Public Safety Canada | Sécurité publique Canada

Sécurité publique Canada

Évaluation horizontale de la Stratégie de cybersécurité du Canada

Rapport Final

29-09-2017

TABLE DES MATIÈRES

SOMMAIRE

Le programme

La Stratégie de cybersécurité du Canada a été publiée le 3 octobre 2010. Elle énonce le plan prévu par le gouvernement fédéral pour sécuriser les systèmes de cybersécurité du Canada et protéger les Canadiens en ligne. La stratégie repose sur trois piliers : protéger les systèmes du gouvernement du Canada; nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement du Canada; aider les Canadiens à se protéger en ligne. Le premier pilier consiste à mettre en place les structures, les outils et le personnel nécessaires pour renforcer la capacité du gouvernement à prévenir et à détecter les cybermenaces, à intervenir et à se rétablir après coup. Le deuxième pilier consiste à travailler avec les gouvernements provinciaux et territoriaux ainsi qu'avec le secteur privé pour favoriser les initiatives visant à renforcer la cyberrésilience du Canada, y compris celle des secteurs des infrastructures essentielles. Quant au troisième pilier, il consiste à conscientiser les Canadiens et à les sensibiliser à se protéger, eux, ainsi que les membres de leur famille, dans leurs activités en ligne. En outre, ces piliers ont pour but d'accroître la capacité des organismes d'application de la loi de lutter contre la cybercriminalité. La Stratégie est mise en œuvre par neuf organisations du gouvernement du Canada, et l'ensemble des fonds permanents accordés à tous les partenaires s'élève à un peu plus de 60 millions de dollars par année.

Pourquoi c'est important

Les Canadiens utilisent de plus en plus le cyberespace, et l'économie canadienne repose fortement sur Internet. Bien que les Canadiens en tirent énormément d'avantages et de possibilités, le cyberespace peut les exposer à des menaces. Par conséquent, il est important pour le Canada et les Canadiens de prévoir les nouvelles menaces découlant des cyberactivités et de les contrer. Les activités prévues dans le cadre de la Stratégie de cybersécurité du Canada visent à veiller à ce que les Canadiens profitent au maximum des avantages qu'offrent le cyberespace et les cybertechnologies tout en atténuant les risques connexes.

Ce que nous avons examiné

L'évaluation a été réalisée afin de répondre aux exigences de la *Loi sur la gestion des finances publiques* et de la *Politique sur les résultats de 2016* du Conseil du Trésor du Canada. Elle visait à déterminer dans quelle mesure la structure de gouvernance horizontale a supervisé efficacement la mise en œuvre de la Stratégie; dans quelle mesure les ministères et organismes participants ont mis en œuvre les activités financées dans le cadre de la Stratégie; et dans quelle mesure les activités prévues ont contribué à l'atteinte les objectifs principaux de la Stratégie.

Ce que nous avons constaté

Gouvernance

Il a été déterminé que même si la structure de gouvernance a facilité la collaboration, la coordination et l'échange de renseignements entre les organisations participantes. Cependant, l'absence de documentation n'a pas permis à l'évaluation de déterminer dans quelle mesure les

comités de surveillance ont rempli leurs objectifs tel qu'indiqués dans leur mandat. Par exemple, conformément à leurs mandats, les comités de surveillance, en particulier le Comité des sous-ministres, devaient se réunir sur une base régulière pour fournir du conseil stratégique et surveiller les progrès dans la mise en œuvre de la stratégie. L'évaluation n'a pu déterminer, dans quelle mesure ces rôles et responsabilités ont été assumées étant donné que les comptes rendus de réunions et les décisions n'ont pas été produits de façon constante.

L'évaluation a aussi conclue que l'échange de renseignements ne s'est fait que de façon ponctuellement ou sélective, et aucune politique claire n'a été établie quant à la nature des renseignements devant être communiqués, ni avec qui et quand. À l'heure actuelle, il n'existe aucun mécanisme efficace pour l'échange de renseignements classifiés, plus particulièrement en temps réel.

La Stratégie a contribué à préciser les rôles et les responsabilités des organisations du gouvernement du Canada grâce à la mise en place d'un cadre de gestion qui définit mieux les objectifs, attribue les rôles et les responsabilités et établit divers comités et groupes de travail. Toutefois, selon l'évaluation, il y avait dans certains cas une impression de chevauchement des rôles et des responsabilités qui a causé de la confusion et de la frustration chez les ministères et organismes fédéraux et les intervenants du secteur privé.

Rendement - Mise en œuvre

L'évaluation a permis de constater que la plupart des activités financées dans le cadre de la Stratégie ont été mises en œuvre comme prévu. Cependant, au moins quatre activités n'ont pas été mises en œuvre en totalité : l'activité de Recherche et développement pour la défense Canada (une agence du ministère de la Défense nationale) qui consistait à élaborer une architecture d'entreprise et ses produits livrables connexes; l'activité de la GRC visant à publier un rapport annuel sur la cybercriminalité; l'activité de Services partagés Canada visant à sécuriser une troisième connexion Internet; ainsi que l'activité de Services partagés Canada visant à établir un système de rappel sur l'infrastructure de cybersécurité.

Certaines des organisations participantes se sont heurtées à des difficultés quant à la communication de renseignements pertinents sur le rendement, ce qui peut donner à penser que ces renseignements n'ont pas été recueillis de façon régulière et constante. Trois organisations ont signalé ne pas avoir dépensé tous les fonds accordés, deux organisations ont dépensé plus, deux ont dépensé le montant exact et une organisation n'a pas été en mesure de faire le suivi des dépenses pertinentes. Comme les comités de surveillance n'ont pas rédigé de comptes rendus de réunion ni des décisions de façon constante, l'évaluation n'a pu déterminer dans quelle mesure les comités de surveillance, en particulier celui des sous-ministres, ont été tenus informés de ces retards dans la mise en œuvre afin qu'ils puissent remplir leurs objectifs établis en matière de surveillance des progrès dans la mise en œuvre de la stratégie.

Rendement – Efficacité

L'évaluation a permis de constater que la Stratégie a contribué à renforcer la capacité du gouvernement du Canada à prévenir et à détecter les cyberattaques et d'intervenir et de se rétablir après coup. Plus particulièrement, la Stratégie a aidé à améliorer l'aptitude des

organisations gouvernementales à analyser rapidement les atteintes à la protection des données et à les contenir. Bien que des cyberincidents et des intrusions surviennent encore, ils sont de moins en moins fréquents. Ces améliorations ont été remarquées, malgré une hausse des cyberattaques étatiques et non étatiques qui ont été lancées contre les réseaux du gouvernement du Canada au cours des dernières années. Néanmoins, les personnes rencontrées ont indiqué qu'il existe d'autres possibilités d'amélioration.

Toujours d'après l'évaluation, la Stratégie a aussi contribué à favoriser l'établissement de partenariats avec les propriétaires et les exploitants d'infrastructures essentielles, ainsi qu'avec d'autres intervenants du secteur privé. Toutefois, les personnes rencontrées et les documents consultés laissent entendre que, dans l'ensemble, les progrès dans l'établissement de partenariats visant à sécuriser les cybersystèmes essentiels à l'extérieur du gouvernement du Canada ont été limités. En particulier, l'investissement global dans le cadre de la Stratégie au chapitre de la protection des cybersystèmes importants pour le Canada a été jugé inadéquat. Des progrès timides ont été réalisés en ce qui a trait à l'établissement de normes réciproques pour l'échange de renseignements avec le secteur privé, les provinces et les territoires.

Enfin, la majorité des personnes rencontrées croient que les Canadiens sont maintenant plus conscients des cybermenaces qu'auparavant. Toutefois, on ignore si cette conscience accrue est attribuable à la Stratégie et si elle a amélioré la sécurité des Canadiens en ligne.

Étant donné ces constatations, l'évaluation a permis de relever un certain nombre de possibilités d'amélioration et de formuler plusieurs recommandations pour y donner suite. À titre d'organisation responsable, le ministère de la Sécurité publique s'est engagé à remédier aux lacunes en collaboration avec les organisations partenaires dans le cadre du renouvellement de la Stratégie de cybersécurité du Canada afin de mieux préparer le Canada à améliorer sa situation du point de vue national, économique et de la cybersécurité.

Recommandations

En collaboration avec les organisations participantes, la sous-ministre adjointe principale du Secteur de la sécurité et de la cybersécurité nationale de Sécurité publique Canada devrait envisager de prendre les mesures suivantes :

1) Renforcer la structure de gouvernance horizontale de la Stratégie de cybersécurité du Canada en procédant aux tâches suivantes :
    a. réévaluer la structure de gouvernance pour déterminer la nécessité et la demande en ce qui a trait à la configuration actuelle des comités et pour améliorer la participation;
    b. améliorer le soutien du secrétariat, notamment la coordination, la gestion de l'information et d'autres services administratifs;
    c. s'assurer que les comités de surveillance ont des mandats qui définissent clairement les rôles et les responsabilités des membres et les attentes envers ceux-ci;

d. s’assurer que les comités de surveillance s’acquittent des rôles et des responsabilités définis dans leur mandat; et
e. rédiger des comptes rendus de réunions de façon systématique.

2) Renforcer les pratiques d’échange de renseignements liés à la cybersécurité en élaborant des politiques et des procédures et concevoir des outils qui permettront un échange de renseignements systématique et opportun avec les partenaires et les intervenants.

3) Renforcer les pratiques de mesure du rendement et de collecte de données en procédant aux tâches suivantes :
   a. recueillir des renseignements pertinents, fiables et axés sur les résultats, y compris des renseignements sur les dépenses de programme, de façon régulière et méthodique; et
   b. fournir les renseignements recueillis sur le rendement et les dépenses aux comités de surveillance pertinents de façon régulière pour favoriser un suivi efficace et la reddition de comptes.

Réponse et plan d’action de la direction

La direction accepte toutes les recommandations et mettra en œuvre un plan d’action.

1. INTRODUCTION

Le présent rapport fait état des constatations de l'évaluation horizontale de la Stratégie de cybersécurité du Canada (Stratégie) effectuée par Sécurité publique Canada.

L'évaluation a été menée afin de fournir aux Canadiens, aux parlementaires, aux ministres, aux organismes centraux et aux sous-ministres des organismes participants une appréciation neutre et fondée sur les faits de la gouvernance, de la mise en œuvre et du rendement de la Stratégie. Elle a été réalisée en conformité avec la *Politique sur les résultats de 2016* du Conseil du Trésor.

Il convient de mentionner qu'à la demande du premier ministre, le ministre de la Sécurité publique a pour mandat, en collaboration avec ses homologues des ministères de la Défense nationale, de l'Infrastructure et des Collectivités, des Services publics et de l'Approvisionnement, de l'Innovation, des Sciences et du Développement économique ainsi que du Secrétariat du Conseil du Trésor, d'effectuer un examen des mesures existantes visant à protéger les Canadiens et les infrastructures essentielles contre les cybermenaces. Les constatations de l'évaluation visent à servir de complément à ce processus et à orienter les futurs efforts de renouvellement des politiques liées à la cybersécurité du gouvernement du Canada.

Publiée le 3 octobre 2010, la Stratégie décrit la réponse du gouvernement du Canada au besoin croissant de sécuriser les cybersystèmes du Canada et de protéger les Canadiens en ligne[1]. À cette fin, la Stratégie a énoncé le plan du gouvernement du Canada pour sécuriser ses cybersystèmes ainsi que sa vision en ce qui concerne l'établissement de partenariats avec les provinces et les territoires, le secteur privé (y compris les propriétaires et exploitants d'infrastructures essentielles), les universités, les alliés internationaux et les Canadiens afin de faire face aux menaces liées à la cybersécurité au pays.

La Stratégie repose sur trois piliers :

- Protéger les systèmes du gouvernement du Canada – vise à renforcer la capacité du gouvernement du Canada à prévenir et à détecter les cybermenaces, à intervenir le cas échéant et à se rétablir après coup;

- Nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement du Canada – vise à renforcer la cyberrésilience au Canada, notamment celle des secteurs des infrastructures essentielles;

- Aider les Canadiens à se protéger en ligne – vise à promouvoir la sensibilisation du public, à renseigner les Canadiens sur les moyens de se protéger et à renforcer la capacité des organismes d'application de la loi à lutter contre la cybercriminalité.

[1] La cybersécurité est définie comme la protection de l'information numérique et de l'infrastructure sur laquelle elle repose contre l'accès, l'utilisation, la manipulation, l'interruption ou la destruction non autorisée par voie électronique (Stratégie de cybersécurité du Canada, page 3).

L'annexe A décrit de façon générale les rôles et les responsabilités des organisations du gouvernement du Canada sous chacun des piliers.

La Stratégie de cybersécurité du Canada vise l'obtention de trois principaux résultats :

- Les systèmes du gouvernement du Canada sont protégés;
- Les systèmes importants pour le gouvernement du Canada sont protégés;
- Les Canadiens sont protégés en ligne.

L'évaluation couvre les activités de neuf organismes du gouvernement du Canada qui étaient impliqués dans la mise en œuvre la Stratégie : Sécurité publique Canada (SP), le Centre de la sécurité des télécommunications Canada (CSTC), Services partagés Canada (SPC), le ministère de la Défense nationale/ Recherche et développement pour la défense Canada (MDN/RDDC), le Secrétariat du Conseil du Trésor du Canada (SCT), Affaires mondiales Canada (AMC), le ministère de la Justice (JUS), la Gendarmerie royale du Canada (GRC) et le Service canadien du renseignement de sécurité (SCRS).

1.1 Gouvernance horizontale et surveillance

Sécurité publique Canada assume un rôle de leadership national et de coordination, notamment en ce qui concerne la mise en œuvre le Stratégie de cybersécurité du Canada y compris l'avancement de la politique nationale de cybersécurité. Sécurité publique Canada supervise la coordination des efforts du gouvernement visant à protéger les infrastructures essentielles du Canada et les Canadiens, et de gérer les urgences touchant la cybersécurité. En collaboration avec ses partenaires de sécurité fédéraux, nationaux et internationaux, Sécurité publique Canada coordonne une approche nationale stratégique intégrée en ce qui concerne la cybersécurité, ainsi que par l'entremise du Centre canadien de réponse aux incidents cybernétiques (CCRIC)[2] et, au besoin, du Centre des opérations du gouvernement (COG), lequel s'inscrit comme la réponse nationale aux incidents cybernétiques d'intérêt national.[3]

Sécurité publique Canada s'appuie sur les comités des sous-ministres (SM), des sous-ministres adjoints (SMA) et des directeurs généraux (DG) sur la cybersécurité pour diriger la mise en œuvre de la Stratégie et régler les problèmes à mesure qu'ils surviennent. Il incombe à ces comités de la haute direction de formuler des conseils stratégiques, au besoin, pour assurer la mise en œuvre rapide et efficace de la Stratégie.

[2] Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) agit comme centre national de coordination du Canada pour la prévention et l'atténuation des incidents cybernétiques, l'intervention s'y rattachant et le rétablissement après coup. À ce titre, il est considéré comme le secteur opérationnel de Sécurité publique Canada.

[3] 2012 document de lancement, page 7, paragraphe 3 and page 37, paragraphe 91.

Tableau 1 : Structure de gouvernance pour la mise en œuvre de la Stratégie de cybersécurité du Canada[4]

<table>
<tr><td colspan="12">Cabinet</td></tr>
<tr><td colspan="12">Comité des sous-ministres sur la cybersécurité (SM responsables de la cybersécurité)</td></tr>
<tr><td colspan="12">Comité des sous-ministres adjoints sur la cybersécurité (SMA responsables de la cybersécurité)</td></tr>
<tr><td colspan="6">Comité des directeurs généraux sur la cybersécurité (DG responsables de la cybersécurité)</td><td colspan="6">Comité des directeurs généraux sur les opérations liées à la cybersécurité (DG responsables des opérations liées à la cybersécurité)</td></tr>
<tr><td colspan="12"></td></tr>
<tr><td>SP</td><td>SCRS</td><td>GRC</td><td>MDN</td><td>CSTC</td><td>MDN/RDDC</td><td>AMC</td><td>JUS</td><td>SPAC[5]</td><td>SPC</td><td>SCT</td><td>BCP[6]</td><td>ISDE[7]</td></tr>
</table>

2. À PROPOS DE L'ÉVALUATION

2.1 Aperçu de l'évaluation

Cette évaluation a été réalisée pour satisfaire aux exigences de la *Loi sur la gestion des finances publiques* et de la *Politique sur les résultats* (2016) du Conseil du Trésor du Canada. Cette démarche consistait surtout à évaluer dans quelle mesure :

- la structure de gouvernance horizontale se révélait efficace dans le cadre de la prestation de la Stratégie, notamment au chapitre de la surveillance exercée et de la clarification des rôles et des responsabilités des différents partenaires;
- les ministères et organismes participants ont mis en œuvre les activités visées par la Stratégie;
- les activités prévues ont contribué à l'atteinte des principaux objectifs de la Stratégie.[8]

L'évaluation a porté sur les activités entreprises entre 2010-2011 et 2015-2016. La collecte des données et les phases d'analyse de l'évaluation ont été réalisées entre mai et septembre 2016.

[4] Il convient de noter que les organismes figurant dans la liste ci-dessus ne sont pas tous membres de tous les comités.

[5] SPAC est chargé, entre autres, du maintien des relations avec les alliés et de la négociation des protocoles d'entente sur les questions relatives à la sécurité industrielle, y compris la cybersécurité, dans le cadre du processus contractuel.

[6] BCP héberge les bureaux du conseiller en matière de sécurité nationale auprès du premier ministre et apporte son soutien à ce dernier. Il est aussi chargé de coordonner les activités du milieu canadien de la sécurité et du renseignement ainsi que de favoriser une approche coordonnée dans le domaine de la sécurité nationale.

[7] ISDE est chargé du maintien d'un système de télécommunications solide et fiable, de l'élaboration de politiques pour assurer un marché en ligne sûr et sécuritaire ainsi que la continuité des télécommunications en cas de situation d'urgence.

[8] Dans le but de minimiser les chevauchements, l'évaluation ne s'est pas attardée à la pertinence de la Stratégie (c.-à-d. le besoin continu, les liens avec les priorités gouvernementales et les résultats stratégiques du Ministère, l'harmonisation avec les rôles et les responsabilités du gouvernement fédéral), car ces questions devraient être traitées dans l'examen sur la cybersécurité susmentionné.

2.2 Méthodologie

L'évaluation a été effectuée au moyen des sources de données suivantes :

Revue de la littérature – comprenant une recherche sur les documents accessibles sur le Web qui sont liés à la cybersécurité en général et à la Stratégie de cybersécurité du Canada en particulier.

Étude de documents – comprenant l'examen des documents initiaux, des rapports de rendement, des données financières et des rapports d'audit récents. Ces rapports incluaient l'édition 2015 de l'*Audit interne horizontal de la sécurité de technologies de l'information dans les grands et les petits ministères* du Bureau du contrôleur général.

Entrevues – incluaient la conduite de 48 entrevues auprès de représentants de onze organismes du gouvernement du Canada, ainsi que d'universitaires et d'autres experts en la matière. Les organismes participants ont déterminé à leur discrétion qui et combien de personnes seraient interrogées.

Tableau 2 : Groupes d'intervenants et nombre d'entrevues

<table>
<tr><th colspan="3">Groupe des personnes interrogées</th><th>Nombre d'entrevues</th></tr>
<tr><td rowspan="10">Ministères et organismes participants</td><td>Organismes</td><td>Ministères et organismes participants</td><td rowspan="10">42</td></tr>
<tr><td>SP</td><td>4</td></tr>
<tr><td>GRC</td><td>6</td></tr>
<tr><td>JUS</td><td>6</td></tr>
<tr><td>MDN</td><td>1</td></tr>
<tr><td>CSTC</td><td>9</td></tr>
<tr><td>SCT</td><td>4</td></tr>
<tr><td>SPC</td><td>4</td></tr>
<tr><td>SCRS</td><td>4</td></tr>
<tr><td>AMC</td><td>4</td></tr>
<tr><td rowspan="2">Autres ministères</td><td>ISDE</td><td>Autres ministères</td><td rowspan="2">2</td></tr>
<tr><td>SPAC</td><td>1</td></tr>
<tr><td colspan="3">Experts en la matière et universitaires externes au gouvernement</td><td>4</td></tr>
<tr><td colspan="3">TOTAL</td><td>48</td></tr>
</table>

Des renseignements financiers et sur le rendement ont été recueillis, passés en revue et analysés afin de suppléer aux renseignements colligés par l'entremise des autres sources de résultats.

2.3 Limitations

D'un partenaire à l'autre, la qualité et l'accessibilité des renseignements sur le rendement variaient. Dans le cas où des renseignements sur le rendement étaient manquants, l'équipe d'évaluation s'est appuyée sur les perceptions des personnes interrogées et l'examen des documents pour suppléer aux données.

Les informations sur les dépenses nous ont été fournies par chacune des organisations participantes. L'évaluation n'a pas permis de vérifier indépendamment la validité des informations fournies.

Nous avons tenté à plusieurs reprises de faire une entrevue avec des représentants du secteur privé. Toutefois, les personnes avec lesquelles nous avons communiqué n'étaient pas en mesure de formuler des commentaires ou n'ont pas répondu à nos demandes d'entrevue.

La portée de l'évaluation s'est limitée à certaines activités menées entre 2010 et 2016. Il convient de noter que de nombreuses autres activités financées et non financées ont été entreprises par les organismes du gouvernement du Canada en appui à la Stratégie. Bien qu'il ait été clairement énoncé que l'évaluation portait uniquement sur la contribution de ces activités particulières, il s'avère impossible de mesurer ou d'isoler la *contribution exacte* d'un groupe d'activités à l'atteinte des objectifs globaux de la Stratégie.

2.4 Questions de l'évaluation

L'annexe B renferme une liste des questions abordées dans le cadre de l'évaluation.

3. CONSTATATIONS DE L'ÉVALUATION

3.1 Gouvernance

Cette section porte sur les questions rattachées à la gouvernance, notamment dans quelle mesure la structure de gouvernance horizontale a-t-elle été efficace? Les rôles et les responsabilités de chaque organisme participant ont-ils été bien définis et respectés? Quel est le niveau d'échange de renseignements, de collaboration et de coordination entre les partenaires? Elle comporte également une brève discussion sur l'état de la recherche et du développement en matière de cybersécurité.

Constatation de l'évaluation : Même si la structure de gouvernance existante a facilité, dans une certaine mesure, la collaboration, la coordination et l'échange de renseignements au sein des organismes participants, l'absence de comptes rendus de réunions, autres documents ou d'employés ayant la mémoire corporative a limité la capacité à évaluer l'efficacité globale de la structure de gouvernance et la mesure dans laquelle les comités de surveillance ont atteint leurs objectifs établis.

3.1.1 Efficacité des comités de gouvernance

La Stratégie reposait sur une structure de gouvernance décentralisée, laquelle s'harmonise à la structure de la plupart des initiatives horizontales du gouvernement du Canada. Dans le cadre de cette structure de gouvernance, quoique Sécurité publique Canada est responsable de coordonner l'ensemble des activités, les organismes participants doivent uniquement rendre compte à leurs propres ministres, qui à leur tour, doivent rendre compte au Parlement.

Bien que certaines personnes interrogées aient soutenu que cette structure renforçait la culture du travail en vase clos, la plupart ont estimé qu'elle se révélait efficace au chapitre de la création de possibilités favorisant une collaboration plus étroite entre les organismes participants.

Sécurité publique Canada devait s'acquitter de sa responsabilité en matière de coordination grâce à une structure de gouvernance qui comprenait différents comités de surveillance, notamment les comités des SM, des SMA et des DG responsables de la cybersécurité, les comités des DG responsables des opérations[9] liées à la cybersécurité, ainsi que les nombreuses communautés de pratique.[10]

Au moins trois comités (Comité des SM responsables de la cybersécurité, Comité des DG responsables de la cybersécurité et Comité des DG responsables des opérations liées à la cybersécurité) ont établi par écrit un cadre de référence. Selon ce cadre, ces comités étaient responsables, entre autres, de « surveiller les progrès liés à la mise en œuvre de la *Stratégie de cybersécurité du Canada*. » Le Comité des SM responsables de la cybersécurité et le Comité des DG responsables de la cybersécurité devaient se réunir tous les deux mois et le Comité des DG responsables des opérations liées à la cybersécurité toutes les deux semaines ou au besoin en réponse aux questions opérationnelles. Toutefois, il semble que seul le Comité des DG responsables des opérations liées à la cybersécurité s'est réuni de manière régulière.

Sur la base de l'information reçue, aucun des comités ne semble avoir établi des comptes rendus de réunions de manière systématique.

La plupart des personnes interrogées ont estimé que le Comité des DG responsables des opérations liées à la cybersécurité s'est révélé efficace et a constitué une bonne tribune pour l'échange de renseignements entre les organismes participants. Néanmoins, certaines d'entre elles ont également fait remarquer que la composition du Comité doit être élargie de façon à inclure d'autres intervenants en cybersécurité du gouvernement du Canada, comme le Secrétariat

[9] Le comité des DG en charge des opérations cybernétiques a été mis en place pour assurer qu'il y eut une coordination dans la lutte contre les menaces cybernétiques et les incidents d'intérêt national et que les questions de politique opérationnelle nationale soient avancées. Il est différent du Comité des DG cybernétique par son orientation opérationnelle. Le Comité était composé des ministères ayant un rôle opérationnel à l'intérieur et / ou à l'extérieur du gouvernement fédéral, y compris, mais sans être limité à : SP, CST, SCRS, MDN, SPC, la GRC et le Conseil de la radiodiffusion et des télécommunications du Canada.

[10] Il convient de noter qu'il existe d'autres piliers propres aux comités de travail ainsi qu'aux cadres supérieurs et aux groupes de travail qui sont établis afin de favoriser la sécurité en matière de TI en général et d'atteindre les objectifs de la *Stratégie de cybersécurité du Canada* en particulier. Toutefois, cette évaluation a porté uniquement sur la structure de gouvernance pangouvernmentale et les comités de gouvernance, comme il est indiqué dans les documents officiels liés à la Stratégie, y compris le cadre de mesure du rendement de la Stratégie.

du conseil du trésor. Certaines préoccupations ont été soulevées quant au fait que le Comité avait perdu de sa robustesse au cours de la dernière année puisque ses membres ont envoyé un nombre accru de délégués aux réunions.

Outre cette structure officielle, différentes communautés de pratique se sont constituées et se sont réunies plus régulièrement que les comités d'origine afin d'échanger des renseignements et de discuter des enjeux. Bien qu'elles soient dynamiques, ces communautés de pratique n'ont pas le pouvoir d'établir une orientation et dépendent largement de personnes en particulier. Par conséquent, les changements de personnel influent sur leurs relations de travail et leur efficacité.

En vertu de son mandat, le comité des sous-ministres devait établir une orientation en matière de politique, établir les priorités en matière de cybersécurité pour les organisations membres et surveiller les progrès relatifs à la mise en œuvre de la stratégie. Cependant, vu l'absence de comptes rendus de réunions, d'autres documents ou d'employés ayant la mémoire corporative, l'évaluation n'a pu déterminer dans quelle mesure le comité a été pu assumer ces responsabilités.

Observations et possibilités d'amélioration

Dans le cadre de l'évaluation, on a établi que le renforcement de la structure de gouvernance représentait une possibilité d'amélioration. À cette fin, la composition de la structure de gouvernance doit être revue et les activités de celle-ci officialisées, notamment celles des comités de surveillance. Cette officialisation pourrait inclure, entre autres :

- améliorer l'offre de services de secrétariat;
- l'établissement, pour chaque comité de surveillance, d'un mandat définissant clairement les rôles et les responsabilités des membres et les attentes envers ceux-ci;
- la réunion régulière des comités conformément à leur mandat;
- la consignation des comptes rendus de réunions de manière régulière.

En outre, étant donné l'évolution de la cybersécurité et son importance accrue pour la prospérité économique du Canada, il importe que les cadres supérieurs se rencontrent régulièrement afin de discuter des enjeux stratégiques en matière de cybersécurité, notamment les aspects internationaux (p. ex. la politique étrangère en matière de cybersécurité).

3.1.2 Clarté des rôles et des responsabilités

Avant l'établissement de la Stratégie, il régnait une confusion quant aux rôles et aux responsabilités des organismes du gouvernement du Canada au chapitre de la cybersécurité.[11] Il n'existait aucun processus ni mécanisme clairs pour l'échange de renseignements, plus particulièrement avec les organismes de sécurité et d'exécution de la loi.

[11] Cet énoncé ne s'applique pas à la GRC, étant donné qu'elle a indiqué que ses rôles, ses responsabilités et ses pouvoirs en matière de cybersécurité ont toujours été clairement établis.

La Stratégie a mis en place un cadre de gestion afin de préciser les objectifs, d'assigner les rôles et les responsabilités et d'établir divers comités et groupes de travail, tels que les comités des SM, des SMA, des DG responsables de la cybersécurité et des DG responsables des opérations de cybersécurité, pour aider les organismes du gouvernement du Canada à échanger de l'information, collaborer et assurer une coordination entre eux.

L'articulation de la Stratégie autour de trois piliers distincts, mais complémentaires, a permis de clarifier les rôles et les responsabilités de tous les partenaires. De surcroît, les rôles et les responsabilités de chaque organisme ont été décrits de manière détaillée dans des documents tels que le *Plan de gestion des événements de cybersécurité du gouvernement du Canada*[12], le *Plan fédéral d'intervention d'urgence* [13] et le *Cadre de gestion des incidents cybernétiques pour le Canada*.[14]

Bien que grâce à la publication de ces documents et des autres efforts déployés, les rôles et les responsabilités des différents acteurs ont été précisés au cours des années, de nombreuses personnes interrogées ont relevé des cas précis où les mandats se chevauchent et les rôles et les responsabilités ne sont pas clairement établis, ce qui génère parfois de la confusion et de la frustration chez les ministères et organismes concernés, ainsi que chez les intervenants du secteur privé. Par exemple :

- Dans certaines situations, deux ou trois organismes gouvernementaux ont assisté à des réunions avec les propriétaires et les exploitants d'infrastructures essentielles et/ou les organismes du secteur privé sans avoir au préalable harmonisé les messages du gouvernement. On a également observé ce manque de coordination au chapitre des messages au sein de Sécurité publique Canada, plus particulièrement entre les groupes de la cybersécurité et des infrastructures essentielles;
- Plusieurs organismes du gouvernement du Canada ont déclaré (et peuvent même déclaré aujourd'hui) qu'ils agissent à titre d'unique personne-ressource auprès du secteur privé en cas d'incident;
- Différentes organisations partenaires ont élaboré des logiciels ou d'autres outils pour s'attaquer à la question de la cybersécurité, sans se rendre compte que d'autres organisations ont conçu ou étaient en voie de concevoir les mêmes logiciels ou outils.

Parmi les personnes interrogées et les intervenants du secteur privé avec lesquels nous avons été en communication, certains sont d'avis que les rôles, les responsabilités et le mandat du Centre canadien de réponse aux incidents cybernétiques (CCRIC) empiètent, dans une certaine mesure, sur ceux du Centre de la sécurité des télécommunications Canada (CSTC).[15,16]

---

[12] https://www.canada.ca/fr/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html.

[13] https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/index-fr.aspx.

[14] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-ncdnt-frmwrk/index-fr.aspx#_Toc360619103.

[15] Le mandat du Centre de la sécurité des télécommunications du Canada consiste à acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement; fournir des avis, des conseils et des services pour aider à protéger les

Par conséquent, les propriétaires et les exploitants d'infrastructures essentielles étaient particulièrement confus à propos des rôles et des responsabilités de ces deux organismes. Cette confusion subsiste malgré les tentatives entreprises au cours des dernières années pour mettre l'accent sur les mandats des deux organismes. En effet, le Centre de la sécurité des télécommunications Canada (CSTC) devait aborder les questions rattachées aux systèmes importants pour le gouvernement du Canada, et le Centre canadien de réponse aux incidents cybernétiques (CCRIC) devait jouer davantage un rôle de coordination au chapitre de l'échange de renseignements et de la gestion des incidents. Plusieurs personnes interrogées ont indiqué que bon nombre de propriétaires et d'exploitants du secteur privé ne savaient pas quel organisme agissait comme point de contact pour les questions de cybersécurité.[17]

Observations et possibilités d'amélioration

Étant donné que le contexte de la cybersécurité a évolué, on doit redéfinir les rôles et les responsabilités des entités gouvernementales, plus particulièrement en ce qui a trait à la détermination d'une unique personne-ressource pour le secteur privé en ce qui concerne tous les cyberincidents.[18]

En outre, étant donné l'importance croissante de la cybersécurité sur l'économie, on doit préciser quels devraient être les rôles, les responsabilités et les niveaux de participation appropriés des ministères au sein du portefeuille économique, notamment Innovation, Sciences et Développement économique Canada (ISDE), au chapitre de la cybersécurité.

---

renseignements électroniques et les infrastructures d'information qui revêtent une importance pour le gouvernement du Canada; de fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère et est l'autorité de la sécurité des communications (COMSEC) pour le Canada ce qui inclut l'audit de la doctrine du COMSEC (https://www.cse-cst.gc.ca/fr/inside-interieur/what-nos).

[16] Cette évaluation ne se penche pas sur la question à savoir si un tel chevauchement existe en fait entre les mandats du Centre canadien de réponse aux incidents cybernétiques (CCRIC) et du Centre de la sécurité des télécommunications Canada.

[17] Un document intitulé *Cadre de gestion des incidents cybernétiques pour le Canada* désigne, dans la plupart des cas, le Centre canadien de réponse aux incidents cybernétiques (CCRIC) comme le premier point de contact du gouvernement du Canada pour un organisme touché. Parallèlement, le document indique aux organismes touchés de communiquer avec les responsables de l'exécution de la loi s'ils croient qu'un acte criminel a été commis ou avec le Service canadien du renseignement de sécurité (SCRS) s'ils estiment que la sécurité nationale est menacée. En cas de doute, les organismes concernés sont priés de communiquer avec le CCRIC. Ces diverses options peuvent en partie expliquer pourquoi certaines personnes interrogées ne savaient pas avec qui les exploitants et les propriétaires d'infrastructures essentielles et les autres organismes du secteur privé devaient communiquer au préalable au sein du gouvernement du Canada dans le cadre d'un incident touchant la sécurité.

En outre, certaines personnes interrogées extérieures au gouvernement du Canada ont mentionné que le secteur privé ne comprenait pas clairement le rôle de Sécurité publique Canada. Selon leur expérience, dans le cas d'un cyberincident, les organismes touchés sont plus susceptibles de se tourner vers la Gendarmerie royale du Canada (GRC) ou le Centre de la sécurité des télécommunications Canada (CSTC) plutôt que vers Sécurité publique Canada, étant donné leur manque relatif de familiarité avec le rôle de cette dernière.

[18] Il convient de noter que les personnes interrogées qui ont soulevé ce point n'ont pas défini ce qu'elles voulaient dire par « cyberincidents ». Par contre, les évaluateurs supposent qu'elles faisaient référence aux incidents pour lesquels il n'y a pas de pratiques ou de protocoles de rapport bien établis.

3.1.3 Degré de coordination et de collaboration

La plupart des personnes interrogées ont indiqué que Sécurité publique Canada était bien placée pour coordonner le dossier de la cybersécurité. Toutefois, l'autorité de Sécurité publique Canada repose seulement sur son pouvoir de persuasion et, dans une certaine mesure, sur le rôle de premier plan qu'elle joue en ce qui concerne les processus de renouvellement des politiques.[19]

Il n'en reste pas moins qu'on croyait que Sécurité publique Canada accomplissait un bon travail en coordonnant les activités inhérentes à la Stratégie, plus particulièrement sur le plan opérationnel. Toutefois, plusieurs personnes interrogées ont observé un décalage entre les aspects liés aux opérations et aux politiques. Ainsi, certains des organismes qui intervenaient uniquement sur le plan des politiques ont soutenu qu'ils ignoraient souvent les progrès accomplis relativement aux opérations.

Par conséquent, ce décalage a donné lieu à la création de deux structures parallèles, une s'articulant autour des politiques et l'autre autour des questions opérationnelles. On a soutenu que cette scission avait miné l'horizontalité de la Stratégie. Certains ministères et organismes qui intervenaient uniquement sur le plan des politiques ont indiqué qu'en raison de leurs mandats, ils devaient également participer aux opérations. Inversement, les autres qui prenaient part uniquement aux opérations estimaient qu'ils n'avaient pas été informés à propos des progrès réalisés au chapitre des politiques.

Dans le cadre de la Stratégie, les provinces et les territoires sont considérés comme des partenaires importants en ce qui touche la protection du cyberespace pour les Canadiens. À cette fin, une table ronde fédéral-provincial-territorial des sous-ministres sur la cybersécurité a été mis sur pied pour aider le gouvernement du Canada à collaborer avec les provinces et les territoires et à échanger des renseignements avec ceux-ci. Toutefois, les résultats escomptés se sont révélés non concluants. Pour différentes raisons, il s'est avéré difficile de tenir des discussions sur les politiques parmi les intervenants et de s'entendre sur la façon de procéder en ce qui concerne des enjeux donnés, notamment l'échange de renseignements. Dans la pratique, les participants ont constaté qu'échanger des renseignements classifiés comportait d'énormes limites, que de déclassifier des renseignements se révélait difficile et qu'établir des systèmes efficients permettant l'échange de renseignements nécessitait des investissements autant de la part des bénéficiaires que du gouvernement du Canada.

Selon certaines des personnes interrogées, la création de Services partagés Canada, qui regroupe les infrastructures en matière de technologies de l'information (TI) au sein du gouvernement du Canada, a permis de faciliter davantage la collaboration parmi les organismes du gouvernement du Canada en ce qui touche la cybersécurité.[20]

---

[19] Selon le Cadre de mesure du rendement de la Stratégie, l'absence de pouvoir central constitue l'un des risques susceptibles de nuire à la mise en œuvre et à la réussite de la Stratégie (page 19).

[20] Le gouvernement du Canada a créé Services partagés Canada (SPC) le 4 août 2011 afin de transformer la manière dont le gouvernement gère son infrastructure de TI. SPC a le mandat de fournir les services de courriels, de centres de données et de télécommunications ainsi que tous les services liés à la cybersécurité et à la sécurité des TI à 43 ministères et organismes

3.1.4 Facilitateurs et obstacles liés à l'échange de renseignements

Au cours des années, on a observé des améliorations au chapitre de l'échange de renseignements parmi les ministères et les organismes participants ainsi que les acteurs non gouvernementaux, notamment les propriétaires et les exploitants d'infrastructures essentielles et les autres intervenants du secteur privé.

Divers mécanismes officiels et non officiels ont été mis en place pour échanger des renseignements. À titre d'exemple, tel que mentionné précédemment, avant l'avènement de la Stratégie, il n'y avait pas de mécanisme clair pour l'échange d'information avec les organismes responsables du renseignement et de l'application de la loi. Les comités de surveillance établis dans le cadre de la Stratégie servent aux organismes participants de tribune pour échanger de l'information, notamment au niveau opérationnel. Le Centre canadien de réponse aux incidents cybernétiques a aussi mis en place des mécanismes permettant d'échanger de l'information, de diffuser des alertes et des avertissements pour informer les organisations des infrastructures essentielles, les entreprises et les partenaires des gouvernements provinciaux, territoriaux et municipaux au sujet de menaces, de vulnérabilités et d'incidents potentiels, imminents ou réels.

En dépit des améliorations apportées, l'échange de renseignements entre les organismes participants a été effectué en grande partie de façon ponctuelle et sélective. Il n'existait aucune politique claire énonçant les éléments qui devaient faire l'objet d'un échange de renseignements, avec qui et à quel moment. Dans la plupart des cas, les organisations décidaient selon leurs propres conditions des renseignements à communiquer.

Bien que les mandats concurrents ou différents nuisent dans certains cas à l'échange de renseignements, le volume de travail et les délais serrés se sont avérés les plus importants obstacles à la collaboration et à la communication de l'information. Autrement dit, les organisations ont manqué de temps et non de volonté pour échanger des renseignements.

On constate un manque d'outils et d'infrastructures adaptés à l'échange de renseignements classifiés. À l'heure actuelle, plusieurs réseaux classifiés du gouvernement manquent d'interopérabilité. En outre, seuls certains employés y ont accès.

Observations et possibilités d'amélioration

L'échange de renseignements doit devenir systématique et officiel. On doit préciser clairement quels sont les renseignements à communiquer, qui les transmettra et à quel moment, en tenant compte des paramètres juridiques et politiques.

On doit également renforcer l'infrastructure pour l'échange de renseignements classifiés. Ainsi, le gouvernement du Canada doit établir une infrastructure de communications qui est plus

---

fédéraux. SPC fournit également d'autres services facultatifs aux ministères et organismes selon le principe de recouvrement des coûts. Il convient de noter qu'à l'heure actuelle plus de 50 organismes gouvernementaux échappent à la compétence de SPC.

interopérable et mieux protégée, et fournir un accès aux réseaux protégés à un nombre accru d'employés.[21]

3.1.5 État de la recherche et du développement en matière de cybersécurité (R&D)

La Stratégie a incité à faire certains investissements limités en matière de recherche et de développement, plus particulièrement en ce qui touche le Pilier I – Protéger les systèmes du gouvernement du Canada. La plupart des fonds ont été appliqués aux recherches ayant pour but de procurer des avantages d'ici un à cinq ans.[22]

Certains des organismes participants à la Stratégie de cybersécurité du Canada ont éprouvé de la difficulté à pourvoir certains postes hautement techniques. De plus, l'effectif actuel de la cybersécurité est décrit comme étant surutilisé. Ces questions témoignent que le Canada doit accroître et améliorer sa capacité au chapitre de la cybersécurité et que les universités et les collèges canadiens doivent produire plus de diplômés détenant des compétences en cybersécurité.

Observations et possibilités d'amélioration

Le gouvernement du Nouveau-Brunswick a été cité comme un exemple de réussite d'un gouvernement qui alimente un écosystème de cybersécurité par la littérature et certaines personnes interrogées. Ainsi, le Nouveau-Brunswick s'est inscrit comme la première province au Canada à élaborer une stratégie détaillée sur la cybersécurité et l'innovation cybernétique. L'axe principal du plan d'action du Nouveau-Brunswick sur la cybersécurité consiste à renforcer la capacité et l'expertise en cybersécurité dans le cadre de programmes universitaires et l'établissement de partenariats avec le secteur privé.[23]

Pour renforcer la R&D en cybersécurité, certaines des personnes interrogées ont souligné la nécessité pour le gouvernement canadien d'investir davantage dans ce domaine. Malgré que la majorité de ces suggestions puissent aller au-delà la conception originale de la stratégie, elles sont présentées ici à des fins de leçons apprises et de planification future. Selon ces personnes interrogées, il est opportun pour le gouvernement du Canada d'investir davantage dans :

---

[21] Services partagés Canada, en collaboration avec le Bureau du Conseil privé, le Secrétariat du Conseil du Trésor du Canada et le Centre de la sécurité des télécommunications Canada, a mis en œuvre un service temporaire mais limité d'infrastructure de niveau secret du gouvernement du Canada, et s'affaire à l'heure actuelle à fournir ce service centralisé à un plus vaste auditoire au sein de l'appareil gouvernemental (en fonction du financement).

[22] Le gouvernement du Canada a financé de nombreux projets de recherche et de développement en matière de cybersécurité au moyen d'autres initiatives. Par exemple, le Programme canadien pour la sûreté et la sécurité (PCSS), codirigé par le ministère de la Défense nationale et Sécurité publique Canada, comprend un Portefeuille de la sécurité électronique dont les projets axés sur la science et la technologie visent à contribuer à protéger les systèmes importants pour le gouvernement du Canada et à aider les Canadiens à mieux se protéger en ligne.

[23] http://cybernb.ca/en/news/.

- Une stratégie globale pour assurer le développement des compétences requises ainsi que le recrutement et le maintien en poste d'une main-d'œuvre hautement qualifiée en cybersécurité;
- Les jeunes entreprises en cybersécurité afin qu'elles s'enracinent au Canada;
- Les Canadiens et les sociétés canadiennes afin de promouvoir l'entrepreneuriat en cybersécurité;
- Les universités canadiennes et les autres établissements d'enseignement en vue d'offrir un nombre accru de cours et de programmes en cybersécurité.

3.2 Rendement – Mise en œuvre

Dans cette section, on a examiné dans quelle mesure les activités financées dans le cadre de la Stratégie avaient été mises en œuvre. Si une activité n'a pas été pleinement réalisée, on cherchait à savoir pourquoi. La mesure dans laquelle ces activités ont contribué à l'atteinte des objectifs de la Stratégie est mise en lumière dans la prochaine section.

Constatation de l'évaluation : La plupart des activités financées dans le cadre de la Stratégie ont été entièrement mises en œuvre comme prévu. Les exceptions furent l'activité de Recherche et développement pour la défense Canada du ministère de la Défense nationale (MDN) qui consistait à élaborer une architecture d'entreprise et ses produits livrables connexes ainsi que l'activité de la GRC visant à publier un rapport annuel sur la cybercriminalité et les activités de Services partagés Canada visant à sécuriser une troisième connexion Internet ainsi qu'à établir un système de rappel sur l'infrastructure de cybersécurité.

Les organisations participantes ont reçu un financement afin de mener des activités précises liées à la cybersécurité. Selon les renseignements recueillis sur le rendement, la majorité des activités financées dans le cadre de la Stratégie ont été mises en œuvre comme prévu, mais l'évaluation a permis d'en trouver au moins quatre qui ne l'ont pas été :

- Recherche et développement pour la défense Canada du MDN devait concevoir et mettre en œuvre un cadre d'architecture ainsi qu'un lexique sur la cybersécurité et un document relatif à la taxonomie (documents communs). L'organisme a signalé que le 12 avril 2011, ses représentants ont soumis un plan de travail lié à l'architecture, une charte de projet approuvée, un lexique sur la cybersécurité et un document relatif à la taxonomie auprès du Comité des DG responsables de la cybersécurité. Toutefois, on ignore pourquoi la proposition a été annulée. Recherche et développement pour la défense Canada a donc cessé de travailler à ce projet et a consacré la somme de 200 000 $ qui y était allouée annuellement au financement d'autres activités inhérentes à la cybersécurité.
- La GRC devait mettre sur pied le Centre de fusionnement sur la cybercriminalité (CFCC), publier un rapport annuel sur la cybercriminalité et élaborer une stratégie de lutte contre la cybercriminalité. Le Centre de fusionnement ait été mis sur pied, et la GRC a publié un

rapport en 2014 portant sur les tendances en matière de criminalité de 2010 à 2013. Le CFCC a contribué à des documents sur le renseignement criminel destiné au milieu de l'application de la loi et à des rapports produits par le Groupe de travail sur la cybercriminalité du Groupe des cinq.[24] Les ressources du CFCC de la GRC ont été transférées des Opérations techniques au Centre national de coordination du renseignement;[25] et, en décembre 2015, la GRC a lancé sa Stratégie de lutte contre la cybercriminalité, qui devrait permettre à l'organisme de mieux lutter contre la cybercriminalité de concert avec ses partenaires nationaux et internationaux de l'application de la loi et d'autres intervenants.

- Services partagés Canada devait sécuriser une troisième connexion Internet pour assurer la continuité des services Internet du gouvernement du Canada et améliorer le rendement de l'environnement réseau sécurisé existant. Services partagés Canada a indiqué que les connexions Internet actuelles étaient renforcées et qu'elles offraient une plus grande disponibilité et des contrôles de sécurité accrus et qu'il était prêt à activer la troisième connexion avec le fournisseur de service. Cette troisième connexion est en voie d'être terminée.
- Services partagés Canada devait aussi mettre en place un système de rappel sur l'infrastructure de cybersécurité pour veiller à ce qu'il ait accès aux renseignements sur le matériel de TI servant à soutenir les services d'infrastructure pour ses 43 ministères partenaires, ainsi que sur les vulnérabilités et les menaces liées à ce matériel, lui permettant ainsi d'évaluer rapidement les répercussions de la compromission. Services partagés Canada a mis en place un programme d'intégrité de la chaîne d'approvisionnement en collaboration avec le Centre de la Sécurité des télécommunications afin de régler de manière proactive les risques associés à l'achat de matériel, de logiciels et de services informatiques vulnérables, ainsi que de gérer le matériel compromis déjà en place.Dans le cadre du Programme d'intégrité de la chaîne d'approvisionnement, le centre de la sécurité des télécommunications effectue des évaluations de risques et fournit des conseils en matière d'atténuation pour accroître la sécurité de nouveaux équipements dans le réseau du gouvernement du Canada. Sur la base de cette orientation, Services partagés Canada a pris la décision d'appliquer les mesures appropriées afin de réduire les risques à des niveaux acceptables. À la date de ce rapport, Services partagés Canada a mené plus de 21 000 évaluations de l'intégrité de la chaîne d'approvisionnement.

Comme nous l'avons mentionné précédemment, plusieurs organismes ont signalé qu'ils avaient de la difficulté à combler certains postes techniques, surtout dans les milieux Secret et Très Secret.

[24] Ce groupe de travail compte des représentants du Canada, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni, et des États-Unis.

[25] La GRC a indiqué en lien avec le document *Faire avancer la deuxième phase de la Stratégie de cybersécurité du Canada,* , que ces ressources ont mené des activités de renseignement criminel plutôt que de produire des rapports publics sur les tendances en matière de cybercriminalité.

Trois organismes ont signalé une sous-utilisation des fonds. Le ministère de la Justice a dépensé 90 % du financement alloué, alors que la GRC et Services partagés ont signalé avoir dépensé respectivement 69 % et 85 % du financement alloué.[26] Le Service canadien du renseignement de sécurité a signalé que le financement reçu servait à accroître les travaux existants. Il n'a dont pas été en mesure de déterminer exactement quelles activités ont eu lieu en raison du financement reçu. Le Secrétariat du Conseil du Trésor du Canada et Affaires mondiales Canada ont entièrement dépensé leur financement alloué. Le Centre de la sécurité des télécommunications et Sécurité publique Canada ont déclaré des dépenses légèrement supérieures aux montants alloués.

Dans le cadre de la Stratégie, un cadre de mesure du rendement horizontal a été mis en place et un rapport d'étape couvrant les activités horizontales au cours de 2012-2013 et de 2013-2014 a été produit. Bien que le rapport d'étape ait mentionné l'intégration des ressources du CFCC de la GRC au Centre national de coordination du renseignement ainsi que la publication du premier rapport de la GRC sur la cybercriminalité, il n'a pas abordé les questions liées à la mise en œuvre précitées (c.-à-d. pourquoi certaines activités n'avaient pas été mises en œuvre tel que prévu). Les difficultés auxquelles se sont heurtés certains des organismes participants quant à la communication de renseignements pertinents sur le rendement laissent entendre que cette information n'a pas été recueillie de manière régulière et uniforme ou qu'elle n'était pas facilement accessible.

Étant donné que les comités de surveillance ne consignent pas les comptes rendus de réunions et en l'absence de tout autre document, l'évaluation n'a pas permis de déterminer le processus qui a été employé de manière individuelle ou collective par les organismes quant à décision de ne pas mettre pleinement en œuvre les activités financées dans le cadre la Stratégie. Elle n'a pas pu aussi établir dans quelle mesure les comités de surveillance étaient informés de ces développements. En tant que tel, l'évaluation a considéré la mise en œuvre partielle de certaines activités financées comme une déviation par rapport à la conception originale de la Stratégie.

Observations et possibilités d'amélioration

Les questions soulevées ci-haut soulignent le besoin de renforcer le Cadre de mesure du rendement de la Stratégie afin de recueillir des données sur le rendement qui soient pertinentes, fiables et orientées sur les résultats, et ce, de manière régulière et uniforme, et d'assurer le suivi des dépenses de programme. De tels renseignements sur le rendement et les dépenses doivent être transmis aux comités de surveillance afin qu'ils puissent assumer leurs responsabilités en surveillant les progrès accomplis par les organismes participants en ce qui touche la mise en œuvre de la Stratégie et en améliorant le rendement de celle-ci de façon permanente.

[26] Subséquemment à sa création, Services partagés a assumé la responsabilité des postures de sécurité en place de 43 organismes partenaires à différents stades d'avancement. Services partagés Canada a signalé qu'en 2014-2015 il avait officialisé un programme de cybersécurité et de sécurité des TI, lequel a été suivi par la création en 2015-2016 d'une direction générale dédiée à cette fin. Par la suite, Services partagés Canada a augmenté de manière importante ses propres dépenses de crédits liées à la cybersécurité afin de fournir des services de cybersécurité et de sécurité des TI pour atteindre les objectifs stratégiques connexes de la Stratégie.

3.3 Rendement – Efficacité

Cette section aborde des enjeux tels que dans quelle mesure le gouvernement du Canada a protégé ses systèmes et renforcé sa capacité à prévenir les cyberincidents, à détecter les cybermenaces et à se défendre contre celles-ci. En outre, cette section se penche sur la capacité du gouvernement du Canada à intervenir en cas de cybermenaces et à se rétablir après coup. De surcroît, cette section examine les progrès accomplis au chapitre de l'établissement de partenariats visant à protéger les cybersystèmes essentiels à l'extérieur du Canada et à aider les Canadiens à se protéger en ligne. Le dernier point portera sur l'examen de la réussite des campagnes de sensibilisation du public en vue d'améliorer les connaissances des Canadiens sur les menaces en ligne, et du degré de sensibilisation des organismes d'exécution de la loi à l'égard des tendances en matière de cybercriminalité.

3.3.1 Progrès liés à la protection des systèmes du gouvernement du Canada

Constatation de l'évaluation : Le gouvernement du Canada a amélioré de manière considérable sa capacité à prévenir et à détecter les cyberattaques, à intervenir et à se rétablir après coup. Cette amélioration est attestée par une baisse constante des atteintes à la protection des données et à une meilleure capacité des organismes gouvernementaux à analyser et à maîtriser rapidement celles-ci. Ces réalisations existent, malgré une hausse des cyberattaques étatiques et non étatiques qui ont été lancées contre les réseaux du gouvernement du Canada au cours des dernières années.

Toutes les personnes interrogées conviennent que le gouvernement du Canada a amélioré sa capacité à prévenir et à détecter les cyberincidents, à intervenir et à se rétablir après coup. Cela dénote que les investissements du gouvernement dans la Stratégie de cybersécurité du Canada ont contribué directement à ces réalisations. Par conséquent, en 2009 et avant la mise en œuvre de la Stratégie :

- L'approche à l'égard de la cybersécurité était extrêmement fragmentée;
- On observait une faible capacité à détecter et à prévenir les cybermenaces;
- Les organismes du gouvernement avaient des infrastructures de sécurité des TI, des postures de sécurité et des stades d'avancement différents, et ils avaient assumé différents niveaux de risque;
- Il régnait une confusion quant aux rôles et responsabilités des organismes du gouvernement en matière de cybersécurité et ces organismes devaient, pour la plupart, protéger leurs propres systèmes;
- De nombreux obstacles empêchaient l'échange de renseignements;
- Les systèmes de TI du gouvernement du Canada présentaient de nombreuses vulnérabilités. Celles-ci incluaient plus de 2 900 points d'accès Internet et plus de

400 centres de données, ce qui offrait amplement l'occasion d'exploiter ou de perturber les systèmes.

Après l'avènement de la Stratégie et la mise en œuvre des initiatives de cybersécurité subséquentes, comme la création de Services partagés Canada, l'infrastructure des TI du gouvernement du Canada a été regroupée, centralisée et améliorée. Cette consolidation a permis à Services partagés Canada de développer et de mettre en œuvre une approche d'entreprise pour la prestation de services de sécurité informatique à ses clients.Par exemple, le nombre de points d'accès à l'Internet a été réduit à deux services Internet d'entreprise de base (avec un troisième en préparation), trois centres de données d'entreprise ont été établis et un processus a été entamé pour regrouper les systèmes de courriel afin d'en avoir un seul. Ceci est toujours en cours.

Outre les avantages sur le plan de la sécurité inhérents à ce regroupement, comme la réduction de la « surface d'attaque », une approche pangouvernementale en matière de cybersécurité a été élaborée pour la première fois pour le gouvernement du Canada. Cette approche comprenait l'établissement d'un lien de travail étroit entre les principaux organismes de sécurité par la mise en place d'une structure de gouvernance tripartite axée spécifiquement sur la protection et la sécurisation des systèmes du gouvernement du Canada.[27]

Ces mesures et la mise en œuvre des mesures de Sécurité ci-dessous financées dans le cadre de la Stratégie ont amélioré la capacité du gouvernement de prévenir, de déceler et de gérer les menaces touchant les TI :[28]

- Un seul centre des opérations de sécurité pangouvernemental qui fonctionne en tout temps pour surveiller et déceler les cyberincidents a été établi au sein de Service partagés Canada et un processus de gestion des incidents pour l'ensemble du gouvernement du Canada a été promulgué par le Secrétariat du Conseil du Trésor du Canada, en collaboration avec Services partagés Canada. À ce jour, le centre des opérations de sécurité a trié des milliers d'événements cybernétiques et géré les cyberincidents connexes confirmés. Au taux actuel, les enquêtes sur les incidents devraient augmenter de 261 %[29] en raison des améliorations apportées continuellement à la surveillance et à la détection.
- Une équipe mobile et spécialisée en cyber rétablissement a été créée à Services partagés Canada pour assurer le rétablissement rapide des services à la suite d'une compromission de l'infrastructure de TI du gouvernement du Canada. Il est notamment question des services d'analyse judiciaire permettant d'enquêter sur les cyberincidents et leurs causes, dans le but de mettre en place des mesures futures d'atténuation. L'équipe chargée du rétablissement a été déployée d'un océan à l'autre, a travaillé en étroite collaboration avec au moins 25 ministères et organismes différents afin de leur fournir de l'aide, des conseils et un leadership sur un grand nombre d'incidents documentés. Selon les tendances observées entre 2014-2015 et 2015-2016, toutes les activités liées à l'analyse judiciaire devraient augmenter comme suit : 137 % dans les domaines des enquêtes judiciaires et du

[27] Les comités de Sécurité tripartites comptent des représentants (DG, SMA et SM) du Centre de la sécurité des télécommunications, du Secrétariat du Conseil du Trésor du Canada et de Services partagés Canada.

[28] En date du 1er avril 2016.

[29] 2015-2016 : 1163; 2016-2017 – cinq premiers mois : 1 197.

rétablissement, 240 % dans le domaine de l'aide donnée par Services partagés Canada aux agents de sécurité des ministères pour les enquêtes judiciaires, et 144 % dans le domaine des conseils et de l'orientation.

- Déploiement de capacités avancées de détection et de dissuasion vers un nombre important de ministères. En 2016, le nombre de tentatives pour identifier et exploiter les vulnérabilités dans les réseaux et les systèmes du gouvernement du Canada que le Centre de la sécurité des télécommunications bloque quotidiennement a augmenté de près de dix fois. La consolidation des réseaux du gouvernement du Canada a permis au gouvernement de déployer simultanément ces capacités de détection et de dissuasion. Par conséquent, si une vulnérabilité est détectée dans un seul ministère, elle peut servir d'alerte précoce pour la protection de tous les ministères sur le réseau consolidé. Sur la base de l'étendue de la menace actuelle, les défenses au niveau du réseau ne suffisent pas et devraient être complétées par une protection de point final.
- Un programme d'intégrité de la chaîne d'approvisionnement complet pour faire en sorte que seuls des produits de TI (logiciels et matériel) et des services de TI dignes de confiance sont achetés et mis en place et que des mécanismes sont en place pour gérer rapidement le matériel compromis. À ce jour, plus de 16 000 examens de l'intégrité de la chaîne d'approvisionnement ont été faits dans le cadre du programme, selon les statistiques de 2015-2016, ce qui représente une hausse de 300 % par rapport à l'année précédente.
- Une dispersion géographique et une redondance de l'infrastructure de TI pour faire en sorte que les systèmes sont disponibles en cas de cyberincident; augmentation de la sécurité et de la résilience des deux points d'accès Internet de base et mise à niveau de l'infrastructure pour intégrer une troisième connexion Internet dans un lieu géographique distinct afin d'avoir une robustesse accrue. Création d'un autre centre des opérations de sécurité intérimaire actif[30] dans un autre lieu géographique.
- Un plan a été mis en œuvre pour la gestion des incidents de cybersécurité touchant le gouvernement du Canada. Depuis sa création en décembre 2015, on a fait appel au plan et aux processus et procédures connexes à de nombreuses reprises pour orienter les intervenants en cybersécurité du gouvernement du Canada (dont le SCT, SPC et le CST) au sujet du traitement des menaces pour les systèmes du gouvernement et des vulnérabilités de ces derniers. Le plan a servi de modèle pour appuyer les ministères qui coordonnent des activités qui revêtent une importance nationale (comme l'élection fédérale de 2016).
- Un exercice de gestion des incidents cybernétiques a été mené au niveau de sous-ministre adjoint pour veiller à ce que les cadres supérieurs comprennent les processus de gestion des incidents cybernétiques du gouvernement du Canada. L'exercice EnGarde 2016 a rassemblé des représentants de 13 ministères dans le but de faire connaître aux cadres supérieurs les rôles et responsabilités en matière de sécurité cybernétique et de les

[30] Selon Services partagés Canada, l'exigence consistait à mettre en place un site de repli inactif, mais Services partagés Canada a mis en place un site actif avec les crédits votés afin d'assurer une continuité harmonieuse de ce service essentiel.

familiariser avec la diffusion de l'information et les exigences en matière de collaboration ainsi que les processus et procédures en matière de communications stratégiques.

- Un programme d'architecture de sécurité intégrée a été mis en œuvre afin de fournir une approche normalisée en matière d'élaboration de l'architecture de sécurité des TI du gouvernement du Canada. Il permet de s'assurer que les composantes de base en matière de sécurité élémentaire sont mises en place à mesure que l'infrastructure du gouvernement du Canada est renouvelée. Le programme d'architecture de sécurité intégrée a fourni des outils et des modèles détaillés à l'intention des ministères et des organismes en intégrant la sécurité à leurs programmes de TI. Plus particulièrement, le programme a été utilisé pour mettre en œuvre une approche de sécurité dès la conception pour les initiatives de transformation de Services partagés Canada, comme l'Initiative de transformation des services de courriel, les projets liés à la transformation des services administratifs, dont GCDOCS,[31] MesRHGC,[32], la Plate-forme d'interopérabilité du gouvernement du Canada et la Stratégie du gouvernement du Canada pour l'adoption de l'infonuagique.
- Le Plan stratégique des TI du gouvernement du Canada, dans le cadre duquel la sécurité est un facteur clé, a été mis sur pied en 2016. Ce plan, qui couvre la période quinquennale de 2016 à 2020, articule la nécessité de compter sur des défenses par couches pour réduire l'exposition aux menaces cybernétiques et l'utilisation de TI dignes de confiance pour assurer le traitement et le stockage sécuritaires de données et d'information, en plus d'accroître la sensibilisation aux menaces et la compréhension de ses dernières. Le plan souligne aussi diverses initiatives actuelles ou futures qui seront mises en œuvre dans l'ensemble du Ministère afin d'améliorer la poste du gouvernement du Canada en matière de sécurité cybernétique.

Les activités financées dans le cadre de la Stratégie ont contribué à cette capacité accrue du gouvernement à prévenir et à détecter les cyberincidents, à intervenir et à se rétablir après coup. Par exemple, le CST a amélioré sa capacité de défendre les réseaux et systèmes du gouvernement du Canada en déployant des services de cyberdéfense en collaboration avec Services partagés Canada. En tant que tel, le CST défend la majorité des ministères et organismes gouvernementaux contre les menaces cybernétiques. Pour ce faire, le CST analyse des dizaines de téraoctets de télémétrie réseau et système et, par conséquent, effectue quotidiennement des centaines de millions d'atténuations défensives directes sur les réseaux et les systèmes du gouvernement du Canada.

De nombreuses personnes interrogées ont mentionné qu'en l'absence de la plus grande protection offerte par la Stratégie de cybersécurité du Canada, les cybersystèmes du gouvernement du Canada auraient sans cesse fait l'objet de perturbations étant donné l'évolution et la sophistication des menaces de nos jours.

[31] GCDOCS est un système de gestion des documents et des dossiers électroniques qui est déployé dans le cadre de l'Initiative Gouvernement ouvert du gouvernement du Canada afin de permettre une tenue de documents uniforme.

[32] L'application Mes RH du gouvernement du Canada (MesRHGC) appuie les ministères au moment où ils passent de leur application existante en matière de RH à la norme du gouvernement du Canada.

Bien que des cyberincidents et des intrusions surviennent encore, ils sont de moins en moins fréquents :

- Selon les renseignements sur le rendement fournis par le CST, le gouvernement du Canada empêche en moyenne plus de 600 millions de tentatives quotidiennes d'identification et d'exploitation des vulnérabilités de ses systèmes et réseaux.
- Selon la même source, entre 2013 et 2015, le gouvernement du Canada a détecté en moyenne par année plus de 2 500 activités cybernétiques parrainées par des États contre ses réseaux;
- Bien que plus de six pour cent de ces tentatives aient donné lieu à des intrusions dans les systèmes du gouvernement du Canada en 2013, ce pourcentage a chuté à moins de 2 pour cent en 2015.

Certaines des personnes interrogées étaient d'avis qu'un taux d'intrusion même de deux pour cent se révèle inacceptable et qu'il faudrait un degré de tolérance zéro à cet égard. Toutefois, la majorité d'entre elles ont indiqué que la prévention de toutes les cyberattaques est irréaliste. Elles ont soutenu que le gouvernement du Canada devrait mettre l'accent sur la réduction des risques d'attaque et la minimisation de leurs répercussions.

La Stratégie de cybersécurité du Canada a permis au gouvernement canadien de répondre plus rapidement aux cyberintrusions et à se rétablir plus vite. Le gouvernement a mis en place un Plan de gestion des événements de cybersécurité fondé sur les leçons retenues à la suite d'attaques antérieures. En outre, le gouvernement a adopté un meilleur régime de reprise des activités, y compris autoriser une seule entité à superviser le processus de reprise, ce qui n'était pas envisageable auparavant.

Ces étapes ont également permis de renforcer le processus de reprise. En raison de la large portée des programmes de cyberdéfense du gouvernement du Canada, le coût et l'heure des compromis ont été considérablement réduits. Par exemple, un compromis en 2014, avant que ces mesures ne soient mises en place, coûtait des dizaines de millions de dollars et des mois à être traiter. Avec ces défenses en place, une tentative de compromis similaire a été abordée en moins d'une semaine à un coût minime.

Le rétablissement de l'Agence du revenu du Canada par suite d'une faille de sécurité appelée « Heartbleed » en 2014 constitue un bon exemple quant à la manière de s'attaquer à une cyberattaque et de se rétablir. L'Agence du revenu du Canada a reconnu d'emblée l'intrusion et a rapidement demandé aux experts de limiter ses répercussions.

Observations et possibilités d'amélioration

En dépit des nombreuses avancées en matière de cybersécurité, des lacunes demeurent. Beaucoup de personnes interrogées ont fait remarquer que le gouvernement du Canada doit renforcer davantage sa capacité à prévenir et détecter les cyberattaques, à intervenir et à se rétablir après coup, notamment par :

- Une meilleure collaboration avec les acteurs internationaux pour élaborer des normes internationales visant à réduire les cybermenaces (p. ex. élaboration d'un politique étrangère en matière de cybersécurité);
- L'élaboration d'un ensemble d'outils d'entreprise pour l'information de Sécurité du gouvernement du Canada et la surveillance des incidents (les bases de la surveillance de sécurité et de la détection), et la mise en place d'un laboratoire de développement, d'essai et d'intégration pour l'ensemble du gouvernement du Canada;
- Un investissement dynamique en immobilisations pour l'infrastructure classifiée en appui à l'échange et au traitement d'information ministérielle sécurisés (en ce moment, le matériel servant aux communications classifiées est financé selon le principe de recouvrement des coûts auprès des partenaires – un investissement dans les infrastructures est nécessaire dès le départ pour mettre en place une infrastructure dédiée); et
- La mise en place élargie des mesures d'atténuation élaborées par le Centre de la Sécurité des télécommunications, qui, selon certaines des personnes interrogées, éliminerait la grande majorité des cybermenaces envers les systèmes du gouvernement du Canada.[33]

3.3.2 Progrès liés à la protection des systèmes importants pour le gouvernement du Canada

Constatation de l'évaluation : La Stratégie a contribué à nouer des partenariats avec les propriétaires et les exploitants d'infrastructures essentielles et les autres intervenants du secteur privé. Toutefois, selon certaines des personnes interrogées et la littérature examinée, les progrès globaux liés à la protection des systèmes importants pour le gouvernement du Canada (c'est-à-dire infrastructures essentielles) ont été limités.

De nombreux forums sectoriels et intersectoriels, des tables rondes et des groupes consultatifs ont été mis sur pied afin de mobiliser les représentants des gouvernements provinciaux et

[33] En 2014, le Centre de la sécurité des télécommunications a recommandé que les organismes du gouvernement du Canada mettent en œuvre les dix mesures d'atténuation les plus efficaces en vue d'améliorer la sécurité des réseaux. Cette liste comprend l'utilisation des passerelles Internet de Services partagés Canada. Le Centre de la sécurité des télécommunications croit que les utilisateurs tireront ultérieurement parti de « la protection assurée par les mesures de cyberdéfense plus poussées en place au niveau de l'organisme qui détectent et empêchent les accès non autorisés, l'exfiltration de données et d'autres activités malveillantes » (https://www.cse-cst.gc.ca/fr/node/1297/html/25231). L'*Audit interne horizontal de la sécurité de technologies de l'information dans les grands et les petits ministères* de 2015 du Bureau du contrôleur général a révélé que « ces cadres de contrôle n'avaient pas été mis en œuvre dans la plupart des ministères ainsi que l'infrastructure de TI ». Certaines des personnes interrogées dans le cadre de notre évaluation ont mentionné que l'infiltration des réseaux du Conseil national de recherches du Canada (CNRC) en 2014 peut être attribuée directement au choix de ce dernier de ne pas utiliser les passerelles de Services partagés Canada et de demeurer à l'extérieur des réseaux normalisés du gouvernement du Canada. D'après les rapports des médias, l'infiltration du CNRC a occasionné la fermeture de ses systèmes pendant plusieurs mois et a nécessité une refonte de la TI durant toute l'année à des coûts estimés à 32,5 millions de dollars (http:// ottawacitizen.com/ news/politics/ cyber-attack- at-nrc-kept-secret-from-other-departments).

territoriaux, les propriétaires et les exploitants d’infrastructures essentielles et les autres intervenants du secteur privé sur les questions associées à la cybersécurité.

Depuis le lancement de la Stratégie, plusieurs centaines d’activités de mobilisation ont eu lieu avec les secteurs des infrastructures essentielles, y compris les autres ordres de gouvernement. De la même façon, les propriétaires et les exploitants d’infrastructures essentielles et les autres intervenants du secteur privé ont assisté à de nombreuses formations et séances de sensibilisation parrainées dans le cadre de la Stratégie. De plus, les architectes de la cybersécurité du CST, entre autres, fournissent des conseils et des orientations pour atténuer les risques liés à la chaîne d'approvisionnement et développer de manière collaborative les meilleures pratiques pour des secteurs spécifiques.

Le CST a mis en place le programme amélioré de technologie et de partage de l'information pour partager ses capacités en matière de sécurité et de cyberdéfense avec les secteurs de l'industrie privée et des infrastructures essentielles du Canada grâce à une série d'initiatives en cours. Le CST a des relations actives avec plusieurs partenaires de tous les secteurs des infrastructures essentielles du Canada, y compris l'industrie financière, les fournisseurs de télécommunications et les services de sécurité gérés. Le CST a développé une série de story-boards détaillant les capacités et les services qu'il entend déployer pour aider à défendre les partenaires canadiens d'infrastructure essentielle. Trois de ces story-boards ont évolué à la phase de projet.

Dans le cadre de l'amélioration de la cybersécurité de l'infrastructure essentielle du Canada, CST collabore avec diverses institutions financières canadiennes pour lutter contre la fraude cybernétique financière et pour partager des numéros de carte de crédit compromis et des indicateurs de compromis exploités grâce à un programme malveillant ciblant les terminaux de points de vente.

Le CST et Sécurité publique représentent le gouvernement du Canada sur le Conseil d'administration de l'Échange canadien de menaces cybernétiques (ECMC) dans un rôle consultatif. ECMC est un organisme national de partage de l'information sur la cybersécurité dirigé par le secteur privé, représenté par les principaux secteurs de l'infrastructure essentielle, offrant un point de contact unique pour la collaboration du secteur privé sur la cybersécurité.

Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) a élargi ses activités et renforcé ses capacités techniques (préventives et réactives), y compris sa faculté à recueillir et à analyser les renseignements. On compte au moins 1 300 organismes du secteur privé qui ont reçu régulièrement des alertes du CCRIC.

À l’heure actuelle, le gouvernement du Canada s’est engagé considérablement et plus que jamais auprès des propriétaires et des exploitants d’infrastructures essentielles et des autres intervenants du secteur privé. La plupart des personnes interrogées ont attribué ce niveau d’engagement et les activités de sensibilisation directement à la Stratégie et aux investissements dans ce domaine. Ces éléments ainsi que les autres activités de sensibilisation dirigées par Sécurité publique Canada ont permis de fournir des possibilités d’éducation ainsi qu’une bonne présence à l’échelle nationale et internationale.

Observations et possibilités d'amélioration

En dépit de ces améliorations, certaines lacunes ont également été relevées :

- Selon certaines des personnes interrogées, l'investissement global de la Stratégie au chapitre de la protection des systèmes importants pour les Canadiens s'est avéré inadéquat. Certains ont indiqué que le gouvernement a consacré la majeure partie de ses investissements à la protection de ses systèmes.
- On doit clarifier les rôles et les responsabilités, notamment ceux du CST et du Centre canadien de réponse aux incidents cybernétiques (CCRIC). Plus particulièrement, on doit préciser quel organisme servira de premier point de contact pour le secteur privé en cas de cyberincident;
- Des progrès limités ont été accomplis dans le cadre de l'établissement de normes réciproques pour l'échange de renseignements et la formation de partenariats avec le secteur privé, ainsi qu'avec les provinces et les territoires;
- Il semble y avoir un manque de confiance de la part des entreprises du secteur privé en ce qui a trait à la capacité du secteur public de protéger leurs renseignements;
- Il n'existe aucune politique claire quant à la manière de mobiliser les entreprises qui détiennent des renseignements sensibles du gouvernement, mais qui ne sont pas des propriétaires ni des exploitants d'infrastructures essentielles.

3.3.3 Progrès visant à aider les Canadiens à naviguer en ligne en toute sécurité

Constatation de l'évaluation : La plupart des personnes interrogées ont le sentiment que les Canadiens sont plus renseignés sur les cybermenaces qu'au cours des dernières années. Toutefois, cette sensibilisation accrue ne signifie pas nécessairement que les Canadiens sont mieux protégés en ligne, ni qu'elle peut être attribuée à la campagne de sensibilisation du public de Sécurité publique Canada.

Campagne de sensibilisation du public : L'équipe Communications de Sécurité publique Canada (SP) a coordonné les activités de sensibilisation et de communication liées à la cybersécurité, notamment la publicité, le marketing social, les partenariats, les relations avec les médias Internet, les expositions et les événements spéciaux.

Peu avant le lancement de la campagne de sensibilisation du public, SP a effectué une recherche sur l'opinion publique pour sonder les connaissances, les attitudes et les comportements des Canadiens par rapport à la cybersécurité. Cette recherche devait être effectuée chaque année pour mesurer les progrès.

La recherche a conclu qu'il y avait une attente générale selon laquelle «une campagne de sensibilisation devrait fournir des informations simples, directes et orientées vers l'action conformément à ce qui est à la portée des Canadiens».

À cette fin, et dans le but de joindre un vaste public, le Ministère a entrepris de nombreuses activités, par exemple en faisant des publicités à la radio et en ligne afin d'établir des partenariats rémunérés et non rémunérés. Ces partenariats mettaient en cause des organismes du secteur public, différents bureaux de presse, commerces de détail et organisations du secteur privé, notamment Bell, TELUS, Best Buy, Twitter, Facebook, et LinkedIn. Le Ministère a également :

- lancé le site Web Pensez cybersécurité et son équivalent Get Cyber Safe. Ces sites Web proposent des étapes simples que les Canadiens peuvent suivre pour se protéger en ligne;
- noué un partenariat avec le groupe STOP. THINK. CONNECT, un partenariat global axé sur la sensibilisation à la cybersécurité. Il s'agit d'une coalition d'entreprises du secteur privé et d'organisations gouvernementales et sans but lucratif, dont le département américain de la Sécurité intérieure;
- élaboré des trousses d'outils et des guides destinés aux petites et moyennes entreprises, aux secteurs des finances et aux banques et des télécommunications;
- lancé le Mois de la sensibilisation à la cybersécurité, qui a lieu chaque mois d'octobre afin d'aider les Canadiens à apprendre comment se protéger en ligne.

Des centaines d'heures de programmes promotionnels et éducatifs ont été produites au cours de ces activités.

La campagne de sensibilisation du public a généré une quantité importante de statistiques liées aux résultats (p. ex. le nombre de personnes qui ont consulté le site Web ou assisté à une activité éducative). Néanmoins, aucune donnée accessible ne permettait de conclure dans quelle mesure ces activités ont contribué au résultat prévu de la Stratégie visant à faire en sorte que les « Canadiens soient protégés en ligne ».

Contrairement au plan initial, l'équipe Communications de Sécurité publique, en raison de la décision du gouvernement de consolider le nombre d'enquêtes d'opinion publique, était incapable d'effectuer sur une base annuelle une recherche sur l'opinion publique afin de mesurer les progrès quant à l'atteinte des repères établis dans la base de référence de la recherche sur l'opinion publique. Étant donné que l'évaluation s'appuyait sur les renseignements tirés des entrevues et de la revue de la littérature, on n'a pas été en mesure de déterminer dans quelle mesure la campagne de sensibilisation du public a permis d'accroître la sensibilisation ou de modifier les comportements.

Sensibilisation des organismes d'exécution de la loi envers les tendances en matière de cybercriminalité: La GRC devait créer un Centre de fusionnement sur la cybercriminalité pour faire progresser la connaissance situationnelle et l'analyse des tendances de la cybercriminalité ainsi qu'élaborer une stratégie de lutte contre la cybercriminalité. Ce centre visait à :

- combler les principaux écarts analytiques en matière de cybercriminalité;
- mieux évaluer les cyberincidents et aider à y répondre;
- fournir une meilleure compréhension des menaces et des risques inhérents à la cybercriminalité;

- publier un rapport annuel sur la cybercriminalité et décrire le travail accompli en ce qui a trait à la collecte et à l'analyse des statistiques.

Selon les documents examinés et les responsables de la GRC interrogés dans le cadre de cette évaluation, la GRC a mis sur pied un Centre de fusionnement sur la cybercriminalité (CFCC) en 2011, et celui-ci fournissait aux organismes d'exécution de la loi des renseignements en vue de permettre une meilleure compréhension des menaces et des risques associés à la cybercriminalité.

En 2014, la GRC a publié un rapport intitulé *Cybercriminalité : survol des incidents et des enjeux au Canada*.[34] Ce rapport porte sur les menaces et les tendances en matière de cybercriminalité, fournit une définition officielle des différents types de cybercriminalité, présente des statistiques sur la nature et l'ampleur des cyberincidents signalés en 2011 et en 2012, en plus de citer des exemples et des études de cas de 2010, 2011, 2012 et 2013.

Bien que les documents initiaux précisent que le Centre de fusionnement sur la cybercriminalité préparerait un rapport annuel de la GRC sur la cybercriminalité, la GRC a indiqué, en lien avec le document *Faire avancer la deuxième phase de la Stratégie de cybersécurité du Canada* de 2014, que ses ressources ont mené des activités de renseignement criminel plutôt que de produire des rapports publics sur les tendances en matière de cybercriminalité.

En 2015, la GRC a lancé sa Stratégie de lutte contre la cybercriminalité visant à réduire la menace de la cybercriminalité au Canada ainsi que les répercussions et la victimisation qui en découlent au moyen de mesures d'application de la loi.

Politique en matière de cybercriminalité et développement législatif: Le ministère de la Justice du Canada était chargé de fournir des conseils juridiques, de soutenir des partenariats en représentant le Canada aux forums internationaux et fédéraux / provinciaux / territoriaux et de mettre au point des politiques et des lois sur la cybercriminalité.

La Section de la politique en matière de droit pénal du ministère de la Justice a mené un certain nombre d'activités, y compris la prestation de conseils juridiques. Elle a notamment participé à des discussions sur la cybercriminalité à l'ONU, dans le contexte pénal, et au Conseil de l'Europe, en relation avec la Convention sur la cybercriminalité, qui est en vigueur au Canada.

Le Ministère a également participé à l'élaboration de politiques et de lois sur la cybercriminalité, notamment à des modifications récentes au Code criminel, à la Loi sur la concurrence, à la Loi sur la preuve au Canada et à la Loi sur l'entraide juridique en matière criminelle (ancien projet de loi C-13) ainsi qu'à des modifications à la Loi antiterroriste (ancien projet de loi C-51) et au Code criminel visant à assurer la constitutionnalité de l'article 184.4 (ancien projet de loi C-55).

L'imposition de certaines restrictions de dépenses à l'échelle du gouvernement et des ministères, notamment en ce qui concerne les voyages, a eu un impact négatif sur la capacité du ministère de

[34] http://www.rcmp-grc.gc.ca/fra/cybercrime-an-overview-incidents-and-issues-canada.

la Justice de représenter le Canada aux forums internationaux et fédéraux / provinciaux / territoriaux.

Observations et possibilités d'amélioration

Bon nombre des personnes interrogées ont affirmé qu'elles n'étaient pas familières avec la campagne de sensibilisation du public. Par conséquent, elles n'ont pas voulu formuler de commentaires à cet égard. Ce manque de familiarité souligne peut-être le besoin d'accroître la visibilité de la campagne.

Certaines des personnes interrogées qui ont commenté la campagne ont souligné la nécessité d'intégrer la cybersécurité dans les programmes scolaires.[35] Ce besoin a également été soulevé par les participants du Forum des politiques publiques sur la protection du cyberespace au Canada, qui a eu lieu à Toronto en mars 2016. Les participants ont recommandé que les « écoles primaires, secondaires et postsecondaires s'efforcent davantage d'enseigner aux étudiants en quoi consistent la cybersécurité et le protocole en ligne. » En outre, dans le cadre du Forum, on a recommandé que les « programmes d'éducation visent également à informer et éduquer les parents, étant donné que bon nombre d'entre eux ne comprennent pas comment les cybermenaces peuvent influer sur leurs familles. »[36]

On doit réaliser des sondages de suivi afin de mesurer le degré de sensibilisation des Canadiens envers la cybersécurité et évaluer les progrès accomplis quant à l'atteinte des repères établis dans la base de référence de la recherche sur l'opinion publique. Ces sondages peuvent également orienter la planification des prochaines campagnes.

Il semble y avoir de faibles taux de signalement de la cybercriminalité à la police. Les Canadiens disposent d'une myriade de moyens pour signaler ces crimes à la police et au gouvernement, ce qui engendre de la confusion. Les entreprises semblent réticentes à signaler ces crimes puisque cela pourrait nuire à leur revenu ou à leur réputation, ou aux deux. [37]

Selon les données les plus récentes de Statistique Canada, en 2013, « plus de la moitié de tous les crimes cybernétiques signalés [à la police] ont été décrits comme des infractions frauduleuses, avec 6 203 infractions sur un total de 11 124 infractions toutes catégories confondues. »[38]

4. CONSTATATIONS DE L'ÉVALUATION ET CONCLUSIONS

La structure de gouvernance de la Stratégie de cybersécurité du Canada a permis aux organismes participants d'échanger des renseignements, de collaborer et de se coordonner les uns aux autres.

---

[35] Il convient de noter que cet aspect ne relève pas de la compétence directe du gouvernement fédéral.

[36] http://www.ppforum.ca/sites/default/files/Securing%20Canada%27s%20Cyberspace%20-%20Toronto%20report%20-%20Final_0.pdf, page 10 [accessible uniquement en anglais].

[37] https://www.thestar.com/business/2015/08/19/canadian-companies-have-no-incentive-to-report-cyber-attacks-like-that-on-ashley-madison.html. [accessible uniquement en anglais].

[38] http://www.statcan.gc.ca/daily-quotidien/150609/dq150609d-fra.pdf.

Toutefois, en l'absence de documentation à l'appui, il n'a pas été possible d'évaluer l'efficacité globale de la structure de gouvernance.

Hormis le Comité des DG responsables des opérations liées à la cybersécurité, aucun des comités de surveillance responsables de la cybersécurité ne s'est réuni de manière régulière et n'a maintenu les comptes rendus de réunions sur une base constante. Ce manque d'uniformité dans la tenue à jour des comptes rendus de réunions a limité la capacité de l'évaluation de vérifier la mesure dans laquelle les comités de surveillance s'acquittent de leurs rôles et de leurs responsabilités tels qu'ils sont décrits dans leurs mandats, notamment en ce qui a trait la surveillance continue de la mise en œuvre de la Stratégie et des progrès réalisés.

Bien que la Stratégie ait contribué à préciser les rôles et les responsabilités des organismes participants, on a relevé au cours de l'évaluation des cas particuliers où il semblait y avoir un chevauchement au chapitre du mandat, des rôles et des responsabilités. Ce chevauchement a suscité de la confusion et de la frustration chez les ministères et les organismes concernés, ainsi que chez les intervenants du secteur privé.

Cette confusion s'applique plus particulièrement aux rôles et aux responsabilités inhérentes au CCRIC et au CST. De nombreuses personnes interrogées nous ont confié, d'après leurs interactions, que les intervenants du secteur privé ne savaient pas vers qui ils doivent se tourner en premier au sein du gouvernement dans le cas d'un incident ou d'un autre problème lié à la cybersécurité.

En grande partie, les organismes participants échangent des renseignements de manière ponctuelle et sélective. Il n'existe aucune politique claire qui stipule quels renseignements doivent être communiqués, à qui et à quel moment. En règle générale, les organismes décident selon leurs propres conditions des renseignements à communiquer. En outre, les organismes ne disposent d'aucun moyen efficace de transmettre des renseignements classifiés en temps réel.

La plupart des activités financées de la Stratégie ont été mises en œuvre comme prévu. Dans le cadre de l'évaluation, on a relevé quatre cas où les activités financées ont été réalisées en partie. Trois organismes ont signalé ne pas avoir dépensé tous les fonds attribués, et deux organismes n'ont pas été en mesure de faire le suivi des dépenses pertinentes. En outre, trois organismes ont indiqué qu'ils avaient de la difficulté à combler certains postes techniques, surtout dans les milieux Secret et Très Secret.

La Stratégie a contribué à nouer des partenariats avec les propriétaires et les exploitants d'infrastructures essentielles et les autres intervenants du secteur privé. Néanmoins, selon les personnes interrogées, les progrès liés à la protection des systèmes importants (p. ex. les infrastructures essentielles) pour le Canada sont limités. L'investissement global dans le cadre de la Stratégie au chapitre de la protection des systèmes importants pour le Canada a été jugé inadéquat. Des progrès timides ont été réalisés en ce qui a trait à l'établissement de normes réciproques pour l'échange de renseignements et la formation de partenariats avec le secteur privé, les provinces et les territoires.

Le gouvernement du Canada a accru de manière considérable sa capacité à prévenir et à détecter les cyberattaques, à intervenir et à se rétablir après coup. Le nombre d'atteintes à la protection

des données a chuté de manière constante. Le gouvernement peut dorénavant analyser et contenir plus rapidement qu'auparavant les atteintes à la protection des données. Ces réalisations existent, malgré une hausse des cyberattaques étatiques et non étatiques qui ont été lancées contre les réseaux du gouvernement du Canada au cours des dernières années.

Bien que Sécurité publique Canada ait entrepris de nombreuses activités visant à informer les Canadiens à propos de la cybersécurité, on ne sait pas dans quelle mesure ces activités ont contribué à renforcer la sécurité des Canadiens en ligne.

Étant donné ces constatations, l'évaluation a permis de relever un certain nombre de possibilités d'amélioration et de formuler plusieurs recommandations pour y donner suite. Par contre, comme cela a été mentionné précédemment, le gouvernement du Canada a entrepris, dans le cadre d'un processus parallèle (c.-à-d. les lettres de mandat des ministres), un examen exhaustif des mesures en place pour protéger les Canadiens et les infrastructures essentielles du Canada contre les cybermenaces. Ce processus devrait se traduire par une réforme de la Stratégie de cybersécurité du Canada visée par l'évaluation et il établira une nouvelle approche, plus globale pour aborder les questions de cybersécurité, notamment celles relevées dans l'évaluation.

Peu importe ce qui pourrait remplacer la Stratégie actuelle, du point de vue de la conception et de l'évaluation du programme, les principaux défis qui attendent les organismes participants pour la suite des choses consisteront à maintenir des réalisations obtenues jusqu'à maintenant, tout en continuant à renforcer la gouvernance horizontale, la reddition de compte et la surveillance de la performance pour faire en sorte que le Canada soit mieux préparé à maintenir sa posture de sécurité dans un contexte où les cybermenaces évoluent constamment et deviennent de plus en plus complexes. C'est dans ce contexte que les recommandations ci-dessus sont formulées aux fins d'examen.

5. RECOMMANDATIONS

En collaboration avec les organismes participants, la sous-ministre adjointe principale du Secteur de la sécurité et de la cybersécurité nationale de Sécurité publique Canada devrait envisager de prendre les mesures suivantes :

1) Renforcer la structure de gouvernance horizontale de la Stratégie de cybersécurité du Canada en :
    a) réévaluant la structure de gouvernance pour déterminer la nécessité et la demande en ce qui a trait à la configuration actuelle des comités et pour améliorer la participation;
    b) améliorant le soutien d'un secrétariat, notamment la coordination, la gestion de l'information et d'autres services administratifs;
    c) s'assurant que les comités de surveillance ont des mandats qui définissent clairement les rôles et les responsabilités des membres et les attentes envers ceux-ci;
    d) en s'assurant que les comités de surveillance s'acquittent des rôles et des responsabilités définis dans leur mandat;
    e) en rédigeant des comptes rendus de réunions de façon systématique.

2) Renforcer les pratiques d'échange de renseignements liés à la cybersécurité en élaborant des politiques et des procédures claires et concevoir des outils qui permettront un échange de renseignements systématique et opportun avec les partenaires et les intervenants.

3) Renforcer les pratiques de mesure du rendement et de collecte de données en :

   a) recueillant des renseignements pertinents, fiables et axés sur les résultats, y compris des renseignements sur les dépenses de programme, de façon régulière et méthodique; et

   b) fournissant les renseignements recueillis sur le rendement et les dépenses de façon constante aux comités de surveillance pour favoriser une surveillance efficace et la reddition de comptes.

6. RÉPONSE ET PLAN D'ACTION DE LA DIRECTION

En parallèle avec la présente évaluation, Sécurité publique Canada mène un examen complet de la cybersécurité, qui devrait aboutir au renouvellement de la stratégie de cybersécurité pour le gouvernement du Canada. Les recommandations de l'évaluation informeront l'élaboration de l'approche renouvelée en ce qui concerne :

- la gouvernance de la cybersécurité;
- l'échange d'information au sein du gouvernement fédéral et avec les partenaires externes; et
- les pratiques de mesure du rendement et de collecte de données.

Recommandation	Réponse de la direction	Mesures prévues	Date d'achèvement prévue
1. En collaboration avec les organismes participants, la sous-ministre adjointe principale du Secteur de la sécurité et de la cybersécurité nationale de Sécurité publique Canada devrait envisager de prendre les mesures suivantes : Renforcer la structure de gouvernance horizontale de la Stratégie de cybersécurité du Canada en procédant aux tâches suivantes : a) réévaluer la structure de gouvernance pour déterminer la	Acceptée	Dans le cadre du processus de renouvellement de la politique à la suite de l'examen du gouvernement du Canada sur la cybersécurité : a) envisager des options pour améliorer l'efficacité des mécanismes de gouvernance sur la cybersécurité au sein du gouvernement fédéral, notamment la configuration et la composition des comités; b) explorer les options pour formaliser le soutien aux	Octobre 2018

nécessité et la demande en ce qui a trait à la configuration actuelle des comités et pour améliorer la participation; b) améliorer le soutien du secrétariat, notamment la coordination, la gestion de l'information et d'autres services administratifs; c) s'assurer que les comités de surveillance ont des mandats qui définissent clairement les rôles et les responsabilités des membres et les attentes envers ceux-ci; d) s'assurer que les comités de surveillance s'acquittent des rôles et des responsabilités définis dans leur mandat; e) rédiger des comptes rendus de décision de façon systématique.		mécanismes de gouvernance interne, en portant une attention spéciale à la formalisation des communications et des pratiques de gestion de l'information; c) revoir le cadre de référence pour les comités sur la cybersécurité et l'adapter au besoin pour s'assurer que les rôles, les responsabilités et les attentes des participants soient clairs; d) explorer les mesures pour améliorer la responsabilisation dans la gouvernance fédérale de la cybersécurité; e) évaluer les options de tenue de documents pour tout mécanisme de gouvernance (par ex., procès-verbaux formalisés, comptes rendus des décisions).	
2. Renforcer les pratiques d'échange de renseignements liés à la cybersécurité en élaborant des politiques et des procédures claires et concevoir des outils qui permettront un échange de renseignements systématique et opportun avec les partenaires et les intervenants.	Acceptée	Explorer les options (politiques, procédures, outils) pour améliorer les pratiques de partage de l'information avec les partenaires (au sein du gouvernement fédéral) et avec les intervenants (entre le gouvernement et les partenaires externes).	Décembre 2017
3. Renforcer les pratiques de mesure du rendement et de collecte de données en procédant aux tâches suivantes : a) recueillir des renseignements pertinents, fiables et axés sur les résultats, y compris des renseignements sur les dépenses de programme, de façon régulière et méthodique; b) fournir les renseignements recueillis sur le rendement et les dépenses aux comités de surveillance	Acceptée	Mettre à jour la stratégie horizontale de mesure du rendement pour refléter les priorités d'une stratégie renouvelée sur la cybersécurité. a) S'assurer que les résultats déterminés dans la stratégie de mesure du rendement mise à jour soient atteignables et mesurables, et que les indicateurs du rendement soient pertinents. b) Veiller à ce que la mise en œuvre de la stratégie de mesure du rendement	Octobre 2018

pertinents de façon régulière pour favoriser un suivi efficace et la reddition de comptes.		comprenne des rapports périodiques à un organisme de surveillance (par ex., comité sur la cybersécurité ou mécanisme comparable)	

ANNEXE A – RÔLES ET RESPONSABILITÉS [39]

Ministère	Rôles et responsabilités		
	Pilier 1	**Pilier 2**	**Pilier 3**
SP	Diriger et coordonner la mise en œuvre de la Stratégie, y compris la conception de l'approche globale de la mesure du rendement et des rapports connexes.	-Diriger et coordonner la mobilisation avec les provinces et les territoires, le secteur privé, le gouvernement du Canada et les intervenants internationaux. -Établir des liens avec des experts de la cybersécurité du milieu universitaire.	Diriger et coordonner les activités de sensibilisation de la population visant à informer les Canadiens des risques auxquels ils sont exposés et des mesures qu'ils peuvent prendre pour se protéger et protéger leur famille dans le cyberespace.
CSTC	-Surveiller les réseaux du gouvernement du Canada et en assurer la défense en détectant les cybermenaces complexes contre le gouvernement, en intervenant, et en offrant aux ministères des conseils pour les aider à atténuer les répercussions de ces menaces ou pour se rétablir après coup. -Collecter et analyser les renseignements étrangers, produire des rapports connexes, et agir comme point de contact pour le Canada auprès de la collectivité cryptologique du Groupe des cinq. -Effectuer des recherches et mettre sur pied des projets classifiés dans le domaine de la cybersécurité. -Fournir des connaissances spécialisées et des conseils techniques sur la conception de l'architecture et sur la façon de choisir et d'utiliser convenablement les produits de sécurité liés aux TI. -Offrir des programmes de formation et de sensibilisation sur la sécurité des TI à tous les professionnels de la sécurité des TI du gouvernement du	-Engager, coordonner et échanger des informations afin d'améliorer la collaboration nationale et internationale en matière de cybersécurité. -Partenaire avec le secteur privé pour renforcer la résilience cybersécurité du Canada et aider à sécuriser l'infrastructure essentielle d'importance pour le gouvernement du Canada.	

[39] L'information compilée dans ce tableau est tirée de nombreux documents, y compris la Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité, pages 9 à 13 (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf), ainsi que le document intitulé *Measuring the Performance of Canada's Cyber Security Strategy*, page 11.

Ministère	Rôles et responsabilités		
	Pilier 1	**Pilier 2**	**Pilier 3**
	Canada et à d'autres employés.		
SPC	- À titre d'équipe d'intervention en cas d'incident informatique du gouvernement du Canada, protéger l'infrastructure de TI du gouvernement du Canada en coordonnant l'intervention en cas d'incidents, ainsi qu'en produisant et diffusant des produits de sensibilisation. -Protéger l'infrastructure de TI gérée par SPC en surveillant et détectant les cybermenaces, et en intervenant à ce chapitre. Offrir aux ministères des conseils et une orientation afin de les aider à atténuer les répercussions de ces menaces ou à se rétablir des cyberincidents. -Veiller à ce que seuls des produits et des services de TI de confiance soient achetés et déployés sur l'infrastructure de TI de SPC au moyen d'un programme d'intégrité de la chaîne d'approvisionnement complet et d'une remise en état des produits compromis qui sont en fonction. -Soutenir le gouvernement du Canada comme fournisseur de services chargé de la consolidation et de la modernisation de l'infrastructure de TI en produits et services de TI de catégorie professionnelle qui sont fiables et sécuritaires. -Appuyer les partenaires de la cybersécurité du gouvernement du Canada dans le cadre de la mise en œuvre des stratégies horizontales de cybersécurité.		
MDN/RDDC	Appuyer les activités en matière de recherche et de développement sur la cybersécurité. • en effectuant la conception et la mise en œuvre d'un cadre d'architecture d'entreprise cybernétique; • en créant une cybertaxonomie commune dans un Wikipédia commun (GCPedia) aux fins d'interopérabilité;	Appuyer les activités en matière de recherche et de développement sur la cybersécurité.	

Ministère	Rôles et responsabilités		
	Pilier 1	**Pilier 2**	**Pilier 3**
	• en élaborer les énoncés qui définissent les problèmes et en faisant l'analyse des liens entre les menaces, la vulnérabilité, les risques et les lacunes des capacités; • en produisant un rapport sur les pratiques exemplaires; • en produisant un rapport sur les nouvelles approches à l'égard de solutions novatrices.		
SCT	Élaborer et superviser une approche pangouvernementale en matière de cybersécurité, notamment : • en établissant une orientation pangouvernementale et les priorités à respecter pour assurer la sécurité des réseaux et des systèmes gouvernementaux de la TI; • en fournissant une orientation et des conseils à l'intention des organismes-chefs de file en matière de sécurité pour les aider à mettre en œuvre les démarches et les mesures qui s'imposent pour gérer les incidents de sécurité touchant la TI; • en prévoyant une surveillance de la gestion des incidents touchant la TI, ce qui comprend les analyses rétrospectives et les leçons tirées.		
SCRS	-Mener des enquêtes de sécurité nationale. -Signaler au gouvernement du Canada les activités constituant une menace contre la sécurité du Canada aux termes de la *Loi sur le Service canadien du renseignement de sécurité*, et lui offrir des conseils à cet égard. -Aider le gouvernement du Canada à comprendre les cybermenaces ainsi que les intentions et les capacités des agents cybernétiques menant leurs activités au Canada et à l'étranger et constituant une menace pour la sécurité de notre pays. Grâce à ces renseignements, le	-Mener des enquêtes de sécurité nationale. -Signaler au gouvernement du Canada les activités constituant une menace contre la sécurité du Canada aux termes de la *Loi sur le Service canadien du renseignement de sécurité*, et lui offrir des conseils à cet égard. -Aider le gouvernement du Canada à comprendre les cybermenaces ainsi que les intentions et les capacités des agents cybernétiques menant leurs activités au Canada et à l'étranger et constituant une menace pour la sécurité de notre pays. Grâce à ces	

Ministère	Rôles et responsabilités		
	Pilier 1	**Pilier 2**	**Pilier 3**
	gouvernement du Canada peut améliorer sa connaissance générale de la situation, cerner les vulnérabilités cybernétiques, empêcher les actes d'espionnage cybernétique et les autres cybermenaces et prendre des mesures pour protéger ses infrastructures essentielles.	renseignements, le gouvernement du Canada peut améliorer sa connaissance générale de la situation, cerner les vulnérabilités cybernétiques, empêcher les actes d'espionnage cybernétique et les autres cybermenaces et prendre des mesures pour protéger ses infrastructures essentielles. -Établir une liaison directe avec le secteur privé et offrir aux exploitants d'infrastructures essentielles des séances de sensibilisation portant sur les cybermenaces complexes et persistantes dans le but d'augmenter la collecte de renseignements.	
AMC		-Participer à la cybersécurité à l'échelle internationale. -Participer, au moyen d'activités diplomatiques bilatérales et multilatérales, au façonnement de l'environnement stratégique international en ce qui a trait au cyberespace, notamment par la promotion de l'applicabilité du droit international dans le cyberespace, la promotion des normes de comportement des États dans le cyberespace et l'élaboration de mesures de confiance visant à réduire les risques de conflits. -Élaborer une politique étrangère sur la cybersécurité pour renforcer la cohérence des activités liées à la cybersécurité menées à l'étranger par le gouvernement du Canada. -Aider les partenaires internationaux à se protéger eux-mêmes contre les cybermenaces.	
JUS		-Fournir des conseils juridiques à tous les ministères concernés au sein du gouvernement du Canada, au besoin. -Représenter le Canada dans le cadre de forums internationaux et fédéraux-provinciaux-territoriaux.	

Ministère	Rôles et responsabilités		
	Pilier 1	**Pilier 2**	**Pilier 3**
GRC			-Établir un centre de fusionnement afin d'améliorer l'évaluation des incidents cybernétiques d'origine criminelle, donnant au gouvernement du Canada une compréhension plus globale des menaces et des risques en la matière. -Élaborer une stratégie de lutte contre la cybercriminalité, y compris la fraude, le crime organisé et le vol d'identité. -Publier un rapport annuel sur la cybercriminalité portant sur les incidents et les tendances émergentes.

ANNEXE B – QUESTIONS DE L'ÉVALUATON

Gouvernance
1. Dans quelle mesure la structure de gouvernance horizontale a-t-elle été efficace?
2. Les rôles et les responsabilités des différents partenaires ont-ils été bien définis et respectés?
3. Quel est le degré de collaboration, de coordination et d'échange de renseignements entre les partenaires?
RENDEMENT – MISE EN ŒUVRE
4. Dans quelle mesure les activités financées ont-elles été mises en œuvre?
RENDEMENT – EFFICACITÉ
5. Dans quelle mesure des progrès ont-ils été accomplis au chapitre de la protection des systèmes du gouvernement du Canada et du renforcement de la capacité à : a. prévenir les cyberincidents; b. détecter et combattre les cybermenaces; c. intervenir en cas de cyberincidents et se rétablir?
6. Quels progrès ont été réalisés pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement du Canada ?
7. Quel est le degré de collaboration nationale et internationale en ce qui touche la cybersécurité?
8. Dans quelle mesure les Canadiens sont-ils mieux protégés en ligne? a. Dans quelle mesure les campagnes de sensibilisation ont-elles permis aux Canadiens de mieux comprendre les menaces en ligne? b. Dans quelle mesure les organismes d'exécution de la loi sont-ils plus au courant des tendances en matière de cybercriminalité? c. Quels progrès ont été accomplis dans le cadre de l'élaboration de politiques et de règlements en matière de cybercriminalité?
RENDEMENT – EFFICIENCE ET ÉCONOMIE
9. Dans quelle mesure le financement a-t-il été utilisé aux fins prévues?
10. Quelle est la valeur obtenue à la suite des investissements?
11. Existe-t-il d'autres méthodes pouvant offrir une plus grande optimisation des ressources?
12. Existe-t-il des leçons apprises, y compris celles d'autres pays aux vues similaires, qui pourraient être appliquées dans le contexte canadien?