationnels complets, tout en augmentant la précision des données. Plus précisément, on prévoit lancer un nouveau rapport sur l'évolution de l'enquête qui devrait améliorer l'exhaustivité des données opérationnelles en donnant un accès aux données à toutes les étapes d'une enquête, augmentant ainsi la responsabilisation et permettant la prise de décisions fondées sur des données probantes au moyen de données à jour, exactes et complètes. Le nouveau rapport sera mis à l'essai à compter de l'été 2024 et devrait être déployé dans l'ensemble de la Police fédérale à l'hiver 2024. De plus, la Police fédérale s'engage à collaborer avec le centre de décision pour le Système d'information sur la gestion des ressources humaines de la GRC, les systèmes de rapport financiers (TEAM) et le SGDO afin de développer des indicateurs qui démontreront le rapport qualité-prix (retour sur les investissements), mettre en place des méthodologies standardisées et d'identifier les capacités actuelles et les limites reliées à ces indicateurs.
7.50 Le Conseil de la radiodiffusion et des télécommunications canadiennes devrait s'assurer d'avoir des politiques et des procédures claires décrivant quand et dans quelles circonstances les renseignements qu'il acquiert doivent être communiqués aux forces de l'ordre.	**Conseil de la radiodiffusion et des télécommunications canadiennes** — Recommandation acceptée. Le CRTC, ainsi que le Bureau de la concurrence et le Commissariat à la protection de la vie privée, est responsable du régime réglementaire civil qui promeut et veille au respect de la *Loi canadienne anti-pourriel* (LCAP). La divulgation de renseignements par les organismes de règlementation civile aux organismes chargés de l'application de la loi pénale est soumise à des contraintes juridiques et de protection de la vie privée bien définies.

Recommandation	Réponse
	Le CRTC examinera ses procédures pour s'assurer qu'elles indiquent clairement dans quels cas le CRTC peut passer outre les mesures de protection de la vie privée et de divulguer des renseignements à des organismes chargés de l'application de la loi tout en respectant les lois pertinentes. L'examen des procédures se terminera d'ici la fin de l'exercice financier 2024-2025. Le CRTC s'engage aussi à collaborer avec ses partenaires en lien à la LCAP pour clairement : 1. informer la population canadienne que seules les plaintes relatives aux courriels et aux messages textes non sollicités devraient être déposées au Centre de notification des pourriels; 2. demander à la population canadienne de toujours signaler toute activité criminelle présumée à l'organisme chargé de l'application de la loi approprié; 3. avertir la population canadienne, au moyen de l'énoncé de confidentialité, que ses renseignements peuvent être divulgués aux organismes chargés de l'application de la loi dans des circonstances bien précises.
7.51 Le Conseil de la radiodiffusion et des télécommunications canadiennes devrait s'assurer que les rôles et responsabilités des personnes responsables de l'application de la loi soient conformes aux exigences de la loi. En outre, il devrait veiller à ce que seules les « personnes désignées » aux termes de la *Loi canadienne anti-pourriel* prennent les décisions clés dans le cadre de leur rôle consistant à faire appliquer la loi.	**Conseil de la radiodiffusion et des télécommunications canadiennes** — Recommandation acceptée. En 2023, le CRTC a conçu et mis en place un protocole détaillé qui clarifie les rôles et les responsabilités des personnes chargées d'enquêter sur le respect de la LCAP. Le CRTC a également fait appel à un expert externe pour donner une formation obligatoire aux employés au cours de l'exercice 2024-2025. Le CRTC continuera à veiller à ce que les rôles et les responsabilités des personnes chargées d'enquêter sur le respect de la LCAP respectent les exigences de la loi et à ce que seules les « personnes désignées » prennent les décisions clés.

Recommandation	Réponse
7.58 La GRC devrait améliorer ses systèmes et pratiques de gestion de l'information afin d'associer systématiquement les signalements reçus par le Centre antifraude du Canada aux mesures prises. La GRC pourra ainsi suivre les progrès réalisés par rapport aux cas hautement prioritaires et de cerner les approches efficaces utilisées.	**Réponse de la GRC** — Recommandation acceptée. Le Centre antifraude du Canada (CAFC) de la GRC veillera à effectuer le suivi et à rendre compte de toutes les mesures prises pour lutter contre les fraudes et les cybercrimes qui lui sont signalés. Le signalement des cybercrimes et des fraudes est essentiel pour les organismes d'application de la loi, car il leur permet d'orienter les mesures de lutte contre ces types de crimes prolifiques et graves. Sur le plan national, les mesures d'application de la loi comprennent l'identification de nouvelles menaces de cybercriminalité, les renvois à la police locale, la collaboration avec les partenaires de l'industrie pour perturber les menaces et adopter des tactiques de prévention pour réduire la victimisation, entre autres objectifs. Lorsqu'il est possible d'agir, le CAFC mène des activités de suivi pour les signalements prioritaires de victimes. Le CAFC reconnaît que de nouvelles capacités techniques sont nécessaires pour améliorer le suivi systématique des signalements de victimes. En 2024, le CAFC et le CNC3 mettront en œuvre un nouveau système national de signalement des incidents de cybercriminalité et de fraude qui améliorera le signalement des victimes à l'échelle nationale à des fins d'application de la loi. Le système de signalement en ligne comprend de nouvelles capacités techniques permettant au CAFC de relier systématiquement les signalements de victimes aux activités de suivi.

Recommandation	Réponse
7.64 La GRC devrait mener une analyse pour comprendre ses difficultés à recruter et à maintenir en poste du personnel pour les postes spécialisés en cybercriminalité. Elle devrait ensuite se servir des résultats de cette analyse pour orienter ses futurs efforts de recrutement et de maintien en poste en vue d'accroître sa capacité de lutte contre la cybercriminalité.	**Réponse de la GRC** — Recommandation acceptée. La Police fédérale a élaboré une stratégie de recrutement et de développement de l'expertise en cybersécurité. La GRC s'attaquera également aux défis liés au recrutement et à la rétention des employées dans le cadre des efforts futurs visant à améliorer la capacité de lutte contre la cybercriminalité au cours des deux ou trois prochaines années, notamment, dans le cadre d'initiatives de modernisation plus vastes, des gains d'efficacité dans le processus de sélection pour le Programme des enquêteurs criminels civils ainsi qu'en explorant comment des initiatives comme le Programme des policiers expérimentés peuvent aider à relever ces défis. Malgré la pénurie de cybercompétences, la GRC continue de recruter des personnes spécialisées, notamment au moyen du programme des enquêteurs criminels civils et des stages pour étudiants COOP afin d'attirer de nouveaux talents. La formation est un autre outil stratégique. Le Programme de formation de la Police fédérale fournit un guide pour tous les enquêteurs, y compris ceux du domaine de la cybercriminalité, qui a été diffusé à l'échelle nationale en janvier 2024. Il tire également parti d'autres formations offertes par des partenaires externes et le Collège canadien de police de la GRC. Le CNC3 a lancé le Portail de cyberapprentissage qui fournit des ressources aux employés de la GRC à l'appui des enquêtes liées à la cybercriminalité.
7.69 La GRC devrait veiller à régler les problèmes associés à la mise en adéquation des fonctionnalités de la Solution nationale en matière de cybercriminalité avec les besoins des utilisatrices et des utilisateurs afin que le projet respecte l'ensemble des exigences énoncées. Elle devrait aussi mettre en œuvre des réponses efficaces aux risques et des plans d'urgence pour que le projet soit réalisé dans le respect du budget et du calendrier révisé.	**Réponse de la GRC** — Recommandation acceptée. La GRC veillera à ce que les difficultés liées à la Solution nationale en matière de cybercriminalité soient atténuées et à ce que les besoins des utilisateurs correspondent aux exigences du système d'ici mars 2025. La Solution est une importante initiative technologique qui permettra à la GRC et à la communauté canadienne de l'application de la loi de disposer de capacités nouvelles pour appuyer les enquêtes entre plusieurs administrations sur la cybercriminalité. La Solution nationale en matière de cybercriminalité, lancée au début de la pandémie de COVID-19, est une initiative complexe qui comprend de nouvelles approches en matière d'approvisionnement et de système pour la GRC.

Recommandation	Réponse
	La mise en œuvre de la nouvelle Solution connaît des difficultés et des retards. Pour atténuer les risques, la GRC a demandé un examen indépendant de celle-ci. Bien que l'examen ait cité la Solution comme une initiative phare avec de bonnes pratiques, elle contenait des recommandations sur les contraintes en matière de ressources, l'assurance de la prestation des systèmes, les besoins des utilisateurs et les activités de transfert des connaissances. La GRC mettra en œuvre ces recommandations afin d'atténuer les risques liés à la mise en œuvre continue de la Solution nationale en matière de cybercriminalité et continuera de travailler en collaboration avec les partenaires pour s'assurer que la Solution répond aux besoins des partenaires et qu'elle s'harmonise avec les politiques du gouvernement du Canada en matière de services numériques axés sur l'utilisateur, et ce, dès maintenant et jusqu'au 31 mars 2025.
7.77 Puisque les infractions à la *Loi canadienne anti-pourriel* peuvent être liées aux cybercrimes, Sécurité publique Canada, devrait inclure le Conseil de la radiodiffusion et des télécommunications canadiennes dans l'élaboration des initiatives de lutte contre la cybercriminalité du gouvernement du Canada.	**Sécurité publique Canada** — Recommandation acceptée. Le Ministère consulte de manière exhaustive les ministères et organismes pertinents dans le cadre de ses processus réguliers d'élaboration de politiques. Sécurité publique Canada étudiera de plus amples possibilités d'inclure le Conseil de la radiodiffusion et des télécommunications canadiennes dans les processus d'élaboration de politiques. Il convient de noter que bien qu'il s'agisse d'un organisme de réglementation, on peut tirer profit de certaines procédures pour permettre sa participation aux discussions confidentielles du Cabinet. En ce qui a trait à la nouvelle Stratégie nationale de cybersécurité, Sécurité publique Canada prend les mesures nécessaires pour assurer une approche pangouvernementale qui tient aussi compte des opinions et des besoins de tous les Canadiens. Pendant l'été 2022, Sécurité publique Canada a mené une consultation publique dans le but de donner aux Canadiens l'occasion de préciser sur quoi ils aimeraient que le gouvernement du Canada se concentre au cours de l'élaboration de la nouvelle Stratégie. Comme le Ministère continue de mettre la dernière main à la Stratégie, il continuera de tenir de vastes consultations, notamment avec le Conseil de la radiodiffusion et des télécommunications canadiennes, dans la mesure du possible.

Recommandation	Réponse
7.78 Sécurité publique Canada, la GRC, le Centre de la sécurité des télécommunications Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes devraient collaborer pour veiller à ce que les cybercrimes signalés par les particuliers et les entreprises canadiennes soient acheminés à l'organisation dotée du mandat en la matière.	**Sécurité publique Canada** — Recommandation acceptée. À titre de responsable gouvernemental de la politique de cybersécurité, Sécurité publique Canada collabore étroitement avec les ministères et organismes pour promouvoir la coordination et pour veiller à ce que l'information soit communiquée efficacement et en temps opportun aux ministères et aux organismes requis. L'information est communiquée à tous les niveaux à l'aide de divers mécanismes, comme des réunions régulières de comités auxquelles assistent des représentants du milieu élargie de la cybersécurité. **Réponse de la GRC** — Recommandation acceptée. La GRC continuera de travailler avec ses partenaires fédéraux pour s'assurer que les cybercrimes signalés sont acheminés vers les organismes fédéraux appropriés. Elle reconnaît que les signalements des victimes sont essentiels pour lutter contre la cybercriminalité et que de nombreux incidents ne sont pas signalés aux autorités policières. La GRC continue de mener des activités de sensibilisation auprès d'organismes du secteur privé, de groupes vulnérables et d'autres communautés afin d'améliorer le signalement et d'encourager le rôle des organismes d'application de la loi dans les plans d'intervention en cas d'incidents cybernétiques. La mise en œuvre du nouveau Système national de signalement des incidents de cybercriminalité et de fraude en 2024 permettra également aux victimes de signaler plus facilement les incidents aux organisations d'application de la loi sur le plan national. La GRC reconnaît également qu'il faut redoubler d'efforts pour harmoniser les activités opérationnelles dans la collectivité fédérale en matière d'intervention en cas de cyberincident, ainsi que pour trouver des façons de simplifier et de rationaliser la manière dont les organisations qui représentent les victimes et les particuliers signalent les incidents et reçoivent le soutien de la GRC et de ses partenaires fédéraux. La GRC continuera de travailler en étroite collaboration avec ses partenaires fédéraux en vue d'améliorer les services de signalement et d'intervention offerts aux victimes de cybercriminalité.

Recommandation	Réponse
	Réponse du Centre de la sécurité des télécommunications du Canada — Recommandation acceptée. Le CST est d'accord avec cette recommandation et propose les plans d'action de la direction suivants : • Le directeur général, Politiques stratégiques, en collaboration avec Sécurité publique, la Gendarmerie royale du Canada (GRC) et le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) actualisera le cadre de politique existant sur la cybercriminalité afin d'établir des méthodes cohérentes et sécuritaires de transmission d'informations sur les victimes entre entités (achèvement prévu le 1er avril 2025). • Le dirigeant principal du Centre canadien pour la cybersécurité, en collaboration avec Sécurité publique, la GRC et le CRTC créera une application (guichet unique) permettant de sécuriser la transmission d'informations sur les victimes de façon conforme à la politique susmentionnée (achèvement prévu le 1ier avril 2026). **Réponse du Conseil de la radiodiffusion et des télécommunications canadiennes** — Recommandation acceptée. Le CRTC, ainsi que le Bureau de la concurrence et le Commissariat à la protection de la vie privée, est responsable du régime réglementaire civil qui promeut et veille au respect de la *Loi canadienne anti-pourriel* (LCAP). Le CRTC n'a pas le pouvoir d'enquêter sur la cybercriminalité. Il n'a ni le mandat ni la capacité d'évaluer si les plaintes donnent lieu à un comportement de nature criminelle. Le CRTC s'engage à collaborer avec ses partenaires pour clairement : 1. informer la population canadienne que seules les plaintes relatives aux courriels et aux messages textes non sollicités devraient être déposées au Centre de notification des pourriels; 2. demander à la population canadienne de toujours signaler toute activité criminelle présumée à l'organisme chargé de l'application de la loi approprié; et, 3. avertir la population canadienne, au moyen de l'énoncé de confidentialité, que ses renseignements peuvent être divulgués aux organismes chargés de l'application de la loi dans des circonstances bien précises.