Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques

Présenté au premier ministre le 11 août, 2021 en vertu du paragraphe 21(1) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*
(Version révisée selon le paragraphe 21(5) de la *Loi sur le CPSRN)*

Canada

Ottawa, ON

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques (version révisée conformément au paragraphe 21(5) de la Loi sur le CPSNR)
CP104-3/2022F (Imprimé)
ISBN 978-0-660-4 1356-3 (Imprimé)

CP104-3/2022F-PDF (En ligne)
ISBN 978-0-660-41355-6 (En ligne)

Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques

Comité des parlementaires sur la sécurité nationale et le renseignement

L'honorable David McGuinty, C.P., député
Président

Présenté au premier ministre le 11 août 2021
Version révisée présentée au Parlement en février 2022

Révisions

En application du paragraphe 21(2) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Loi sur le CPSNR), le Comité peut présenter un rapport spécial au premier ministre et aux ministres concernés sur toute question liée à son mandat. Conformément au paragraphe 21(5) de la Loi sur le CPSNR, le premier ministre peut, après consultation du président du Comité, ordonner au Comité de lui présenter un rapport révisé qui ne contient pas de renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales, ou qui sont protégés par le secret professionnel de l'avocat, selon le premier ministre.

Le présent document constitue une version révisée du Rapport spécial fourni au premier ministre le 11 août 2021. À ce moment, le document était classifié Très secret//Renseignement spécial//Réservé aux Canadiens. Les révisions ont été apportées de façon à retirer l'information dont la communication, selon le premier ministre, porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales ou qui est protégée par le secret professionnel de l'avocat. Lorsque la suppression n'affecte pas la lisibilité du texte, le Comité a signalé la suppression par trois astérisques (***) dans le texte du présent document. À l'inverse, le Comité a révisé le document pour résumer l'information retirée. Ces passages sont signalés par trois astérisques au début et à la fin du résumé et sont placés entre crochets (voir l'exemple ci-dessous).

EXEMPLE: [*** Les passages révisés sont signalés par trois astérisques en début et en fin de phrase, et le résumé est placé entre crochets. ***]

LE COMITÉ DES PARLEMENTAIRES SUR LA SÉCURITÉ NATIONALE ET LE RENSEIGNEMENT

L'honorable David McGuinty, C.P., député (président)

Madame Leona Alleslev, députée

Monsieur Stéphane Bergeron, député

Monsieur Don Davies, député

L'honorable Dennis Dawson, C. P., sénateur

Monsieur Ted Falk, député
(a démissionné le 15 juin 2021)

Monsieur Peter Fragiskatos, député

Madame Iqra Khalid, députée

L'honorable Frances Lankin, C.P, C.M., sénatrice

Monsieur Rob Morrison, député

Monsieur Glen Motz, M.O.M., député
(a démissionné le 15 juin 2021)

Madame Jennifer O'Connell, députée
(a démissionné le 19 mars 2021)

Madame Brenda Shanahan, députée

L'honorable Vernon White, C.P., sénateur

National Security and Intelligence Committee of Parliamentarians

Comité des parlementaires sur la sécurité nationale et le renseignement

Chair

Président

Le 8 février 2022

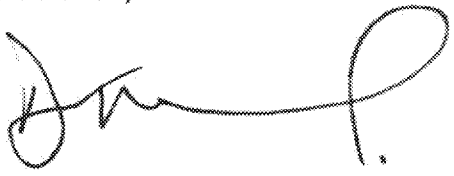
Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureau du premier ministre et du Conseil privé
Ottawa (Ontario)
K1A 0A2

Monsieur le Premier Ministre,

Au nom du Comité des parlementaires sur la sécurité nationale et le renseignement, je suis heureux de vous présenter le Rapport spécial sur le cadre et les activités du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques. Le rapport unanime comprend quatre conclusions et deux recommandations visant à renforcer le cadre du gouvernement pour défendre ses systèmes et ses réseaux contre les cyberattaques et à étendre ce cadre au plus grand nombre d'organisations fédérales possible.

Conformément au paragraphe 21(5) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, le rapport spécial a été modifié pour en retirer les renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales, ou les renseignements protégés par le secret professionnel de l'avocat.

Je vous prie d'agréer, Monsieur le Premier Ministre, l'expression de ma très haute considération,



L'honorable David McGuinty, C.P., député
Président
Comité des parlementaires sur la sécurité nationale et le renseignement

Table des matières

Introduction

Au début de mars 2021, les administrations et les organisations du monde ont pris connaissance de cyberattaques ciblant une vulnérabilité auparavant inconnue dans les systèmes de courriel Microsoft Exchange. Ces attaques attribuées à la Chine ont ciblé les communications par courriel des organisations visées et servaient à obtenir un accès continu aux réseaux des victimes. Alors que l'attaque s'est répandue, d'autres auteurs de menace perfectionnés ont rapidement tiré avantage de la vulnérabilité, et des centaines de milliers d'organisations ont été touchées. Au Canada, le gouvernement a immédiatement déclaré qu'il s'agissait d'un événement de cybersécurité et trois organisations — le Secrétariat du Conseil du Trésor du Canada (SCT), Services partagés Canada (SPC) et le Centre canadien pour la cybersécurité (CCC) — ont travaillé avec les ministères pour déterminer leurs vulnérabilités et leur ont ordonné de déployer les correctifs nécessaires pour leurs systèmes. Le CCC a aussi averti des centaines d'organisations du secteur privé de la possible vulnérabilité. En quelques jours, les organisations touchées ont apporté les changements requis et un seul ministère a été touché. En date de juin 2021, aucune organisation fédérale n'a perdu de données à la suite de l'attaque[1].

De façon générale, le gouvernement a réussi à défendre rapidement et efficacement ses réseaux d'une vulnérabilité grave et auparavant inconnue. Comment le gouvernement en est-il arrivé là? Quels obstacles lui reste-t-il à surmonter? Le gouvernement est-il prêt à lutter contre les cybermenaces de l'avenir? Le présent examen s'efforce de répondre à ces questions.

1. Les cybermenaces représentent un risque considérable et omniprésent pour la sécurité nationale du Canada. Elles touchent les Canadiens sur différents plans, menaçant les systèmes et services gouvernementaux, les fournisseurs de services essentiels, les systèmes financiers et de la santé, les réseaux des universitaires et de recherche, et les renseignements personnels sensibles. Les gouvernements sont des cibles attrayantes pour les cyberattaques. Le gouvernement fédéral détient une quantité énorme de données sur les Canadiens, les entreprises et les secteurs de l'innovation du Canada comme les universités et les instituts de recherche. Les cybercompromissions de ces données pourraient révéler des renseignements personnels sensibles de Canadiens et miner la vitalité d'entreprises précises et de l'économie. Le gouvernement gère aussi des relations de sécurité, de commerce et avec l'étranger par l'entremise d'infrastructures électroniques qui, si elles sont compromises, pourraient porter atteinte aux politiques du gouvernement et mettre en péril les intérêts vitaux du Canada. De plus, le gouvernement fournit de nombreux services essentiels qui dépendent grandement d'infrastructures électroniques solides et sans échec.

---

[1] Krebs on Security, « At least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software », 5 mars 2021, https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/; CST, « NSICOP Cyber Defence Review. Compromise of Microsoft Exchange », courriel au Secrétariat du CPSNR, 27 mai 2021; Affaires mondiales Canada, « Déclaration sur les campagnes cybernétiques de la Chine », 19 juillet 2021, https://www.canada.ca/fr/affaires-mondiales/nouvelles/2021/07/declaration-sur-les-campagnes-cybernetiques-de-la-chine.html.

2. Depuis sa création, le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité) s'intéresse à la sécurité des systèmes gouvernementaux. Ces systèmes sont au cœur de l'infrastructure essentielle du Canada et font partie intégrante de la sécurité nationale. Les ministères ont maintes fois renseigné le Comité sur les types de cybermenaces qui pèsent sur le Canada, et le Comité a résumé ces menaces dans son Rapport annuel 2018 au premier ministre, puis plus en détail dans son Rapport annuel 2020. Il exprime ses préoccupations concernant l'omniprésence des cybermenaces et, en particulier, la complexité et la constance des menaces que représentent plusieurs acteurs étrangers étatiques et non étatiques, y compris la menace grandissante du rançongiciel. Il reconnaît aussi l'ampleur des changements que le gouvernement a apportés au cours des dernières décennies, y compris l'ajout ou la mise à jour de pouvoirs, la création de nouvelles organisations et de nouveaux programmes, et des investissements considérables dans la cybersécurité et la cyberdéfense. En fait, le Comité a reporté la tenue d'un examen sur des questions de cybersécurité en 2018 afin d'éviter d'avoir des effets défavorables sur la mise en œuvre de changements récemment annoncés à l'appareil gouvernemental, notamment la création du Centre canadien pour la cybersécurité et les changements inhérents dans les rôles et les responsabilités de Services partagés Canada et de Sécurité publique Canada.

3. La cybersécurité est un domaine vaste et complexe. Dans la Stratégie nationale de cybersécurité de 2018, le gouvernement a défini la cybersécurité comme étant « la protection de l'information numérique et de l'infrastructure sur laquelle elle repose[2]. » Une telle définition forcément extensive implique un éventail d'acteurs de l'industrie, du monde universitaire et du gouvernement, et peut englober n'importe quoi allant de l'approvisionnement de matériel, de logiciels et de services, à l'élaboration de lois et de règlements. Même si ces domaines sont essentiels en soi, bon nombre d'entre eux n'ont aucun lien ou presque avec les enjeux de sécurité et du renseignement, qui sont au cœur du mandat d'examen du Comité.

4. Le Comité a donc décidé d'entreprendre l'examen d'un sous-ensemble précis des activités de cybersécurité : la cyberdéfense. On peut définir la cyberdéfense comme la capacité technique de repérer et de détecter des cyberincidents, et d'élaborer et de déployer des contre-mesures pour les enrayer[3]. Au Canada, le Centre de la sécurité des télécommunications (CST) est l'organisation principale chargée du développement et du déploiement d'activités de cyberdéfense. Ses efforts ont été facilités par son rôle complémentaire en tant qu'organisation responsable du renseignement électromagnétique au Canada. En effet, ce rôle lui a permis d'être informé des activités et des tactiques des cyberacteurs les plus avancés, particulièrement les états étrangers possédant les ressources et les moyens de préparer des attaques persistantes et d'avant-garde sur le plan technique contre des systèmes et des réseaux cibles (ces acteurs sont considérés comme étant des menaces persistantes avancées). Le CST s'est servi de l'information obtenue pour concevoir des capteurs de cyberdéfense et des technologies de défense sur mesure qui peuvent repérer et contrecarrer de telles menaces, que les

[2] Canada, *Stratégie nationale de cybersécurité*, 2018, p. 9.
[3] Canada, *Progress Report on the Cyber Security Strategy*, sans date, p. 9. La référence originale se rapporte au « réseau de défense ».

technologies commerciales ne peuvent pas déjouer. Les changements fondamentaux aux pouvoirs dérivés de la loi ont été au centre de la capacité du CST de monter ses opérations et de les adapter à l'évolution rapide de la technologie. Le premier changement important a eu lieu en 2001 par l'adoption de modifications à la *Loi sur la défense nationale*, qui a créé le fondement légal des activités du CST liées à la sécurité des technologies de l'information et au renseignement électromagnétique étranger. En 2019, la *Loi sur le Centre de la sécurité des télécommunications* est entrée en vigueur, et a précisé et élargi ces pouvoirs. Le présent rapport explique cette évolution.

5. Le cadre de la cyberdéfense comprend deux autres grands acteurs : Services partagés Canada et le Conseil du Trésor, soutenu par le Secrétariat du Conseil du Trésor du Canada. Créé en 2011, Services partagés Canada (SPC) joue plutôt un rôle opérationnel. SPC offre aux ministères trois services essentiels — réseaux, courriels et centres de données — et collabore étroitement avec le CST pour agir face aux cyberincidents graves. Lorsque SPC a été créé, 43 ministères devaient se procurer ses services, ce qui représentait environ 95 pour cent des dépenses liées à l'infrastructure de la technologie de l'information du gouvernement; les autres ministères et organismes plus petits représentaient les 5 pour cent restants. Ces 43 partenaires originaux continuent de recevoir tous les services de SPC, y compris ceux liés à la cybersécurité. Au fil du temps, 117 autres organisations fédérales ont choisi d'obtenir certains de ces services, faisant passer le nombre total d'organisations qui reçoivent les services de SPC à 160 des 169 organisations, soit 95 pour cent de toutes les organisations fédérales.

6. Le rôle que joue SPC dans la cyberdéfense est essentiel dans deux mesures. Premièrement, le gouvernement a réduit sa vulnérabilité à toutes les formes de cyberattaques en groupant le nombre de points de connexion entre les réseaux du gouvernement et Internet et en réduisant le nombre de centres de données patrimoniales. Deuxièmement, le gouvernement a grandement diminué la probabilité de la réussite de cyberattaques, et leurs dommages possibles s'il y a lieu, en plaçant la majorité des organisations fédérales (c'est-à-dire celles qui reçoivent les services de SPC) sous la zone de couverture des capteurs et des systèmes de cyberdéfense perfectionnés du CST.

7. Le Conseil du Trésor et son Secrétariat jouent un rôle prédominant dans la cyberdéfense, tant comme dirigeant principal de l'information du gouvernement, que par l'entremise de directives et de politiques applicables à tous les ministères. Le Conseil du Trésor et son Secrétariat sont habilités à créer des politiques au titre de différents textes législatifs, plus particulièrement la *Loi sur la gestion des finances publiques* (LGFP). D'abord adoptée en 1985, la LGFP définit les rôles et les responsabilités de certains acteurs clés dans l'ensemble du gouvernement et permet au Conseil du Trésor de publier des politiques, des directives, des normes et des lignes directrices relatives à la gestion et à l'administration des entités fédérales. Conformément au système parlementaire du Canada, la LGFP comporte une structure d'autorité verticale : chaque ministre et les administrateurs généraux sont responsables des activités de chaque ministère.

8. Les instruments politiques promulgués au titre de la LGFP sont fondamentaux pour la cyberdéfense. Ils précisent les rôles et les obligations de responsabilisation de différents ministères, donnent une orientation et définissent les exigences. Les instruments les plus importants comprennent la Politique sur la sécurité du gouvernement, la Politique sur les services et le numérique, le Plan stratégique des opérations numériques, la Stratégie d'adoption de l'informatique en nuage, et le Plan de gestion des événements de cybersécurité. Ils définissent le cadre des cyberactivités de sécurité et de défense. Comme toutes les directives du Conseil du Trésor, le SCT estime que la mise en œuvre des instruments liés à la cyberdéfense est « obligatoire ». Cela dit, conformément aux pouvoirs verticaux de la LGFP, les administrateurs généraux de chaque ministère sont en définitive responsables de veiller à l'intégrité et à la sécurité de leurs systèmes et réseaux électroniques et à la mise en œuvre des directives du SCT. Pour intervenir face aux cas de non-conformité, le Conseil du Trésor a mis en place un cadre stratégique sur la gestion de la conformité, qui comprend un éventail de conséquences administratives[4].

9. D'autres pouvoirs jouent un rôle plus précis dans le cadre de cyberdéfense. Les changements apportés aux pouvoirs du CST en 2001 et en 2019 ont permis à l'organisation de créer un secteur d'activités qui s'est révélé crucial à la cyberdéfense du Canada. Il ne faut pas oublier les modifications apportées en 2004 au *Code criminel* et à la LGFP pour préciser de quelle manière les organisations gouvernementales sont habilitées à protéger leurs propres cybersystèmes. Le présent examen résume l'évolution de ces pouvoirs et instruments et le rôle qu'ils jouent dans le domaine de la cyberdéfense.

10. Enfin, le gouvernement a fourni une orientation clé stratégique, apporté d'importants changements structurels et investi des ressources considérables pour renforcer sa cybersécurité et ses moyens de cyberdéfense. En effet, le gouvernement a fourni une orientation stratégique dans les domaines de la cybersécurité et de la cyberdéfense par l'entremise de la Politique de sécurité nationale de 2004, de la Stratégie de cybersécurité de 2010 et de la Stratégie nationale de cybersécurité de 2018. Il a apporté des changements considérables à la structure du gouvernement, notamment en créant SPC en 2011 et le CCC en 2018. Bon nombre de ces changements ont demandé des investissements importants : au total, entre 2010 et 2021, le gouvernement a investi plus de 6 milliards de dollars dans la défense de ses réseaux contre les cyberattaques[5]. Le présent rapport décrit les différents changements apportés par le gouvernement au cours des deux dernières décennies et présente des recommandations quant aux efforts à réaliser pour terminer ce travail, y compris en ce qui a trait aux pouvoirs gouvernementaux.

---

[4] Conseil du Trésor, « Cadre stratégique sur la gestion de la conformité », 2009, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=17151.

[5] Canada, *Budget 2021* (chapitres 9 et 10), https://www.budget.gc.ca/2021/report-rapport/toc-tdm-fr.html; Budget 2019, https://www.budget.gc.ca/2019/docs/plan/chap-04-fr.html#Partie-4-Securite-publique-et-justice; Budget 2018, https://www.budget.gc.ca/2018/docs/plan/chap-04-fr.html#Assurer-la-securite-et-la-prosperite-a-l-ere-numerique; Budget 2016, https://www.budget.gc.ca/2016/docs/plan/ch5-fr.html#_Toc446176081; et Sécurité publique Canada, *Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date*, 2015.

Aperçu de l'examen

11. Le 19 juin 2020, le Comité a décidé d'entreprendre un examen du cadre et des activités du gouvernement du Canada pour défendre ses systèmes et réseaux contre les cyberattaques. Le 6 juillet 2020, le président du Comité a envoyé des lettres de notification aux ministres de la Défense nationale et de la Sécurité publique et de la Protection civile ainsi qu'au président du Conseil du Trésor. L'examen comprenait les organisations qui suivent :

- le Centre de la sécurité des télécommunications;
- Services partagés Canada;
- le Secrétariat du Conseil du Trésor du Canada;
- Sécurité publique Canada.

12. Le Comité a informé les ministres que l'examen porterait sur le cadre fédéral de la cyberdéfense, les activités qui constituent la cyberdéfense pour le gouvernement et les pouvoirs et les structures de gouvernance, y compris la gouvernance et la coordination interministérielles au titre desquelles elles sont menées. Les objectifs de l'examen seraient :

- d'étudier l'évolution des cadres législatif, réglementaire, politique, opérationnel, administratif ou financier associés à la tenue des activités de cyberdéfense;
- de définir le type, la nature et l'étendue des activités qui constituent la cyberdéfense pour le gouvernement et la menace en évolution qu'elle vise à contrer;
- d'examiner l'évolution des structures de pouvoir, de responsabilisation et de gouvernance pour les activités de cyberdéfense, y compris la gouvernance et la coordination interministérielles;
- de définir les systèmes et les réseaux qui constituent les systèmes de technologie de l'information du gouvernement;
- d'examiner les études de cas pertinentes relatives à la cybercompromission des systèmes gouvernementaux;
- de se pencher sur les risques découlant des activités de cyberdéfense (p. ex. les droits des Canadiens en matière de protection des renseignements personnels).

13. Le Comité a concentré sa recherche sur la défense des systèmes du gouvernement fédéral contre les cyberattaques, un domaine d'examen qui convient parfaitement à son mandat défini dans la loi. Ce faisant, le Comité a exclu plusieurs enjeux de la portée de son examen. Il n'a pas examiné les activités de cyberdéfense liées à la protection des infrastructures essentielles à l'extérieur des systèmes du gouvernement fédéral (p. ex. d'autres paliers gouvernementaux ou des secteurs comme celui de l'énergie). La protection des infrastructures essentielles est un sujet large et complexe en soi, sur lequel le Comité pourrait se pencher ultérieurement. Il n'a pas examiné les activités du gouvernement liées à la défense des élections fédérales de 2019 contre les cybermenaces. Le gouvernement avait déjà entamé un rapport à ce sujet au moment où le Comité a annoncé son examen. Lorsque le Comité a reçu ce rapport en 2020, il a présenté des commentaires et des recommandations au premier

ministre. Enfin, le Comité n'a pas examiné la réponse du gouvernement à la cybercriminalité : la Gendarmerie royale du Canada (GRC), l'une des organisations centrales de la sécurité et du renseignement pouvant faire l'objet d'un examen du Comité, était en train de mettre en œuvre d'importants changements dans sa façon de mener des enquêtes sur les cybercrimes. De plus, dans l'ensemble, la cybercriminalité ne s'inscrit pas dans le mandat d'examen du Comité.

14. Le Comité a étudié une quantité importante de documentation historique de 2001 jusqu'à présent, principalement pour explorer l'évolution de la compréhension du gouvernement sur les cybermenaces et les moyens et ressources nécessaires pour y faire face. Le Comité a centré son analyse sur des périodes clés où des incidents majeurs ont forcé des ministères à réorienter leurs opérations et où le gouvernement a adopté des lois habilitantes ou a apporté des changements à sa structure pour mener une action concernant les obstacles en matière de cyberdéfense. Dans la même ligne que ses examens antérieurs, le Comité a mis un accent considérable sur la responsabilisation, les pouvoirs, et la gouvernance et la coordination des activités.

15. L'examen du Comité s'est déroulé en deux étapes. La première était un examen des documents gouvernementaux qui décrivent l'évolution des réponses aux menaces nouvelles et émergentes. Le Comité a complété ces documents avec des sources d'information universitaires et publiques, mais il a été limité dans les discussions qu'il pouvait tenir avec des experts à l'extérieur du gouvernement en raison de la pandémie. La deuxième étape était de tenir des séances de breffage et des audiences avec des représentants du gouvernement. Le Secrétariat du Comité a travaillé étroitement avec les ministères en question pour obtenir de l'information et la préciser. Au total, le Comité a tenu cinq réunions avec différents ministères et a consulté plus de 2 500 documents, représentant plus de 37 000 pages de documentation.

16. Le présent rapport se compose de cinq parties. La première est une description des cybermenaces qui pèsent sur le gouvernement et un examen des enjeux découlant d'une attaque contre les réseaux du gouvernement par des auteurs de cybermenace. La deuxième est une description historique de l'évolution du cadre du gouvernement pour défendre ses réseaux depuis 2001. Cette partie explique l'importance des pouvoirs dérivés de la loi dans les fondements des activités de cyberdéfense, le rôle de différentes politiques du gouvernement, particulièrement les stratégies successives en matière de cybersécurité, et les principaux changements dans la structure du gouvernement, notamment la création de Services partagés Canada en 2011 et du Centre canadien pour la cybersécurité (CCC) en 2018. La troisième partie porte sur les rôles, les responsabilités, les pouvoirs et les activités des principaux partenaires dans le cadre de cyberdéfense du gouvernement : le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications, connus ensemble comme le groupe tripartite sur la sécurité des technologies de l'information. La quatrième partie décrit le cadre de gouvernance qui englobe les activités de cyberdéfense au gouvernement. Finalement, le Comité présente son évaluation, ses conclusions et ses recommandations.

17. Dans cette dernière section, le Comité souligne que le cadre de cyberdéfense du gouvernement a évolué au fil du temps vers une approche « d'entreprise » horizontale qui traite les systèmes et les réseaux du gouvernement comme étant une seule entité. Ces dix dernières années ont montré que cette évolution a grandement amélioré les moyens de cyberdéfense du Canada. Toutefois, le Canada ne peut pas baisser la garde : le gouvernement doit continuer de mettre en œuvre les mesures nécessaires pour s'adapter aux changements. Particulièrement, l'approche horizontale à la cyberdéfense concorde de moins en moins avec les pouvoirs verticaux des ministères, où les différentes organisations et sociétés d'État conservent une certaine latitude à savoir s'ils adhèrent au cadre de cyberdéfense du gouvernement ou s'ils font les changements nécessaires pour protéger leurs systèmes des menaces complexes. Ces pouvoirs ont été établis avant l'ère numérique et doivent être mis à jour pour tenir compte des nouvelles technologies et menaces.

Examens des activités de cyberdéfense réalisés

Examens externes

18. Plusieurs examens, audits et évaluations ont été menés sur des aspects du cadre de cyberdéfense du gouvernement. Ils ont tous été réalisés par des organes d'examen ou d'audit indépendants et externes, des comités parlementaires, le commissaire du CST (l'ancien organisme consacré à l'examen des activités du CST) et des organismes internes du gouvernement. Comme toile de fond à l'examen du Comité, la présente section résume chacun d'entre eux, à tour de rôle. La mise en œuvre des recommandations formulées dans ces examens n'a pas été vérifiée dans le cadre du présent examen.

19. Les examens ou audits externes suivants contenaient des références précises à la protection des systèmes d'information du gouvernement contre les cybermenaces.

- **Bureau du vérificateur général du Canada — Chapitre 3 : Protéger l'infrastructure essentielle contre les cybermenaces (2012) :** Une partie de cet audit examinait la façon dont le gouvernement protège ses systèmes d'information et les rôles et responsabilités des ministères touchés. On y recommandait que le Secrétariat du Conseil du Trésor du Canada mette à jour les politiques pertinentes afin de tenir compte des nouveaux rôles et des nouvelles responsabilités de Services partagés Canada (SPC) concernant la sécurité de l'information[6].
- **Bureau du vérificateur général du Canada — Rapport 4 : Services partagés en technologies de l'information (2015) :** Cet audit portait sur la façon dont SPC fournit des services de technologie de l'information à d'autres ministères, y compris la sécurité des technologies de l'information. On y recommandait que SPC définisse les attentes ou fournisse de l'information sur des éléments centraux de la sécurité aux partenaires afin qu'ils puissent se conformer aux politiques, aux lignes directrices et aux normes du gouvernement en matière de sécurité des technologies de l'information[7].
- **Comité sénatorial permanent des banques et du commerce – Les cyberattaques : Elles devraient vous empêcher de fermer l'œil (2018) :** Ce rapport examinait principalement la façon d'améliorer la cybersécurité pour les Canadiens et les entreprises. Cependant, il s'est aussi penché sur la façon d'améliorer le cadre de cybersécurité du gouvernement et de renforcer la surveillance des nombreux ministères dont la cybersécurité fait partie du mandat. Dans le rapport, on recommandait la création d'un ministre fédéral de la cybersécurité qui serait responsable de la politique entourant

[6] Bureau du vérificateur général du Canada (BVG), Automne 2012, *Chapitre 3 : Protéger l'infrastructure essentielle contre les cybermenaces*, 2012, https://publications.gc.ca/site/fra/9.604725/publication.html.
[7] BVG, Automne 2015, *Rapport 4 : Services partagés en technologies de l'information*, 2015, https://www.oag-bvg.gc.ca/internet/francais/parl_oag_201604_04_f_41061.html.

la cybersécurité au Canada et qui coordonnerait les efforts en matière de cybersécurité avec les gouvernements provinciaux et territoriaux et le secteur privé[8].

Le commissaire du CST

20. Entre 1996 et 2019, le commissaire du CST avait pour mandat d'examiner les activités du CST pour en vérifier la conformité avec les lois ainsi qu'avec les orientations politiques prescrites par le ministre de la Défense nationale. Dans le rapport final qu'il a déposé en 2019, le commissaire a rapporté que le CST avait agréé et mis en œuvre 166 des 175 recommandations formulées depuis 1997 relativement aux divers volets du mandat du CST, ce qui représente un taux de mise en œuvre de 95 %. Entre 2001 et 2019, le commissaire du CST a réalisé un certain nombre d'examens des activités de cyberdéfense du CST, lesquelles étaient désignées par diverses appellations, notamment tests actifs de sécurité réseau, évaluation de la posture de sécurité, opérations de cyberdéfense et activités de sécurité des technologies de l'information. En résumé, le commissaire du CST a examiné les programmes d'activités ou les divers aspects des activités du CST en matière de cyberdéfense, et ce, dans le but de vérifier si :

- les autorisations ministérielles pour les activités de cyberdéfense répondaient aux conditions énoncées dans la *Loi sur la défense nationale*;
- les activités de cyberdéfense avaient été menées conformément aux exigences législatives, ministérielles et stratégiques;
- le CST avait dirigé ses activités de cyberdéfense contre des Canadiens ou des personnes se trouvant au Canada;
- les communications privées interceptées par le CST étaient vraiment essentielles à la reconnaissance, à l'isolement et à la prévention des dommages pouvant être causés aux systèmes et réseaux informatiques du Canada.

21. En octobre 2006, le commissaire du CST a remarqué que la haute direction avait été mise au courant de la possibilité que des activités de cyberdéfense n'aient pas été conformes aux politiques et aux procédures opérationnelles. En outre, le commissaire a noté que la gestion n'accordait pas suffisamment d'attention aux conditions ou aux règles de conformité énoncées dans les autorisations ministérielles, et que le cadre de contrôle s'appliquant au déroulement des activités permises par les autorisations ministérielles aurait pu être plus clair, cohérent, complet et actuel. L'effet cumulatif de ces difficultés a suscité des doutes quant à la conformité du CST aux dispositions de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la défense nationale*. En conséquence, le CST a interrompu les activités de cyberdéfense qu'il menait en vertu des autorisations ministérielles le temps qu'une enquête

[8] Comité sénatorial permanent des banques et du commerce, *Les cyberattaques : elles devraient vous empêcher de fermer l'œil*, octobre 2018, https://sencanada.ca/fr/info-page/parl-42-1/banc-cyber-security/.

interne soit réalisée. Ces activités ont repris en octobre 2007 suivant une refonte du programme des autorisations ministérielles et du cadre stratégique[9].

22. Depuis 2007, le commissaire du CST juge que les autorisations ministérielles visant les activités de cyberdéfense répondent aux exigences de la *Loi sur la défense nationale* et que ces activités sont menées conformément aux lois de même qu'aux politiques du CST[10]. Le commissaire du CST a également été en mesure de confirmer que le CST ne dirigeait pas ses activités de cyberdéfense contre des Canadiens ou des personnes se trouvant au Canada. Or, entre 2001 et 2019, le commissaire du CST a tout de même formulé un certain nombre de recommandations ayant pour objet de veiller à ce que les activités de cyberdéfense du CST comportent :

- des définitions concrètes, de nouvelles classifications de documents et des calendriers clairement définis pour la conservation et l'élimination des renseignements personnels[11];
- des politiques adéquates en matière de classement, de conservation et d'élimination des renseignements clés obtenus en vertu d'une autorisation ministérielle[12];
- des descriptions plus précises et complètes des autorisations ministérielles permettant de comprendre sans équivoque ce que le ministre est appelé à autoriser[13];
- une transparence accrue de la *Loi sur la défense nationale* sur le plan des autorisations pouvant poser un risque d'interception des communications privées[14].

23. En 2019, la *Loi sur la sécurité nationale* entraînait la création de deux nouveaux organismes. Le premier est l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, qui a pris en charge les activités d'examen du commissaire du CST. Le second est le commissaire au renseignement qui, entre autres, examine les autorisations annuelles pour la cybersécurité que le ministre de la Défense nationale délivre au CST[15]. Ces autorisations permettent au CST d'accéder aux infrastructures de l'information des

---

[9] Bureau du commissaire du Centre de la sécurité des télécommunications (BCCST), *Review of CSEC's activities under the Protection of Computer Systems and Networks of the Government of Canada Ministerial Authorizations – CSEC's Security Posture Assessment – Active Network Security Testing (ANST) Activities in 2007–2008 and 2008–2009*, Report 58, 14 février 2011, pp. 4 à 5.

[10] BCCST, *Review of CSEC's activities under the Protection of Computer Systems and Networks of the Government of Canada Ministerial Authorizations, Report 58*, 14 février 2011, p. 25.

[11] BCCST, *Report on CSE ITS Ministerial Authorizations, Report 24*, 20 mai 2003, pp. 31 à 32.

[12] BCCST, *Information Security Activities Conducted Under the Industry Canada Ministerial Authorization, Report 38*, 19 décembre 2006, pp. 10 à 11.

[13] BCCST, *Privacy and Technology, Report 46*, 11 juin 2008, p. 24.

[14] BCCST, *Review of ITS ANST/CDO 2013, Report 89*, 31 mars 2015, p. 23.

[15] Le Bureau du commissaire au renseignement est un organe indépendant et quasi judiciaire chargé d'examiner les conclusions : a) du ministre de la Défense nationale, relativement à la délivrance et à la modification des autorisations de renseignement étranger ou des autorisations de cybersécurité pour le Centre de la sécurité des télécommunications; b) du ministre de la Sécurité publique et de la Protection civile, relativement à la définition des catégories d'ensembles de données que le Service canadien du renseignement de sécurité (SCRS) est en droit de recueillir ou à la définition des catégories d'actes ou d'omissions que le SCRS serait autorisé à commettre, sans quoi ces collectes, actes ou omissions constitueraient des infractions à la Loi sur le SCRS; et c) le directeur du SCRS, relativement à l'autorisation du SCRS à interroger un ensemble de données en circonstances impératives ou à

institutions fédérales ou d'organisations non fédérales désignées sans enfreindre les lois du Parlement (p. ex. le *Code criminel*) et sans contrevenir aux attentes raisonnables des Canadiens ou des personnes se trouvant au Canada en matière de respect de la vie privée. Depuis la création de son commissariat en 2019, le commissaire au renseignement a jugé que toutes les autorisations de cybersécurité qu'il avait examinées s'étaient avérées raisonnables. Toutefois, le commissaire au renseignement a également noté qu'au chapitre de la mise en œuvre, les autorisations de cybersécurité comportaient de nombreuses incohérences, notamment, l'absence de description des résultats et des services de cybersécurité reçus par les clients ou des conditions prescrites par le ministre à l'égard de ces autorisations. Toutefois, ces questions n'ont aucunement influé sur l'évaluation du commissaire au renseignement quant à la raisonnabilité des conclusions du ministre.

Examen interne

24. Les examens ou les audits internes suivants présentent un intérêt particulier pour le cadre de cyberdéfense du gouvernement.

- **Secrétariat du Conseil du Trésor du Canada – *Report on Cyber Security of Government Systems* (2016) :** Cette étude analysait les aspects de la cybersécurité dans l'ensemble du gouvernement et a déterminé qu'il manquait une prise de décisions claire au niveau de l'entreprise du gouvernement. Elle suggérait de nommer un haut dirigeant chargé de pallier les lacunes en matière de responsabilité et de faciliter les initiatives d'entreprise. Elle suggérait aussi de réduire les redondances entre les comités de gouvernance[16].
- **Bureau du contrôleur général du Canada — Audit interne horizontal de la sécurité des technologies de l'information dans les grands et les petits ministères (2016) :** Mené dans le cadre d'un effort sur plusieurs années comportant plusieurs étapes, cet audit a examiné les cadres de gouvernance et de contrôle qui encadrent la sécurité des technologies de l'information pour les réseaux non classifiés du gouvernement. Il a constaté que de tels cadres étaient en place et que le Secrétariat du Conseil du Trésor du Canada avait établi une orientation stratégique pour la sécurité des technologies de l'information. Toutefois, l'audit a souligné que les instruments politiques étaient désuets et qu'une précision des rôles et responsabilités était nécessaire, y compris pour SPC,

---

conserver des ensembles de données étrangères. Voir Bureau du commissaire au renseignement, *Rapport annuel 2020*, 31 mars 2020, https://www.canada.ca/fr/commissaire-renseignement/rapportannuel.html.

[16] Les références à la prise de décision d'entreprise ou aux initiatives de sécurité d'entreprise renvoient à l'Architecture de la sécurité d'entreprise dirigée par le Secrétariat du Conseil du Trésor qui comprend des approches communes pangouvernementales à la planification et à la prestation des services de sécurité communs. Essentiellement, il s'agit de traiter le gouvernement comme une entité unique, plutôt qu'un regroupement d'organisations individuelles chacune responsables de leur propre cybersécurité et cyberdéfense. Dans le contexte de la cybersécurité, cette approche d'entreprise accroît la capacité du gouvernement à se protéger contre les cybermenaces en normalisant les contrôles de sécurité et en améliorant la communication de l'information sur les cybermenaces, ce qui contribue à l'amélioration des réponses aux cyberincidents. Voir Services partagés Canada, *SSC Cyber and IT Security Framework*, Version 1.0, 8 octobre 2014; et Sécurité publique Canada, *Progress Report on Canada's Cyber Security Strategy – Horizontal Initiative for 2012-13 and 2013-14*, sans date.

afin de définir davantage les attentes pour rendre sécuritaires les systèmes patrimoniaux. L'audit a aussi permis de révéler que plusieurs comités gouvernant les instruments politiques sur la technologie de l'information devraient améliorer les relations de coordination et de communication des données. D'autres étapes étaient prévues pour les exercices 2019-2020 et 2021-2022[17].

- **Sécurité publique Canada — Évaluation horizontale de la Stratégie de cybersécurité du Canada (2017) :** Cet examen portait sur les avancées du gouvernement pour lutter contre les cyberattaques. Malgré des améliorations, il a constaté que de la confusion subsistait entre les ministères relativement à leurs rôles et responsabilités, surtout entre le CST et le Centre canadien de réponse aux incidents cybernétiques de Sécurité publique Canada de l'époque. Le secteur privé a soulevé cette préoccupation, en ajoutant que les organisations du secteur privé ne savaient pas vraiment où signaler les incidents de cybersécurité ou à qui demander de l'aide. L'examen a aussi constaté que le gouvernement devait continuer de renforcer sa capacité de prévenir et de détecter les cyberattaques, d'y répondre et de reprendre ses activités par la suite. Il recommandait que le gouvernement renforce sa gouvernance horizontale de la cybersécurité en évaluant de nouveau la participation à des comités et en élaborant des mandats afin de mieux définir les rôles et responsabilités des ministères[18].

---

[17] Bureau du contrôleur général du Canada, *Audit interne horizontal de la sécurité des technologies de l'information dans les grands et les petits ministères (Étape 1)*, février 2016, https://www.canada.ca/fr/secretariat-conseil-tresor/services/verifications-evaluation/audits-internes-horizontaux/securite-technologie-informations-grands-petits-ministeres-etape-1.html.

[18] Sécurité publique Canada, Évaluations horizontale de la Stratégie de cybersécurité du Canada, 29 septembre 2017, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-fr.aspx.

Partie I : Les cybermenaces : enjeux et intervenants

25. En tant que composante fondamentale de l'infrastructure essentielle du Canada, le gouvernement recueille et détient de l'information, et fournit des services qui représentent une grande valeur pour les adversaires du Canada. En cette ère numérique, la quasi-totalité de ce que détient le gouvernement et de ce qu'il en fait est à risque — qu'il s'agisse de renseignements relatifs aux impôts et à l'emploi des Canadiens, de données exclusives et de recherche appartenant à des entreprises, de politiques, d'enquêtes et d'opérations ou de processus numériques qui sous-tendent les nombreux services et avantages dont dépendent les Canadiens. Les réseaux gouvernementaux sont donc indispensables à la sécurité nationale du Canada. Le présent chapitre porte sur les enjeux posés par les cybermenaces qui guettent les systèmes du gouvernement, l'évolution des cybermenaces au fil du temps et les principaux acteurs menaçant le Canada à l'heure actuelle. Il constitue la base du présent examen.

Quels sont les enjeux?

26. Les cyberattaques contre les systèmes du gouvernement menacent l'information qu'il détient ainsi que divers systèmes et processus électroniques nécessaires à son fonctionnement. Cette vulnérabilité étendue peut être décomposée en cinq volets, lesquels seront décrits dans les prochains paragraphes :

- renseignements personnels des Canadiens;
- information relative à la propriété, à la propriété intellectuelle et à la recherche appartenant à des entreprises et à des chercheurs canadiens;
- politiques du gouvernement et processus d'élaboration de politiques;
- information et opérations relatives à la sécurité et au renseignement;
- intégrité des systèmes du gouvernement.

Menaces aux renseignements personnels des Canadiens

27. Le gouvernement recueille et gère des quantités considérables de renseignements personnels. Ceux-ci comprennent les noms, les dates de naissance, les adresses, les renseignements liés à l'assurance sociale et aux passeports, les dossiers médicaux, les renseignements liés au vote et d'autres détails personnels. Par exemple :

- l'Agence du revenu du Canada détient de l'information relative à l'identité des Canadiens, leur revenu, leur emploi, leurs avantages sociaux et leurs impôts;
- Immigration, Réfugiés et Citoyenneté Canada détient de l'information relative à l'identité et au statut des particuliers au pays;
- l'Agence des services frontaliers du Canada détient des renseignements de nature délicate concernant le Système d'information préalable sur les voyageurs/dossiers du

passager, les entrées et sorties, et les données biométriques (empreintes et photographies numériques) pour certaines catégories de voyageurs.

Des criminels pourraient se servir de telles données afin d'usurper l'identité de Canadiens, ouvrir des comptes bancaires, obtenir des emprunts ou des cartes de crédit ou se prévaloir d'avantages ou de remboursements du gouvernement[19]. Des États étrangers hostiles pourraient avoir recours à ces données pour localiser des Canadiens ou des personnes résidant au Canada[20].

Menaces à l'information organisationnelle, à la propriété intellectuelle, aux réseaux de recherche et aux activités universitaires

28. Le gouvernement détient des renseignements relatifs aux entreprises canadiennes, à la propriété intellectuelle, aux réseaux de recherche et aux activités universitaires. Par exemple :

- le Conseil national de recherche détient de l'information liée aux avancées du Canada en matière de technologies et de propriété intellectuelle qui peut s'avérer cruciale à la réussite technique d'entreprises canadiennes et internationales;
- Défense, Recherche et Développement Canada détient de l'information sur la science et les technologies en matière de défense — y compris celle ayant été élaborée ou communiquée aux ministères partenaires et aux alliés de l'industrie, du milieu universitaire et étrangers — utilisée pour appuyer les opérations de défense et de sécurité au pays et à l'étranger;
- Innovation, Science et Développement économique Canada détient de l'information liée aux conditions du Canada relativement aux investissements, à l'innovation et au commerce international.

Le vol de ces données par des acteurs malveillants pourrait nuire à la capacité de concurrence du Canada à l'échelle internationale et à ses intérêts économiques, miner l'innovation et porter atteinte à la sécurité nationale.

Menaces aux politiques ou aux processus d'élaboration des politiques gouvernementales

29. Le gouvernement détient de l'information sur ses politiques ou ses processus d'élaboration des politiques. Au moyen de divers processus d'élaboration de politiques et de prise de décision, le gouvernement génère et obtient de l'information en quantité considérable et souvent de nature très délicate sur des sujets couvrant son travail au pays et à l'étranger,

---

[19] Agence du revenu du Canada, « Protégez-vous contre le vol d'identité », 2010, http://www.canada.ca/fr/agence-revenu/services/formulaires-publications/publications/rc284/protegez-vous-contre-identite.html.
[20] Pour obtenir plus de renseignements, voir le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). *Rapport annuel 2020*, 2021, https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-fr.html.

comme les politiques et le commerce étrangers, la défense et la sécurité, les ressources naturelles, l'énergie et les finances. Il en va de même quant aux processus et aux décisions qui peuvent avoir une incidence sur les marchés financiers ou les investissements à l'étranger, notamment la planification budgétaire et la réglementation, ou qui ont trait au système judiciaire du Canada. Par exemple :

- Affaires mondiales Canada détient de l'information concernant les relations bilatérales et multilatérales du Canada, le commerce international, les dossiers consulaires et les efforts d'assistance en matière de sécurité et de paix;
- le Secrétariat du Conseil du Trésor du Canada détient de l'information concernant les dépenses du gouvernement, la réglementation et la gestion dans les secteurs touchant les personnes, les finances et les technologies;
- le ministère des Finances détient de l'information relative à l'économie et à la fiscalité, notamment au budget annuel, aux politiques en matière de tarifs et de fiscalité, aux mesures sociales et aux investissements liés à la sécurité;
- la Cour fédérale détient de l'information sur les délibérations concernant le droit administratif; la citoyenneté, l'immigration et les réfugiés; la propriété intellectuelle; le droit maritime et la sécurité nationale (p. ex. les mandats autorisant certaines activités du Service canadien du renseignement de sécurité).

De tels renseignements sont d'intérêt pour les États étrangers ou les criminels. Leur vol pourrait compromettre les intérêts nationaux du Canada, sa capacité de concurrence à l'international, ses positions de négociation, sa réputation sur la scène internationale ainsi que ses relations internationales. Le vol de documents liés aux processus décisionnels et aux finances pourrait mener au dévoilement de renseignements liés aux plans de dépenses et de programmes du gouvernement, nuire à ses stratégies de négociations à l'étranger ainsi qu'ébranler la confiance dans les marchés canadiens. Quant aux cyberattaques ciblant les processus judiciaires, elles pourraient mener à la divulgation de dossiers et de délibérations de nature délicate, ce qui menacerait l'intégrité du système juridique.

Menaces à l'information et aux opérations liées à la sécurité et au renseignement

30. Les réseaux du gouvernement renferment de l'information liée à la sécurité nationale, au renseignement et aux activités de défense du Canada, y compris les opérations et les enquêtes. Par exemple :

- le Service canadien du renseignement de sécurité détient de l'information hautement classifiée, y compris des enquêtes liées à sécurité nationale visant des États précis et des personnes canadiennes. En outre, dans le cadre du processus de filtrage de sécurité du gouvernement, il recueille de l'information de nature délicate sur les employés du gouvernement qui requièrent l'accès à de l'information classifiée ou à des installations afférentes;

- le ministère de la Défense nationale et les Forces armées canadiennes détiennent de l'information sur les opérations militaires du Canada, ses technologies et son équipement, ses stratégies, son renseignement et ses plans d'approvisionnement.

Le vol d'information sur les opérations militaires pourrait mener au dévoilement de stratégies, de cibles, d'opérations et de plans militaires, ce qui risquerait de compromettre la sécurité des troupes canadiennes à l'étranger ainsi que la réussite des opérations militaires. Le vol d'information sur les opérations de sécurité et de renseignement pourrait mener au dévoilement de l'identité de représentants de la sécurité et du renseignement, ce qui compromettrait leur sécurité et les exposerait à l'extorsion et à l'espionnage. La perte de tels renseignements entraînerait possiblement la divulgation des sources et des méthodes utilisées pour recueillir le renseignement, ce qui affaiblirait la capacité du Canada à recueillir des renseignements sur les menaces à la sécurité nationale.

Menaces à l'intégrité des systèmes du gouvernement

31. Enfin, une cyberattaque réussie pourrait compromettre l'intégrité des systèmes du gouvernement. En tant que composante clé de l'infrastructure essentielle du Canada, le gouvernement doit fournir des services ininterrompus. Au sein de nombreux secteurs, il est essentiel de veiller à la continuité des activités du gouvernement. Par exemple :

- le premier ministre, le Cabinet, les ministres et les parlementaires dépendent des technologies de l'information et des communications électroniques pour mener des activités d'État de nature délicate;
- Emploi et Développement social Canada, Service Canada et leurs ministères partenaires dépendent des technologies de l'information pour offrir de nombreux avantages aux Canadiens, y compris des régimes de pension, des passeports, une assurance-emploi et une assurance-invalidité pour les vétérans;
- Services partagés Canada fournit des services centraux et numériques aux organisations gouvernementales afin de permettre la prestation de services et de programmes numériques couvrant une gamme de mandats.

Une cyberattaque contre les systèmes du gouvernement pourrait compromettre la continuité des activités gouvernementales, la prestation de services et l'intégrité de l'information détenue. C'est l'économie et l'aide sociale aux Canadiens qui en subiraient les contrecoups.

Quelle est la situation? Le contexte de la cybermenace

32. Le Centre de la sécurité des télécommunications (CST) entend par **cybermenace** « une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient. » On appelle « **auteurs de cybermenace** » les personnes à l'origine de ces activités. Il s'agit d'États, de groupes ou de personnes malveillants qui cherchent à tirer avantage des vulnérabilités,

d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux appareils, aux systèmes et aux réseaux des victimes[21]. Le CST a établi six catégories d'auteurs de cybermenaces en fonction de leur motivation principale.

- **États-Nations :** Motivés par une gamme d'objectifs stratégiques, politiques, économiques ou liés à la sécurité, les États tentent d'obtenir des avantages dans les sphères économique, politique et militaire.
- **Cybercriminels :** Motivés par des récompenses financières réelles ou perçues, les criminels cherchent à s'enrichir en ciblant les vulnérabilités.
- **Hacktivistes :** Animés par un idéal activiste, ceux-ci tentent de donner de la visibilité à leur cause de nature politique ou sociale[22].
- **Groupes terroristes :** Ils sont guidés par un extrémisme violent fondé sur des croyances religieuses ou politiques et cherchent à recueillir des fonds, à faire du prosélytisme et à organiser des attentats.
- **Amateurs de sensations fortes :** Pour leur satisfaction personnelle, les amateurs de sensations fortes tentent de « déjouer » les mesures de cyberdéfense d'une organisation ou d'un gouvernement.
- **Menaces internes :** Motivés par leur mécontentement et leur insatisfaction, les auteurs de menaces internes cherchent à se venger d'affronts subis dans le passé ou à profiter de la vente de secrets[23].

33. Les auteurs de cybermenaces n'ont pas tous les mêmes capacités et le même degré de perfectionnement. C'est l'accès aux ressources techniques et financières et à une formation qui les différencie principalement. Les auteurs ayant atteint un perfectionnement et des compétences du plus haut niveau représentent des **cybermenaces persistantes avancées**. Pour parvenir à leurs fins stratégiques, ils utilisent des techniques avancées afin de mener des campagnes prolongées et complexes. Les États-Nations sont généralement les auteurs de cybermenaces les plus perfectionnés, en raison de leurs ressources d'état étendues, de leurs technologies avancées (et souvent hautement classifiées), d'une planification et d'une organisation exhaustives, et de la capacité d'agir presque en toute impunité sur le plan judiciaire. À quelques exceptions près, les cybercriminels sont considérés comme des auteurs de cybermenaces modérément perfectionnés, quoiqu'ils puissent parfois avoir recours à une planification rigoureuse, à du soutien et à des moyens techniques de sorte à faire un grand nombre de victimes. Les hacktivistes, les groupes terroristes et les amateurs de sensations fortes se situent habituellement au bas de l'échelle sur le plan du perfectionnement, car ils ont

---

[21] Centre de sécurité des télécommunications (CST), « Introduction à l'environnement de cybermenace », 2019, www.cyber.gc.ca/sites/default/files/publications/intro-ncta-2020_f.pdf.
[22] Bureau de la traduction, Services publics et Approvisionnement Canada, « Hacktiviste », banque de données Termium Plus, 2021. www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=1&srchtxt=hacktivist&index=ent&codom2nd_wet=1#resultrecs.
[23] CST, « Introduction à l'environnement de cybermenace », 2019, www.cyber.gc.ca/sites/default/files/publications/intro-ncta-2020_f.pdf; et CST, « Government of Canada Enterprise Security Architecture Enterprise Threat Assessment », janvier 2017.

recours à des outils dont le déploiement ne requiert que peu d'habiletés techniques. Les personnes travaillant en tant qu'employés au sein d'une organisation qui leur fait confiance constituent des menaces internes. Leur accès aux réseaux internes (et protégés de surcroît) pourrait mener à des pertes de données considérables ou à des perturbations de systèmes[24]. Si le Comité reconnaît que le gouvernement se doit de défendre ses systèmes contre toute menace, quel que soit son degré de perfectionnement ou la motivation de son auteur, il se penche principalement, dans le cadre du présent examen, sur les auteurs de cybermenaces parrainés par l'état en raison de leur haut degré de perfectionnement et de l'ampleur des dommages qu'ils peuvent ainsi causer.

34. **L'environnement de cybermenace** est l'espace en ligne où les auteurs de cybermenace mènent leurs activités malveillantes[25]. Il est constitué de composantes technologiques, y compris d'une connectivité Internet et d'appareils connectés, d'une puissance de traitement et de stockage de données, et des personnes et organisations qui s'en servent, dont les gouvernements, les citoyens, les entreprises, les universités et les industries. Cet environnement de cybermenaces a évolué au fil du temps; les changements les plus remarquables consistent en la croissance exponentielle du nombre d'utilisateurs, de la bande passante, des ordinateurs et d'autres appareils, et une augmentation en parallèle de la création de données personnelles et exclusives[26].

35. Les ministères et organismes ont accru leur interconnectivité, entre eux et avec des environnements Internet externes, tels que des organisations du secteur privé et des citoyens. Pour que le gouvernement assure la prestation de services aux clients, l'interface entre les réseaux gouvernementaux et les cyberenvironnements externes est essentielle. En fait, elle est au cœur même de sa vision des opérations numériques, où les programmes et services sont offerts de façon numérique à tous les Canadiens, n'importe quand, n'importe où et sur n'importe quel appareil[27]. Les systèmes et les réseaux du gouvernement sont donc exposés à des auteurs de menaces délibérés pouvant mener des cyberactivités malveillantes ciblant le gouvernement; et la cybercompromission d'un ministère peut menacer les autres ministères.

36. Les auteurs de cybermenaces ont recours à diverses méthodes pour attenter aux systèmes d'information. Comme le relève le CST, [traduction] « la structure de l'Internet permet aux auteurs de menaces de se connecter directement à un système d'information partout sur la planète ou de surveiller les communications liées à un système d'information pris pour cible[28]. » Par exemple, des auteurs de cybermenaces pourraient :

---

[24] CST, « Introduction à l'environnement de cybermenace », 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_f.pdf.
[25] CST, « Introduction à l'environnement de cybermenace », 2019, www.cyber.gc.ca/sites/default/files/publications/Intro-ncta-2020_f.pdf.
[26] Centre canadien pour la cybersécurité (CCC), *Modern Ransomware and Its Evolution*, 2020
[27] Pour obtenir des renseignements additionnels sur la vision du gouvernement relative aux opérations numériques, consulter le « Plan stratégique des opérations numériques de 2018 à 2022 » à l'adresse https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/plan-strategique-operations-numerique-2018-2022.html#ToC3.
[28] CST, « Government of Canada Enterprise Security Architecture Enterprise Threat Assessment », 2017.

- surveiller l'interaction entre deux appareils ou composantes logicielles dans le système d'information, ce qui entraînerait une compromission des données;
- bloquer la communication entre deux composantes, interrompant la prestation de services essentiels;
- s'insérer entre deux appareils ou modules communicants et intercepter leurs communications;
- obtenir un accès aux systèmes du gouvernement en usurpant l'identité d'un utilisateur légitime ou en volant des justificatifs d'identité[29].

37. L'équilibre entre la cyberdéfense et la cyberattaque est variable. Les ministères utilisent une gamme de navigateurs, de logiciels, d'applications et de matériel informatique, dont l'âge et le perfectionnement varient, qui nécessitent des mises à jour et un entretien constants afin de minimiser leurs vulnérabilités. Les ministères ont aussi mis en œuvre des mesures perfectionnées pour renforcer les mesures de défense. Or, pendant ce temps, la capacité des auteurs de cybermenaces de commettre des cyberattaques s'est accrue. Pour les auteurs de cybermenaces relativement moins perfectionnés, les outils de piratage sont devenus moins coûteux et plus facilement accessibles par l'entremise de fournisseurs de services criminels, ce qui permet à ces premiers d'orchestrer des attaques complexes difficiles à détecter[30]. Comme il est décrit ci-après, les auteurs de cybermenaces les plus perfectionnés, notamment la Chine et la Russie, continuent d'adapter leurs moyens pour faire échec aux mesures de défense, et d'autres états, comme ***, investissent considérablement dans leurs moyens pour faire de même. En somme, les cybermenaces aux réseaux gouvernementaux ainsi que les mesures pour les contrer évoluent rapidement.

Cybermenaces pour les réseaux du gouvernement, de 2015 à 2020

38. Dans son Rapport annuel 2020, le Comité décrit le paysage contemporain des cyberactivités malveillantes menaçant les systèmes gouvernementaux, les fournisseurs de services essentiels, le secteur privé et la population canadienne[31]. Dans le cadre du présent examen, l'analyse du Comité portera précisément sur les cyberactivités malveillantes qui ont ciblé les systèmes et les réseaux du gouvernement de 2015 à 2020.

39. Le CST emploie deux procédés pour cerner les menaces aux systèmes gouvernementaux. Le programme du renseignement étranger du CST surveille les auteurs de cybermenaces étrangers afin de déterminer leurs techniques et leurs champs d'intérêt (entre autres). L'information est ensuite communiquée au Centre canadien pour la cybersécurité (CCC), situé au sein du CST. Pour sa part, le CCC gère trois types de capteurs de cyberdéfense, qui cherchent des menaces connues et des anomalies dans certains

---

[29] CST, « Government of Canada Enterprise Security Architecture Enterprise Threat Assessment », 2017.
[30] CST, *Operational Threat Report: 2019 Annual Threat Landscape – 1 January to 31 December 2019*, 2020. Le CST souligne que le cybercrime est l'une des formes de criminalité transnationale qui enregistre la plus grande hausse et indique qu'il continuera de grandir, car la disponibilité accrue des maliciels diminue l'expertise technique requise pour causer des dommages.
[31] CPSNR, *Rapport annuel 2020*, 2021, https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-fr.html.

ministères, réseaux et environnements d'infonuagique. Le CCC combine l'information recueillie de ces sources et celle transmise par des partenaires pour créer des indicateurs de compromission qui lui permettront de cerner ces cybermenaces malveillantes[32]. Suivant l'augmentation du déploiement des capteurs de cyberdéfense au fil du temps, la capacité du CCC à détecter les cyberactivités malveillantes sur les systèmes du gouvernement a également augmenté.

40. La capacité du CCC à parer cette activité s'est aussi accrue. En 2013 (avant la création du CCC), le CST a commencé à mettre en œuvre des mesures de défense dynamique basées sur le réseau, représentant un tournant révolutionnaire dans les moyens défensifs. Le CST, qui était seulement en mesure de cerner les menaces, a pu dès lors les parer proactivement. Pour créer ces mesures de défense, les menaces nouvellement cernées sont *** mises à jour dans le système de défense dynamique du CST. Les capteurs peuvent ensuite détecter ces menaces et activer automatiquement des mesures d'atténuation. Bien que les auteurs malveillants continuent de cibler le gouvernement, le déploiement de ces mesures de défense dynamique a considérablement miné leur capacité à compromettre les systèmes du gouvernement[33]. Dans le cadre de comparutions devant le Comité, des représentants du CCC ont affirmé que le volume de cyberincidents a diminué depuis 2015, et que les répercussions de tels incidents sont moins importantes grâce à la capacité d'intervention rapide du CCC en cas de nouvelles attaques et de prévention des types de dommages qui par le passé auraient contraint les ministères ciblés à rebâtir leurs réseaux[34]. Les représentants ont aussi déclaré qu'au début des années 2010, le CST a constaté des milliers d'incidents par année, dont plusieurs cas d'exfiltration à partir des réseaux du gouvernement du Canada. Ils ont ajouté que [traduction] « [à] présent, si l'on en constate *** par année, il s'agit d'une mauvaise année, car on est en mesure d'intervenir très rapidement[35]. » L'évolution et le déploiement des capteurs seront abordés ci-après.

Preuve d'une compromission

41. Plusieurs activités malveillantes indiquent la compromission d'un réseau, notamment : le balisage, l'exploitation à distance, les artéfacts de logiciel, le téléchargement de maliciels, l'hameçonnage, l'exploitation basée sur navigateur, l'exfiltration de données, l'accès à distance et le déni de service, décrites ci-dessous[36]. ***

---

[32] CCC, « Review of the Government of Canada's Cyber Defence Activities », comparution devant le CPSNR, 19 février 2021.
[33] CST, *Year Review Cyber Defence Report 2017*, 2018.
[34] CCC, Remarques du chef du CCC, comparution devant le CPSNR, 19 février 2021.
[35] CCC, Remarques du chef du CCC, comparution devant le CPSNR, 19 février 2021.
[36] Il convient de noter que la méthodologie de suivi des cyberactivités malveillantes par le CST a évolué au fil des années, tout comme ses connaissances des auteurs de cybermenaces, et il a élargi le déploiement de ses capteurs de cyberdéfense à d'autres ministères. Lorsque le CST est en mesure de trouver et de décrire une activité de cybermenace malveillante, elle se rapporte seulement aux secteurs des réseaux du gouvernement qu'il peut voir : la circulation ministérielle sur le Service Internet d'entreprise de SPC ou les données tirées de ses capteurs de cyberdéfense sur l'hôte.

Balisage

42. Le balisage est une méthode de communication entre un réseau ciblé compromis et l'ordinateur de l'attaquant. L'auteur d'une cybermenace peut déployer une balise par divers moyens, notamment par l'exploitation à distance, l'hameçonnage ou l'exploitation basée sur navigateur. La balise sert à signaler à l'auteur de la cybermenace que son attaque a réussi et que l'outil implanté est parvenu à déjouer les mesures de défense du réseau (p. ex. un coupe-feu). L'auteur de la cybermenace peut alors créer d'autres canaux de communication (habituellement dissimulés et chiffrés) afin d'y introduire d'autres outils plus poussés (p. ex. afin d'exploiter le réseau davantage ou de voler de l'information)[37]. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST. ***][38]

Exploitation à distance

43. L'exploitation à distance est un processus au cours duquel un auteur de cybermenaces transmet à partir d'un réseau à distance un ensemble de commandes à un appareil ciblé pour y accéder ou accéder à l'information qu'il contient[39]. En général, les exploitations à distance profitent des vulnérabilités ou des faiblesses des logiciels, du matériel informatique ou de la configuration d'un ordinateur ou d'un appareil connecté au réseau. Autrement dit, c'est par l'exploitation à distance que le criminel force une serrure[40]. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST. ***][41]

Accès à distance

44. L'accès à distance renvoie aux connexions à distance non autorisées à un hôte victime par un auteur de cybermenaces sans exploitation (p. ex., recours à une combinaison valide d'un nom d'utilisateur et d'un mot de passe, souvent obtenu par le vol de données ou une tentative réussie d'hameçonnage par courriel)[42]. Des utilisateurs légitimes interagissent avec des dossiers, de l'information et des ressources du système lorsqu'ils travaillent à distance (p. ex. le télétravail)[43]. En tirant profit de l'accès à distance à un réseau ciblé, les auteurs malveillants de cybermenaces peuvent imiter toutes les interactions et les activités d'un utilisateur légitime.

---

[37] CCC, « Glossaire », http://www.cyber.gc.ca/fr/glossaire. Voir aussi la définition de « beaconing ». Association internationale des chefs de police (IACP), Law Enforcement Cyber Center, https://www.iacpcybercentre.org/resources-2/glossary/#8 [en anglais seulement].

[38] CCC, *Operational Threat Report: 2019 Annual Threat Landscape – 1 January to 31 December 2019*, 2020.

[39] CCC, « Glossaire », http://www.cyber.gc.ca/fr/glossaire.

[40] Vice, https://www.vice.com/en/article/mg79v4/hacking-glossary [en anglais seulement].

[41] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; et CST, « NSICOP Cyber Report – Typos and Small Changes », p. 1, 9 juillet 2021.

[42] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.

[43] Techtarget, « Remote Access », Search Security, https://searchsecurity.techtarget.com/definition/remote-access#:~:text=Remote%20access%20is%20the%20ability,distance%20through%20a%20network%20connection.&textA%20VPN%20creates%20a%20safe,network%2C%20such%20as%20the%20Internet.

[*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation par le CST. ***][44]

Artéfacts et téléchargements de maliciel

45. On définit le maliciel comme une grande gamme de logiciels malveillants conçus pour infiltrer ou endommager un système informatique, sans le consentement du propriétaire[45]. Un maliciel peut être déployé par divers moyens (p. ex. l'exploitation à distance, l'hameçonnage ou l'exploitation basée sur navigateur). Le code d'un maliciel est écrit dans le but précis de causer des dommages, de divulguer de l'information ou de porter atteinte à la sécurité ou à la stabilité d'un système[46]. Les artéfacts de maliciel sont des traces détectables de maliciel sur l'appareil d'une victime[47]. Le téléchargement de maliciel renvoie aux occurrences où un maliciel a été téléchargé sur un appareil ***[48]. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST. ***] (voir l'image 1)[49].

Sources : CST, *Rapport annuel de cyberdéfense*, 2016; CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

Image 1 : [*** Cette image a été supprimée pour retirer l'information préjudiciable ou privilégiée. L'image montrait des données recueillies par le CST. ***]

Hameçonnage

46. L'hameçonnage est un procédé par lequel des auteurs de menaces parrainés par l'état et des criminels sollicitent de l'information confidentielle appartenant à des cibles précises pour les inciter à divulguer des renseignements personnels ou des justificatifs d'identité[50]. Une tentative d'hameçonnage peut utiliser des courriels d'apparence officielle (connu sous le nom de harponnage) dont le degré de perfectionnement varie et qui contiennent souvent des liens ou des fichiers malveillants qui, une fois ouverts, infectent l'ordinateur du destinataire avec un maliciel. Un auteur de menaces peut avoir recours à ce maliciel pour accéder à l'ordinateur d'une cible afin de voler de l'information ou d'utiliser les renseignements personnels de la cible

---

[44] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.
[45] CCC, « Glossaire », http://www.cyber.gc.ca/fr/glossaire.
[46] Global Knowledge, « Cyber Security Glossary of Terms », https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/#top.
[47] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.
[48] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.
[49] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019. [*** Une phrase a été revue pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait un moyen du CST. ***] Voir CST, *Rapport annuel de cyberdéfense, 2017*, 2018.
[50] CCC, « Glossaire », http://www.cyber.gc.ca/fr/glossaire.

(comme des justificatifs d'identité ou des renseignements de carte de crédit) pour accéder à des informations bancaires ou commettre un vol d'identité[51].

47. [*** Ce paragraphe a été supprimé pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST. ***][52]

Exploitation basée sur navigateur

48. Les navigateurs Web et les applications connexes comportent des défauts et des vulnérabilités que les auteurs de cybermenaces malveillants exploitent pour prendre le contrôle de l'ordinateur d'une cible qui se connecte à un site Web infecté. Alors, ces auteurs volent les justificatifs d'identité de l'utilisateur, envoient un rançongiciel, exécutent un maliciel, volent de l'information ou obtiennent des autorisations sur un réseau pour accéder à d'autres appareils[53]. [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient un moyen et une évaluation du CST. ***][54] [55] [56]

Exfiltration de données

49. L'exfiltration de données est le retrait non autorisé (vol) d'information d'un réseau ciblé par un auteur de menaces une fois qu'il a obtenu un accès au moyen de l'exploitation à distance par exemple[57]. [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation du CST. ***] [58] [59]

Déni de service

50. Le déni de service est une technique utilisée pour empêcher des utilisateurs légitimes d'accéder à un service relié à un réseau en envoyant des demandes illégitimes pour surcharger les ressources d'un réseau[60]. [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation du CST. ***][61]

---

[51] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; et CCC, « Glossaire », http://www.cyber.gc.ca/fr/glossaire.

[52] CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

[53] Cynet, « Browser Exploits – Legitimate Web Surfing Turned Death Trap », https://www.cynet.com/blog/browser-exploits-legitimate-web-surfing-turned-death-trap/.

[54] Il convient de noter que le CST [*** La fin de la phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. Elle décrivait un moyen du CST. ***]

[55] Le CST a constaté une augmentation de l'exploitation basée sur navigateur en 2019, attribuée à une campagne précise de distribution de rançongiciel. CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

[56] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.

[57] International Association of Chiefs of Police, Law Enforcement Cyber Centre, « Glossary », https://www.iacpcybercenter.org/resources-2/glossary/#E; et CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.

[58] CST, *Year Review Cyber Defence Report 2017*, 2018.

[59] CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

[60] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.

[61] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019.

Les menaces persistantes avancées que présentent les États-nations

51. Le CST surveille les cyberactivités de certains acteurs étatiques. La Chine et la Russie représentent les auteurs de cybermenace qui ciblent le gouvernement les plus expérimentés[62]. L'Iran, la Corée du Nord et *** ont des capacités modérément sophistiquées; et *** présentent des menaces moins avancées. Les auteurs de menaces persistantes avancées peuvent faire partie de l'appareil officiel d'un État (p. ex. les forces armées, ou un organisme de la sécurité ou du renseignement) et être considérés comme étant des acteurs d'État; ou faire partie d'une entité non étatique qui est dirigée et soutenue (p. ex. financièrement) par un État et être considérés comme étant des acteurs parrainés par un État[63]. À des fins de simplicité, le Comité utilise le nom de l'État concerné lorsqu'il est question d'acteurs étatiques et d'acteurs parrainés par un État (p. ex., « la Chine »). L'évolution de ces menaces persistantes avancées pendant la période allant de 2015 à 2020 est présentée ci-dessous. (Remarque : Le CST accorde un niveau de menace faible, modéré ou élevé en fonction de ses connaissances du perfectionnement technologique de l'auteur de menace et de son évaluation de la probabilité que des auteurs de menace précis s'en prennent au Canada.)

Chine

52. La Chine constitue un auteur de cybermenace très sophistiqué. Ses principaux objectifs stratégiques consistent à maintenir une stabilité interne et à se développer à titre de puissance mondiale. Voici ses trois priorités :

- recueillir des renseignements à l'appui des politiques étrangères ainsi que des politiques en matière de sécurité et de commerce du gouvernement;
- recueillir de l'information scientifique et de l'information sur la recherche pertinente sur le plan des technologies stratégiques qui pourraient favoriser l'économie ou les forces armées de la Chine;
- recueillir ***[64].

Le CST a déterminé que [traduction] « on ne peut surévaluer la portée et la ténacité des activités de la Chine visant à accéder à la propriété intellectuelle, à l'information, ainsi qu'aux politiques et aux positions du gouvernement du Canada ». Le CST a également mentionné que les cyberactivités de la Chine étaient agressives et vastes, et plus audacieuses qu'auparavant.

---

[62] Pour évaluer le niveau de menace que présentent des acteurs parrainés par un État envers le gouvernement, le CST se fonde sur trois facteurs : la sophistication technique des cybercapacités, la capacité organisationnelle et le niveau d'intérêt.
[63] Threat Post, « Defending Against State and State-Sponsored Threat Actors », https://threatpost.com/defending-against-state-threat-actors/162518/; et CST, « Introduction à l'environnement de cybermenace », https://cyber.gc.ca/fr/orientation/cybermenace-et-auteurs-de-cybermenaces.
[64] CCC, « Cyber Threat Brief: State Activity Against Canada, January to June 2020 », 2020.

[*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST des moyens de la Chine. ***][65].

53. ***, la Chine a continué d'être un auteur de menace ciblant le gouvernement *** prolifique. Conformément à ses priorités en matière de renseignement, la Chine a ciblé plusieurs secteurs gouvernementaux, notamment la sécurité, le renseignement et la défense (***); les affaires étrangères, le commerce et le développement (***); le développement de l'industrie et du commerce (***); l'administration gouvernementale (***); les transports (***); et les ressources naturelles, l'énergie et l'environnement (***)[66]. Depuis le début de la pandémie de COVID-19, la Chine a pris pour cible des réseaux de recherche aux États-Unis, au Royaume-Uni et au Canada. ***[67].

54. La Chine se sert de diverses techniques pour cibler les systèmes et les réseaux du gouvernement. [*** Quatre phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation par le CST de moyens de la Chine. ***][68] [69] [70] En résumé, la Chine a adapté ses techniques pour qu'elles répondent à la posture de défense de ses cibles.

55. *** le CST a observé un vaste éventail de cyberactivités malveillantes de la Chine de même que la superposition de techniques. [*** Trois phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation par le CST de moyens de la Chine. ***][71] En résumé, la Chine continue de représenter une cybermenace très active et complexe[72].

Russie

56. La Russie constitue un auteur de cybermenace très expérimenté. La Russie mène des activités de cybermenace malveillantes, notamment *** le cyberespionnage et l'ingérence étrangère, à l'appui d'un vaste éventail de priorités stratégiques en matière de renseignement, notamment :

---

[65] CST, *Mise à jour sur les cybermenaces : République populaire de Chine et Russie*, 2015; et CST, *Rapport annuel sur les cybermenaces 2015*, 2016.
[66] CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020; et CCC, « Cyber Threat Brief: State Activity Against Canada, June to December 2020 », 2021.
[67] CCC, « Cyber Threat Brief: State Activity Against Canada Januaryto June 2020 », 2020.
[68] *** CST, *Quarterly Cyber Defence Report Q1 2015*, 2015.
[69] CST, *Mise à jour sur les cybermenaces : République populaire de Chine et Russie*, 2015; et CST, *Rapport annuel sur les cybermenaces 2015*, 2016.
[70] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[71] ***
[72] CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; CCC, *Rapport sur les cybermenaces : Tendances du ciblage des activités parrainées par un État, Rapport annuel de 2018*, 2019; CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020; et CCC, « Cyber Threat Brief: State Activity Against Canada, June to December 2020 », 11 février 2021.

- recueillir des produits du renseignement étrangers et militaires auprès de cibles diplomatiques, économiques et militaires, y compris des établissements d'enseignement supérieur et des organismes du secteur privé;
- reconnaître les fournisseurs de télécommunications et de systèmes de contrôle industriel pour l'infrastructure essentielle;
- cerner les tendances et les événements conflictuels des États rivaux en vue de mener des campagnes d'influence et d'ébranler les normes et les valeurs libérales et démocratiques[73].

La Russie a également recours à certains acteurs non étatiques, notamment des cybercriminels, des entreprises privées et des usines à trolls, pour qu'ils mènent des activités de cybermenace à son nom. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST des priorités de la Russie. ***][74]

57. *** la Russie comptait parmi les auteurs de menace parrainés par un État ciblant le gouvernement les plus prolifiques. Conformément aux priorités stratégiques en matière de renseignement de la Russie, ses activités de cybermenace ont ciblé divers secteurs de manière systématique : les affaires étrangères, le commerce et le développement (***); la sécurité, le renseignement et la défense (***); et les ressources naturelles, l'énergie et l'environnement (***)[75]. En 2020, la Russie a ciblé le système de santé du Canada dans le but de voler la propriété intellectuelle sur la recherche pharmaceutique et la création du vaccin contre la COVID-19. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. La phrase décrivait l'évaluation par le CST. ***][76]

58. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST des moyens de la Russie, et indiquait que la Russie emploie un large éventail de tactiques dans son ciblage des systèmes et des réseaux gouvernementaux et que la Russie demeure une cybermenace très poussée et active pour les réseaux gouvernementaux. ***][77] [78] [79] [80] [81] [82]

---

[73] CCC, « Cyber Threat Brief: State Activity Against Canada, January to June 2020 », 2020.
[74] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[75] CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada, Rapport annuel de 2018*, 2019; et CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020. Voir l'Annexe A pour un échantillon représentatif de ministères du gouvernement, par secteur.
[76] CCC, « Cyber Threat Brief: State Activity Against Canada – January to June 2020 », 2020.
[77] CST, *Rapport annuel sur les cybermenaces 2015*, 2016.
[78] CST, *Rapport annuel de cyberdéfense 2016*, 2017.
[79] CST, *Rapport annuel de cyberdéfense 2017*, 2018; et CST, CCC, *Rapport sur les cybermenaces : Tendances du ciblage des activités parrainées par un État, Rapport annuel de 2018*, 2019.
[80] CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[81] CST, *Rapport annuel sur les cybermenaces*, 2015; CST, *Rapport annuel de cyberdéfense*, 2016; CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020. ***
[82] CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

Iran

59. L'Iran présente une cybermenace modérée. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST des moyens de l'Iran, et indiquait quatre secteurs au centre des cyberactivités de l'Iran. ***][83] [84] [85] [86]

Corée du Nord

60. La Corée du Nord présente une cybermenace modérée. La Corée du Nord agit de la même manière que les cybercriminels : elle vole de la cryptomonnaie et de la monnaie fiduciaire pour financer le gouvernement et ses représentants. [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient l'évaluation par le CST. ***][87] [88]

***

61. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST d'un état qui fait peser une cybermenace modérée.***][89] [90] [91]

***

62. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST d'un état qui fait peser une cybermenace faible. ***][92] [93]

---

[83] CST, *Rapport annuel de cyberdéfense 2017*, 2018.
[84] CCC, *Rapport sur les cybermenaces : Tendances du ciblage des activités parrainées par un État, Rapport annuel de 2018*, 2019. *** CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada*, 2019; CCC, *Rapport sur les cybermenaces : Tendances du ciblage des activités parrainées par un État, Rapport annuel de 2018*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[85] CCC, « Cyber Threat Brief: State Activity Against Canada January to June 2020 », 2020.
[86] CCC, « Cyber Threat Brief: State Activity Against Canada January to June 2020 », 2020
[87] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[88] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020; CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020; et CCC, « Cyber Threat Brief: State Activity Against Canada January to June 2020 », 2020.
[89] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[90] CCC, ***, 2019.
[91] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020; et CST, « NSICOP Cyber Defence Review, Request for Information-4, Item #3 – Question Related to State-Sponsored Threat Actor », 2 juin 2021.
[92] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[93] CST, *Rapport annuel sur les cybermenaces*, 2015; CST, *Rapport annuel de cyberdéfense*, 2016; CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.

***

63. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST d'un état qui fait peser une cybermenace faible. ***][94] [95]

***

64. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST d'un état qui fait peser une cybermenace faible. ***][96] [97]

Réseaux du gouvernement et cybercriminalité

65. Le gouvernement est de plus en plus conscient de la menace que représente la cybercriminalité envers ses systèmes. La cybercriminalité est l'une des cyberactivités les plus répandues touchant les réseaux, les systèmes et les utilisateurs gouvernementaux puisqu'il s'agit d'une activité à faible risque et à rendement élevé. La disponibilité de nouvelles technologies et l'accès à celles-ci ont fait en sorte de grandement diminuer les obstacles à l'entrée de la cybercriminalité, permettant aux cybercriminels amateurs de lancer plus facilement des attaques avancées et difficiles à détecter.

66. Le CST a examiné pour la première fois des activités de cybercriminalité ciblant le gouvernement sous forme classifiée dans le cadre de son Rapport annuel des menaces de 2019. Le CST a déterminé qu'il existe plusieurs raisons pour lesquelles le gouvernement représente une cible attirante pour les cybercriminels. Premièrement, les réseaux du gouvernement hébergent de nombreuses bases de données qui contiennent de l'information d'une grande valeur sur un vaste éventail de sujets, comme les renseignements financiers, la propriété intellectuelle et les renseignements personnels. Deuxièmement, la taille considérable des systèmes et des réseaux du gouvernement fait en sorte qu'il est inévitable que les cyberacteurs opportunistes dont les activités ont une très large portée sur Internet ciblent le gouvernement. Troisièmement, les gouvernements à tous les niveaux représentent une cible intéressante aux fins d'extorsion, surtout par l'entremise de rançongiciels, en raison des importants budgets ministériels et des obligations envers les citoyens qui pourraient forcer le gouvernement à payer une rançon, dans certains cas[98]. [*** La fin du paragraphe a été revue pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait l'évaluation par le CST de l'étendue des attaques par rançongiciel comparativement à tous les cybercrimes qui

---

[94] CCC, « Canada's Cyber Threat Landscape: Overview and Outlook for 2019 », 2019.
[95] CST, *Rapport annuel de cyberdéfense 2017*, 2018; et CCC, *Rapport sur les cybermenaces : Tendances du ciblage des activités parrainées par un État, Rapport annuel de 2018*, 2019.
[96] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 2020.
[97] CST, *Rapport annuel sur les cybermenaces*, 2015; CST, *Rapport annuel de cyberdéfense*, 2016; CST, *Rapport annuel de cyberdéfense*, 2017; CCC, *Rapport sur la cyberdéfense : Vulnérabilités et compromissions TI au gouvernement du Canada*, 2019; et CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[98] CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020. Lorsqu'il a expliqué ce point, le CST a indiqué que ***.

prennent les réseaux du gouvernement pour cible. Bien qu'elle soit faible, le CST a noté que même une seule compromission par rançongiciel fructueuse pourrait être dommageable pour un ministère. Il a donné en exemple une attaque récente contre un ministère, qui a été endiguée, et une autre contre une société d'État, qui a entraîné des dommages considérables. Le paragraphe indiquait que le gouvernement étudie une politique concernant le paiement de rançons à des pirates informatiques. ***][99] [100] [101]

Résumé

67. Les réseaux du gouvernement du Canada font partie intégrante de l'infrastructure essentielle du Canada et permettent au gouvernement de recueillir et de détenir de l'information, ainsi que de fournir des services essentiels pour la population et les entreprises canadiennes. L'information que détient le Canada représente également une grande valeur pour ses adversaires, y compris les auteurs de cybermenace parrainés par un État et les cybercriminels. En cette ère numérique, la quasi-totalité de ce que détient le gouvernement et de ce qu'il en fait peut être la cible de cyberactivités malveillantes — allant d'un vaste éventail de données sur les entreprises et les citoyens du Canada aux processus numériques qui sous-tendent les nombreux services et avantages dont dépendent les Canadiens et les Canadiennes. Les prochaines parties décrivent les efforts du gouvernement visant à renforcer ses mesures de cyberdéfense et à diminuer les vulnérabilités du Canada.

---

[99] CCC, *Operational Threat Report: 2019 Annual Threat Landscape*, 2020.
[100] CST, « NSICOP Cyber Defence Review, RFI-3, Ransomware and GC Depts », 2021.
[101] Secrétariat du Conseil du Trésor du Canada (SCT), commentaires d'un cadre supérieur lors d'une réunion du Secrétariat du CPSNR, 23 mars 2021; et SCT, « NSICOP Review - TBS Comments on Draft Final Report (9-July-2021) », p. 1, 9 juillet 2021.

Partie II : Évolution du cadre de cyberdéfense du gouvernement du Canada

68. On peut qualifier l'évolution du cadre de cyberdéfense du gouvernement du Canada comme ayant été non anticipée, réactive, délibérée et planifiée. Des modifications législatives ont établi de nouveaux pouvoirs, qui ont servi de moteur à l'élaboration d'activités visant à renforcer la sécurité des systèmes gouvernementaux et, au bout du compte, à mieux les défendre. Au même moment, les principaux auteurs de cybermenace ont forcé le gouvernement à adapter ses moyens de défense, surtout à la suite de graves cyberincidents ayant causé d'importantes pertes de données et fait ressortir la vulnérabilité de certains ministères ainsi que du gouvernement de manière plus générale. En réponse, le gouvernement a adopté des politiques et des stratégies clés; a investi dans la modernisation des technologies de l'information et des moyens de cyberdéfense; et a mis sur pied des organisations chargées de se pencher sur les faiblesses du système. De ce fait, le gouvernement s'est progressivement écarté de son approche cloisonnée selon laquelle les différents ministères, peu importe leur taille, étaient chargés d'assurer leur propre cyberdéfense; pour plutôt considérer le gouvernement comme étant une « entreprise » au sein de laquelle des organisations précises se chargent de diriger la mise en œuvre de politiques dans l'ensemble du gouvernement et d'offrir des services de « défense en profondeur » afin de protéger le gouvernement à titre d'organisation.

Les premiers temps (de 2001 à 2010)

69. L'origine de la cyberdéfense au Canada était de nature législative.
Le 18 décembre 2001, le Parlement a adopté la *Loi antiterroriste*. Comme son nom l'indique, la loi a été mise en œuvre en réponse aux attaques terroristes de septembre 2001. Pour le Centre de la sécurité des télécommunications (CST), cela signifiait que son mandat et ses pouvoirs étaient prévus par la loi (la *Loi sur la défense nationale*)[102], lui permettant ainsi d'élargir ses activités liées au renseignement à l'étranger à l'appui, entre autres, de la lutte contre al-Qaïda. Par le fait même, la loi établissait des pouvoirs généraux permettant au CST d'offrir des conseils, des directives et des services visant à protéger l'information électronique et les infrastructures d'information importantes aux yeux du gouvernement, notamment les autorisations ministérielles pour les activités pouvant mener à l'interception de communications privées. Au fil du temps, ces pouvoirs ont permis au CST de mettre sur pied et de mener des activités de cyberdéfense novatrices sur les systèmes ou les réseaux informatiques du gouvernement, notamment des activités de mise à l'essai de mécanismes actifs de sécurité réseau visant à *mesurer* l'état de sécurité de certains systèmes et réseaux gouvernementaux,

[102] *Loi sur la défense nationale*, L.R.C. (1985), ch. 95, paragraphes 273.64(1) et 273.64(2) (avant l'adoption du projet de loi C-59 et de la *Loi sur le Centre de la sécurité des télécommunications*), http://laws-lois.justice.gc.ca/fra/lois/n-5/20181218/P1TT3xt3.html.

de même que des activités de cyberdéfense visant à *protéger* certains systèmes et réseaux du gouvernement[103].

Mise à l'essai de mécanismes actifs de sécurité réseau et évaluations de la posture

70. De 2002 à 2012, le CST a mené des activités de mise à l'essai de mécanismes actifs de sécurité réseau pour les ministères. Dans le cadre de ces activités, le CST s'est servi de diverses méthodes techniques *non classifiées* pour pénétrer dans les systèmes informatiques d'une organisation gouvernementale et ainsi cerner les vulnérabilités et les faiblesses du réseau, et pour tester la réaction d'un ministère face à une cybermenace active. Ces essais de « pénétration » ont été conçus pour déterminer si un auteur de cybermenace (joué par le CST) était en mesure d'accéder à un réseau et d'obtenir des documents classifiés ou sensibles qui n'auraient pas dû être accessibles au public. On s'est servi des résultats pour formuler des recommandations visant à remédier aux faiblesses[104].

71. Le CST a mené ses premières activités en vertu d'autorisations ministérielles en 2002. Il a recherché des vulnérabilités relatives *** à ses propres réseaux, puis mis à l'essai ses réseaux ***, de même que ceux du Bureau du Conseil Privé, pour y déceler des faiblesses[105]. En novembre 2002 et en avril 2003, le CST a obtenu des autorisations ministérielles de soumettre respectivement les réseaux du Service canadien du renseignement de sécurité (SCRS) et du ministère des Affaires étrangères et du Commerce international à des essais similaires. Des suites de cette expérience, le CST a commencé à se servir véritablement de ses pouvoirs. De 2002 à 2006, le CST a obtenu 11 autorisations ministérielles pour effectuer des activités de mise à l'essai et d'évaluation des systèmes pour les organisations suivantes :

- le ministère de la Défense nationale, y compris *** (octobre 2002);
- la Gendarmerie royale du Canada (juin 2003);
- le Bureau du Conseil privé (novembre 2003);
- l'Agence des douanes et du revenu du Canada (décembre 2003);
- le ministère du Développement des ressources humaines (janvier 2004);
- le ministère de la Défense nationale (janvier 2004);
- le ministère de l'Industrie (mai 2004);

---

[103] *Loi sur la défense nationale*, L.R.C. (1985), ch. 95, paragraphe 273.65(9) (avant l'adoption du projet de loi C-59 et de la *Loi sur le Centre de la sécurité des télécommunications*), http://laws-lois.justice.gc.ca/fra/lois/n-5/20181218/P1TT3xt3.html. La Loi limitait explicitement l'application du régime des autorisations ministérielles aux « institutions fédérales », comme définies dans la *Loi sur les langues officielles*.

[104] Commissaire du CST, *Examen combiné des activités du CST dans le cadre des autorisations ministérielles de 2009-2010, 2010-2011 et 2011-2012 sur la mise à l'essai des mécanismes actifs de sécurité réseau et les opérations de cyberdéfense*, 31 mars 2015. Les méthodes utilisées pour mettre à l'essai les mécanismes actifs de sécurité réseau dépendaient de cyberoutils connus des pirates informatiques à l'époque. ***

[105] CST, « Security Posture Assessment », autorisation ministérielle, 23 avril 2002; CST, « Security Posture Assessment: CSE and PCO », autorisation ministérielle, 23 avril 2002; et CST, « Request for Ministerial Authorization. Protection of CSIS Information Systems and Networks », note à l'intention du ministre de la Défense nationale, 25 octobre 2002.

- *** (octobre 2004);
- le CST, y compris les réseaux du Bureau du commissaire du CST (avril 2005);
- le Bureau du Conseil privé (février 2006);
- le ministère de la Défense nationale (février 2006)[106].

Ces activités ont été interrompues en octobre 2006. Lorsqu'elles ont repris en décembre 2007, le CST s'est servi d'une nouvelle approche (paragraphes 74 à 76).

L'origine des activités de défense des réseaux informatiques

72. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] De 2004 à 2006, le CST a commencé à mener des activités qui allaient constituer la base de son programme de cyberdéfense. À la fin de 2003, le ministère de la Défense nationale (MDN) a signalé des intrusions (plus tard, il a été déterminé qu'il s'agissait de la Russie) dans ses systèmes et a demandé l'aide du CST. En janvier 2004, le CST a demandé une autorisation ministérielle pour mener des activités de mise à l'essai de mécanismes actifs de sécurité réseau sur le réseau du MDN et pour mettre en place des mesures de cyberdéfense visant à cerner les tentatives d'exploitation ainsi qu'à surveiller les activités de l'auteur de cybermenace sophistiqué[107]. Au cours de la même année, le CST et Affaires étrangères Canada (AEC) ont suivi les tentatives de la Chine visant à compromettre le réseau d'AEC. En juin 2005, le CST a demandé une autorisation ministérielle pour installer des cyberoutils sur les systèmes d'AEC[108].

73. En 2006, le CST a reçu des autorisations ministérielles pour mener des activités de défense des réseaux informatiques pour les réseaux du MDN (février), les réseaux d'AEC (juin) et ses propres réseaux (juin). Le CST a imputé les attaques de plus en plus sophistiquées contre les réseaux du MDN à la Chine, et les attaques contre les réseaux d'AEC à la Chine et à la Russie. Comme il l'avait fait *** en 2004, le CST *** a déployé des outils pour renforcer sa capacité de détecter les cyberattaques avancées contre les réseaux du gouvernement, d'intervenir face à ces cyberattaques, et de retracer l'origine (étrangère) des attaques détectées dans le cadre des activités liées au renseignement à l'étranger du CST[109]. Ainsi ont commencé

---

[106] CST, « Security Posture Assessment: CSIS », autorisation ministérielle, 2 novembre 2002; et CST, « Protection of the Computer Systems or Networks of the Government of Canada (DFAIT) », autorisation ministérielle, 26 mars 2013.

[107] CST, « Protection of Computer Systems and Networks of the Department of National Defence », autorisation ministérielle, 19 janvier 2004; CST, « Request for Ministerial Authorization. Protection of DND Computer Systems and Networks », note à l'intention du ministre de la Défense nationale, 19 janvier 2004; et Commissaire du CST, *Examen combiné des activités du CST au titre des autorisations ministérielles de 2009-2010, 2010-2011 et 2011-2012 sur la mise à l'essai des mécanismes actifs de sécurité réseau et les opérations de cyberdéfense*, 31 mars 2015.

[108] CST, « Request for Ministerial Authorization. Protection of Government of Canada Computer Systems and Networks: Foreign Affairs Canada », note à l'intention du ministre de la Défense nationale, 16 juin 2005; et CST, « Protection of Government of Canada Computer Systems and Networks: Foreign Affairs Canada », autorisation ministérielle, 22 juin 2005.

[109] CST, « Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks. Communications Security Establishment », note à l'intention du ministre de la Défense nationale, juin 2006; et CST, « Protection of Government of Canada Computer Systems and Networks », autorisation ministérielle, 13 juin 2006.

les activités avancées de défense des réseaux informatiques au sein du gouvernement du Canada, qui sont maintenant appelées les « activités de cyberdéfense ».

Dures leçons apprises en cours de route

74. En octobre 2006, le CST a interrompu toutes ses activités de mise à l'essai de mécanismes actifs de sécurité réseau et de défense des réseaux informatiques. Comme l'a ensuite expliqué le commissaire du CST :

> [traduction] Le CST n'a pas respecté toutes les exigences et les conditions prévues par ses autorisations ministérielles pendant la période allant de juin 2005 à octobre 2006. La direction n'a pas suffisamment porté attention aux conditions des autorisations ministérielles, à leur communication et à leur respect. Le cadre de contrôle à l'intention des personnes qui effectuent ces activités n'était pas assez clair, cohérent, exhaustif ou récent. L'ensemble des répercussions de ces enjeux ont fait en sorte de remettre en doute le respect de la *Loi sur la protection des renseignements personnels* et de la *Loi sur la défense nationale* par le CST[110].

Le CST a examiné son programme et a mis en œuvre plusieurs changements au cours de l'année en vue de restructurer ses activités et son cadre stratégique et d'améliorer la surveillance et la responsabilisation du programme.

75. En décembre 2007, le CST a demandé une autorisation ministérielle en vue de reprendre ses activités de mise à l'essai de mécanismes actifs de sécurité réseau. Le CST a laissé tomber les demandes d'autorisation individuelles pour chaque ministère et a adopté une approche globale consistant à obtenir une seule autorisation ministérielle lui permettant de réaliser des évaluations de la sécurité réseau à la demande d'un ministère, conformément à la Politique du gouvernement sur la sécurité du Conseil du Trésor[111]. Le CST a offert ces services aux ministères jusqu'en 2012, lorsqu'il fut apparent que la valeur relative des essais de pénétration dans les réseaux fût en baisse (le CST était *toujours* en mesure de pénétrer dans les réseaux des organisations visées). Le CST s'est alors entièrement consacré aux activités de cyberdéfense, dans le cadre desquelles il accomplissait des progrès considérables pour cerner et bloquer des cyberattaques complexes à l'aide de ses méthodes de cyberdéfense.

76. En mars 2008, le ministre de la Défense nationale a approuvé une demande globale semblable visant à obtenir une autorisation ministérielle pour reprendre les activités de défense des réseaux informatiques sur les réseaux du gouvernement afin d'assurer une protection

---

[110] Commissaire du CST, *Examen combiné des activités du CST au titre des autorisations ministérielles de 2009-2010, 2010-2011 et 2011-2012 sur la mise à l'essai des mécanismes actifs de sécurité réseau et les opérations de cyberdéfense*, 31 mars 2015.

[111] CST, « Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks », note à l'intention du ministre de la Défense nationale, 21 décembre 2007; CST, « Protection of Government of Canada Computer Systems and Networks », autorisation ministérielle, 21 décembre 2007; et SCT, Politique sur la Sécurité, février 2002, www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12322.

contre le vol de renseignements sensibles par des cyberacteurs sophistiqués. Le CST a constaté que des adversaires très expérimentés, surtout la Chine et la Russie, s'en prenaient à un nombre de plus en plus élevé de ministères. L'autorisation permettait au CST de mener cinq types d'activités de défense des réseaux informatiques :

- **analyse d'incidents :** mener des enquêtes sur les alertes lorsque le système de détection d'intrusion du CST signale de possibles menaces;
- **analyse d'anomalies :** créer des profils normalisés des ministères et du trafic sur leurs réseaux en vue de cerner des comportements inhabituels pouvant indiquer des activités malveillantes;
- **analyse judiciaire d'intrusions :** examiner en profondeur les intrusions malveillantes dans le réseau pour cerner de possibles dommages au réseau du gouvernement;
- **signalement d'incidents :** formuler des conseils d'atténuation en réponse aux intrusions cernées;
- **élaboration d'outils avancés :** renforcer les outils de détection d'intrusion classifiés du CST en fonction de l'analyse des cyberactivités malveillantes afin d'améliorer la détection de cybermenaces[112].

Comme décrit plus loin, ce changement a permis au CST d'installer ses capteurs sur le Réseau de la Voie de communication protégée du gouvernement du Canada et ainsi de regrouper l'accès Internet de plus de 70 ministères. De cette manière, le CST a pu découvrir que la Chine avait porté atteinte à certains ministères et volé d'importantes quantités de données. Cette découverte a entraîné bon nombre de changements au cours des années suivantes (décrits ci-dessous), notamment le fait d'appliquer les mesures de cyberdéfense du CST à un plus grand nombre de ministères[113]. Pour sa part, le CST continue d'offrir ses activités de défense des réseaux informatiques aux ministères, et ce, en vertu d'autorisations ministérielles successives depuis 2008. Ces activités, aujourd'hui connues sous le nom d'activités de cyberdéfense, sont décrites de manière plus détaillée dans la partie sur le CST (paragraphes 154 à 212).

Politiques du gouvernement du Canada en matière de cyberdéfense

77. De 2001 à 2010, le gouvernement a instauré deux politiques présentant un intérêt particulier pour la cyberdéfense : la Politique du gouvernement sur la sécurité en 2002 et la Politique de sécurité nationale en 2004. La Politique du gouvernement sur la sécurité visait à appuyer l'intérêt national et les objectifs opérationnels du gouvernement du Canada tout en assurant la sécurité des employés et des biens ainsi que la prestation continue des services. Selon la politique, les administrateurs généraux étaient chargés d'assurer la sécurité des employés et des biens sous leur responsabilité, et devaient respecter certaines exigences de base en matière de sécurité établies dans la politique. Parmi les exigences auxquelles les

[112] CST, « Request for Ministerial Authorization: Protection of Government of Canada Computer Systems and Networks », note à l'intention du ministre de la Défense nationale, 29 février 2008; et CST, « Defence of Government of Canada Computer Systems and Networks », autorisation ministérielle, 11 mars 2008.
[113] SPC, « SCNet Enterprise Internet – 2010 and 2011 », communiqué de la DGDPI du SCT, 24 février 2021.

ministères devaient se plier, on comptait la nomination d'un agent de sécurité ministérielle dans le but d'établir un programme de sécurité permettant d'assurer la coordination de toutes les fonctions de la politique, notamment la sécurité des technologies de l'information, le filtrage de sécurité et le contrôle des accès. La Politique du gouvernement sur la sécurité exigeait des ministères qu'ils mettent en place des contrôles de sécurité de référence en matière de technologie de l'information visant à prévenir et à détecter les atteintes aux systèmes de technologie de l'information, à intervenir face à celles-ci et à redresser la situation. Qui plus est, les ministères devaient évaluer périodiquement leurs systèmes de technologie de l'information; surveiller continuellement les activités de ces systèmes pour détecter les anomalies relatives aux niveaux de prestation de services; mettre en place des mécanismes pour intervenir efficacement face aux incidents liés aux technologies de l'information, le cas échéant; et échanger de l'information liée à ces incidents avec les ministères responsables en temps opportun[114]. Le Conseil du Trésor a modifié la Politique du gouvernement sur la sécurité en 2009, puis une autre fois en 2019, lorsqu'il l'a renommée « Politique sur la sécurité du gouvernement ». La pertinence et l'application actuelles de la politique sont décrites aux paragraphes 103 à 106.

78. La Politique de sécurité nationale du gouvernement prévoyait un cadre stratégique et un plan d'action permettant de veiller à ce que le gouvernement soit prêt à intervenir face à un éventail de menaces envers la sécurité nationale. Selon la politique, les cyberattaques représentent : « un sujet croissant de préoccupation, car elles peuvent avoir un impact sur divers types d'infrastructures essentielles reliées par des réseaux informatiques ». Le document présentait également deux initiatives visant à éliminer cette menace : premièrement, améliorer considérablement les analyses des menaces et des vulnérabilités pour les systèmes du gouvernement et renforcer la capacité de défendre les systèmes du gouvernement contre les attaques; deuxièmement, élaborer une stratégie nationale de cybersécurité[115]. Ces initiatives ont été financées dans les budgets d'années ultérieures.

Établissement de l'entreprise du gouvernement du Canada (de 2010 à 2018)

79. La période allant de 2010 à 2018 a joué un rôle essentiel dans l'établissement du cadre de cyberdéfense du gouvernement. Pendant cette période, le gouvernement a déployé deux stratégies nationales de cybersécurité et a alloué une quantité substantielle de financement à la cyberdéfense et à la cybersécurité. Le gouvernement a également apporté d'importants changements à sa structure organisationnelle en créant Services partagés Canada et le Centre canadien pour la cybersécurité (CCC). Au même moment, des cyberattaques d'envergure constituaient d'importants moteurs de changement, notamment le déploiement des capteurs du CST sur les réseaux du gouvernement et le regroupement des points d'accès à

[114] SCT, « Politique sur la Sécurité », février 2002, www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12322. La politique s'appliquait à tous les ministères énumérés aux annexes I, I.1 et II de la *Loi sur la gestion des finances publiques*.
[115] Bureau du Conseil privé, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, avril 2004, www.publications.gc.ca/collections/Collection/CP22-77-2004F.pdf.

Internet et des centres de données du gouvernement. Le gouvernement a également mis en place des mécanismes pour gérer la cyberdéfense et préciser les rôles et les responsabilités des intervenants du cadre de cyberdéfense. Les changements sont décrits ci-dessous.

Stratégie de cybersécurité du Canada de 2010

80. En octobre 2010, le gouvernement a mis sur pied la Stratégie de cybersécurité du Canada dans le but de défendre la population canadienne, les entreprises canadiennes et l'économie contre les cybermenaces. La stratégie comportait trois piliers :

- **sécuriser les systèmes du gouvernement :** vise à renforcer la capacité du gouvernement de prévenir et de détecter les cybermenaces, ainsi que d'intervenir face à celles-ci et de redresser la situation;
- **nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral :** vise à renforcer la cyberrésilience au Canada, notamment pour les secteurs de l'infrastructure essentielle;
- **aider les Canadiens et les Canadiennes à se protéger en ligne :** vise à favoriser la sensibilisation du public, à informer les Canadiens et les Canadiennes sur les moyens de se protéger en ligne et à renforcer la capacité des organismes d'application de la loi de lutter contre la cybercriminalité[116].

On a accordé plus de 244 millions de dollars en financement sur cinq ans pour la stratégie, puis 60 millions de dollars par année par la suite[117]. Le premier pilier (sécuriser les systèmes du gouvernement) constituait le plus pertinent sur le plan de la cyberdéfense et a permis d'obtenir trois résultats notables : renforcer le programme de cyberdéfense du CST, créer Services partagés Canada et mettre en œuvre une gouvernance et des politiques améliorées. Chacun de ces éléments est abordé ci-dessous.

Renforcer le programme de cyberdéfense du CST

81. Le principal objectif du premier pilier de la stratégie consistait à accroître les cybercapacités du gouvernement en matière d'enquête, d'analyse du renseignement et de technologie. La majeure partie du financement, c'est-à-dire 205 millions de dollars sur cinq ans (84 % du financement total pour la stratégie) a été alloué au CST dans le but d'améliorer sa capacité de défendre les réseaux et les systèmes du gouvernement. Le financement a notamment servi à installer de nouveaux capteurs réseau afin de surveiller les réseaux des ministères pour détecter les cybermenaces et automatiquement empêcher les cyberattaques, et à développer des capteurs sur l'hôte, un logiciel conçu pour défendre les appareils individuels du gouvernement[118].

---

[116] Canada, *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, 2015.
[117] Sécurité publique Canada, « Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date », 2015.
[118] Sécurité publique Canada, « Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date », 2015.

82. Ces investissements ont permis de nettement améliorer les capacités de cyberdéfense du CST. Avant la mise en œuvre de la stratégie, le programme de cyberdéfense du CST était axé sur l'intervention face aux incidents et l'atténuation de ceux-ci, ce qui nécessitait un traitement manuel laborieux et l'établissement de rapports ponctuels à l'intention de chaque client. Le déploiement de la défense dynamique basée sur le réseau en 2013 a permis au CST de mieux analyser et surveiller l'information sur les menaces pouvant servir à empêcher de manière proactive que les cyberattaques atteignent les systèmes et les utilisateurs du gouvernement en bloquant les attaques au périmètre du réseau du gouvernement. Les avantages de cet outil ont été soulignés en 2014 lorsque le CST a déployé ses capteurs réseau de défense dynamique sur le Réseau de la Voie de communication protégée de Services partagés Canada à l'appui des mesures prises par le gouvernement en vue d'atténuer une importante cybervulnérabilité (voir l'étude de cas 3 sur HEARTBLEED). Dans le cadre de la stratégie, le CST a mis sur pied le Centre d'évaluation des cybermenaces dans le but d'améliorer sa connaissance et sa compréhension des cybermenaces complexes ciblant les systèmes gouvernementaux[119]. Ainsi, le CST a été en mesure d'assurer un meilleur suivi des cybertendances et des cybermenaces connues et d'établir de meilleurs rapports à cet égard, en plus d'automatiser la découverte des cybermenaces et le déploiement des mesures de cyberdéfense[120]. L'élaboration du programme de cyberdéfense du CST a contribué à une expansion constante de la visibilité des réseaux du gouvernement pour le CST, tout en diminuant le nombre de tentatives d'exfiltration de données réussies[121].

Créer Services partagés Canada

83. La création de Services partagés Canada (SPC) a facilité la mise en œuvre des objectifs énoncés dans la Stratégie de cybersécurité du Canada[122]. Ce changement a grandement contribué à l'évolution de l'architecture de cyberdéfense du gouvernement, puisqu'il a permis de regrouper les ressources en matière de technologie de l'information de 42 ministères (environ 95 % des ressources fédérales) et d'accélérer l'adoption d'une approche d'entreprise en ce qui a trait à la cybersécurité. De manière générale, SPC est chargé de concevoir et de gérer l'infrastructure des technologies de l'information sécuritaire qui protège les données et les biens technologiques du gouvernement; d'élaborer des politiques, des normes, des plans et des modèles en matière de sécurité; et d'offrir des services liés à la sécurité pour la prestation des services du gouvernement[123]. Dans le cadre de la stratégie, SPC a amélioré sa capacité en matière de surveillance des menaces, d'évaluation des vulnérabilités et de prestation de services d'informatique judiciaire pour ses 43 principaux partenaires; et a déployé de nouveaux outils pour appuyer la gestion du volume grandissant de cybermenaces (voir la partie sur SPC

---

[119] Sécurité publique Canada, « Canada's Cyber Security Strategy: Funding Allocations and Accomplishments to Date », 2015.
[120] CST, « Cyber Threat Evaluation Centre Overview », mars 2015.
[121] CST, *Year Review Cyber Defence Report 2017*, 2018.
[122] Canada, « Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada », 2013, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-fr.aspx.
[123] SPC, « Cybersécurité et sécurité de la technologie de l'information », 2015, www.canada.ca/fr/services-partages/organisation/cybersecurite-securite-technologie-information.html.

aux paragraphes 126 à 153)[124]. Il convient de noter que SPC a également regroupé plus de 720 centres de données gouvernementaux en 381 centres, dans le but de passer à quatre centres d'activité régionaux, et a réduit le nombre de points d'accès à Internet d'une centaine à deux — il prévoit ajouter trois centres régionaux (comptabilisant cinq connexions protégées) et peut-être trois centres internationaux. Le fait de réduire le nombre de points de vulnérabilité a facilité la protection de l'ensemble de la cyberentreprise du gouvernement. Par l'entremise de son Centre de protection de l'information du gouvernement, SPC a assuré la surveillance des menaces, coordonné tous les incidents de sécurité touchant l'infrastructure soutenue par SPC et regroupé les incidents signalés par ses principaux partenaires. La création de SPC et le regroupement des ministères sous un modèle d'entreprise du gouvernement ont permis au gouvernement de mieux connaître les cybermenaces et les vulnérabilités et d'établir des conditions pour assurer un déploiement plus uniforme des capteurs de cyberdéfense avancés du CST[125].

Mettre en œuvre une gouvernance et des politiques améliorées

84. La gouvernance comptait également parmi les principaux éléments de la stratégie de cybersécurité de 2010. Avant la création de la stratégie, la gouvernance de la cyberdéfense était marquée par un manque de clarté concernant les rôles et les responsabilités de même que par un modèle décentralisé et ponctuel selon lequel les sous-ministres devaient se charger individuellement de la cybersécurité et de la cyberdéfense de leurs organisations respectives[126]. L'un des objectifs de la stratégie de 2010 consistait à définir clairement les rôles et les responsabilités pour la gestion des cyberincidents. À cette fin, Sécurité publique Canada et le CST ont harmonisé leurs responsabilités relatives à la gestion et à la coordination des incidents, faisant en sorte que Sécurité publique Canada soit responsable de la gestion de la cybersécurité pour les organisations non fédérales, notamment de la prestation de conseils stratégiques à d'autres niveaux du gouvernement (à l'époque, la Stratégie était axée sur les engagements avec les gouvernements provinciaux et territoriaux) et à des organismes du secteur privé; et que le CST soit responsable de la réalisation des activités liées à la cybersécurité et de la gestion des incidents relatifs aux systèmes gouvernementaux[127].

85. De son côté, le Secrétariat du Conseil du Trésor du Canada (SCT) a mis sur pied trois comités de gouvernance pour assurer la gouvernance en matière de sécurité des technologies de l'information pour les initiatives horizontales sous le premier pilier de la stratégie de 2010. Connus comme le groupe tripartite sur la sécurité des technologies de l'information, ces comités étaient composés respectivement de directeurs généraux, de sous-ministres adjoints et de sous-ministres. Ils sont décrits plus en détail aux paragraphes 221 à 223. Le SCT a également

---

[124] Sécurité publique Canada, « Update on the Implementation of the 2010 Cyber Security Strategy », 2011.
[125] Sécurité publique Canada, *Progress Report on Canada's Cyber Security Strategy: Horizontal Initiative for 2012-13 and 2013-14*, sans date; et Sécurité publique Canada, *Horizontal Evaluation of Canada's Cyber Security Strategy. Final Report*, 29 septembre 2017.
[126] Sécurité publique Canada, « Cyber Operations Working Group Terms of Reference », 2010; et Sécurité publique Canada, « Options for Government of Canada: Centralized Cyber Security Functions », 2010.
[127] CST et Sécurité publique Canada, *Memorandum of Understanding Between The Communications Security Establishment Canada and Public Safety Canada Concerning Cyber Security Roles and Responsibilities*, 2011.

dirigé l'élaboration d'un plan de gestion des incidents en matière de technologie de l'information amélioré pour permettre au gouvernement d'intervenir de manière plus rapide et cohérente face aux incidents de cybersécurité. Le plan comportait une description des rôles et des responsabilités des ministères quant au signalement des incidents en matière de technologie de l'information et à l'intervention face à ceux-ci; des protocoles horizontaux officiels en matière d'établissement de rapports, d'intervention et d'avertissement; ainsi qu'une liste de dirigeants et de comités de direction désignés avec qui communiquer lorsque les menaces s'intensifient[128]. La gouvernance de la gestion des incidents a encore évolué en 2015 lorsque le gouvernement a remplacé le plan par un nouveau plan de gestion des événements en matière de cybersécurité (paragraphes 224 à 236).

86. En ayant une compréhension des rôles et des responsabilités et une coordination ministérielle améliorées, le gouvernement a créé certains mécanismes de gouvernance interministériels. Le Comité des sous-ministres sur la cybersécurité constituait le principal mécanisme de gouvernance pour les questions stratégiques, avec l'appui de comités aux niveaux des sous-ministres adjoints et des directeurs généraux. Les trois comités étaient présidés par des cadres supérieurs de Sécurité publique Canada et composés de membres de la haute direction du CST, du SCT, de SPC, du SCRS, de la Gendarmerie royale du Canada, du MDN et des Forces armées canadiennes ainsi que du Bureau du Conseil privé. Le Comité des sous-ministres sur la cybersécurité avait pour objectif d'établir une orientation stratégique pour les questions liées à la cybersécurité; de déterminer les priorités liées à la cybersécurité des ministères et organismes membres; et d'examiner les questions émergentes en matière de cybersécurité[129]. En ce qui concerne les résultats, une évaluation effectuée en 2016 a permis de constater que cette structure de gouvernance était propice à la collaboration, à la coordination et à l'échange d'information entre les organisations participantes, et contribuait à mettre au clair les rôles et les responsabilités des ministères. Toutefois, en l'absence de documentation convenable, l'évaluation n'a pas permis de déterminer la mesure dans laquelle les organismes de gouvernance remplissaient leurs fonctions, comme tenir des réunions régulières. Dans le cadre de l'évaluation, on a également remarqué que l'incertitude quant aux rôles et aux responsabilités persistait, ce qui constituait une source de confusion chez les intervenants des ministères, des organismes et du secteur privé, et que l'échange d'information était fait sur une base sélective ou ponctuelle puisqu'il n'y avait aucune politique en place[130].

87. Le SCT a appuyé la gouvernance efficace et l'intervention face aux cyberincidents en établissant des normes, des lignes directrices et des politiques opérationnelles. En 2016, le SCT a publié le plan stratégique en matière de technologie de l'information. Ce plan oriente les organisations fédérales en ce qui a trait à la prise de décisions et à l'établissement de priorités liées aux technologies de l'information, notamment dans le domaine de la sécurité des technologies de l'information. Les initiatives prioritaires pertinentes dans ce domaine

---

[128] Secrétariat du Conseil du Trésor, *Government of Canada Information Technology Incident Management Plan*, 2009.
[129] Sécurité publique Canada, *Comité de sous-ministres sur la cybersécurité – mandat*, mars 2015.
[130] Sécurité publique Canada, *Rapport final de l'Évaluation horizontale de la Stratégie de cybersécurité du Canada*, 2017, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-fr.aspx.

comprennent de sécuriser le périmètre du réseau du gouvernement, de mettre en œuvre des profils de sécurité aux terminaux et d'adopter une approche systématique pour la gestion des correctifs et des vulnérabilités[131]. Le SCT a également publié la première version du Plan stratégique des opérations numériques en 2018, qui donne des directives aux ministères quant aux priorités liées à la gestion intégrée des services, de l'information, des données, des technologies de l'information et de la cybersécurité. En ce qui concerne la cybersécurité et la cyberdéfense, le plan prévoit l'élaboration d'une approche à niveaux multiples qui comprend des points d'interconnexion fiables pour servir de passerelle vers les services infonuagiques[132].

Évolution de la Stratégie de cybersécurité du Canada

88. En 2015, le gouvernement a renouvelé la stratégie de cybersécurité de 2010. Ce renouvellement a marqué la deuxième phase de la stratégie et visait à examiner trois difficultés. Tout d'abord, l'environnement de cybermenace stratégique avait considérablement évolué avec l'émergence d'auteurs de cybermenace plus expérimentés et l'augmentation de la prolifération des cyberoutils. Ensuite, la cybersécurité est devenue un enjeu économique d'envergure puisque les auteurs de cybermenace ciblaient de plus en plus les entreprises canadiennes. Enfin, il existait un besoin grandissant d'assurer la sécurité des Canadiens et des Canadiennes en ligne au moyen de meilleures connaissances sur les technologies numériques et de nouvelles approches relatives à la cybercriminalité. Pour aborder ces difficultés, le gouvernement a financé trois initiatives :

- accroître l'analyse et la collecte du renseignement relatif aux cybermenaces pour communiquer de l'information concernant les menaces avec les intervenants chargés des systèmes du secteur privé et de l'infrastructure essentielle;
- nouer un plus grand nombre de partenariats avec des fournisseurs de services de télécommunication afin d'évaluer les cybervulnérabilités et les dépendances de l'infrastructure essentielle;
- dédier des ressources de l'application de la loi pour mener des enquêtes et perturber la cybercriminalité de manière plus efficace[133].

Ces initiatives relèvent du deuxième et du troisième pilier de la stratégie de cybersécurité de 2010 (nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral, et aider les Canadiens et les Canadiennes à se protéger en ligne), qui avaient reçu moins de financement. Du financement a également été spécialement consacré à

---

[131] SCT, « Le Plan stratégique de la technologie de l'information du gouvernement du Canada 2016-2020 », 2016, www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/strategie-technologie-information/plan-strategique-2016-2020.html.

[132] Pour obtenir de plus amples renseignements, consulter le *Plan stratégique des opérations numériques de 2018 à 2022* du Secrétariat du Conseil du Trésor, 29 mars 2019, www.canada.ca/fr/gouvernment/systeme/gouvernement-numérique/plan-strategique-operations-numerique-2018-2022.html.

[133] Sécurité publique Canada, « Renewal of Canada's Cyber Security Strategy », 20 août 2015.

la résolution des lacunes en matière de sécurité relevées à la suite de la cyberattaque de la Chine contre le Conseil national de recherches en 2014 (voir l'étude de cas 4)[134].

89. En juin 2018, le gouvernement a annoncé la nouvelle Stratégie nationale de cybersécurité. La stratégie de 2018 était axée sur une évaluation à l'échelle du gouvernement de la stratégie de 2010 et comprenait les commentaires d'experts du secteur privé, d'organismes de l'application de la loi et d'universitaires. La stratégie de 2018 présentait trois objectifs à atteindre pour assurer la sécurité et la prospérité à l'ère numérique :

- **des systèmes canadiens sécuritaires et résilients :** vise à améliorer la capacité du gouvernement de protéger les Canadiens et les Canadiennes contre la cybercriminalité; d'intervenir face aux cybermenaces changeantes et de défendre les systèmes essentiels du gouvernement et du secteur privé;
- **un écosystème du cyberespace novateur et adaptable :** vise à appuyer la recherche, à favoriser l'innovation et à développer des compétences en matière de cybersécurité de sorte que le Canada soit reconnu comme étant un chef de file mondial en matière de cybersécurité;
- **une direction, une gouvernance et une collaboration efficaces :** vise à faire progresser la cybersécurité et la collaboration avec les alliés pour façonner l'environnement de cybersécurité international en la faveur du Canada[135].

Les investissements du budget de 2018 en matière de cybersécurité, qui s'élevaient à 508 millions de dollars sur cinq ans, puis à 109 millions de dollars par année par la suite, tenaient compte des objectifs et des initiatives clés de la stratégie de 2018. Plus particulièrement, le CST a reçu 155 millions de dollars sur cinq ans, puis 45 millions de dollars par année par la suite, pour mettre sur pied un nouveau centre pour la cybersécurité.

90. En réponse, le gouvernement a créé le Centre canadien pour la cybersécurité (CCC) en octobre 2018. Ce changement a permis de regrouper les rôles et les responsabilités de certaines cyberorganisations fédérales, comme le programme de sécurité des technologies de l'information du CST, les campagnes de sensibilisation du public et le Centre canadien de réponse aux incidents cybernétiques de Sécurité publique Canada, ainsi que certaines fonctions du Centre des opérations de sécurité de SPC. Voici les quatre principales responsabilités du CCC :

- **informer** la population canadienne des questions en matière de cybersécurité, notamment les menaces à la cybersécurité;
- **protéger** les intérêts du Canada en formulant des conseils, en offrant de l'aide et en collaborant avec des partenaires au Canada et à l'étranger;
- **défendre** les réseaux et les systèmes pour lesquels il a une notoriété;

---

[134] Sécurité publique Canada, « Renewal of Canada's Cyber Security Strategy », 20 août 2015.
[135] Sécurité publique Canada, « Introducing the 2018 National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age », sans date.

- **développer** et perfectionner les connaissances, le personnel et les compétences nécessaires afin d'améliorer en continu la cybersécurité pour les Canadiens et les Canadiennes[136].

Le CCC est destiné à servir d'unique source gouvernementale de conseils, d'orientation, de services et de soutien pour les questions opérationnelles relatives à la cybersécurité. Il agit à titre de responsable opérationnel du gouvernement face aux événements de cybersécurité et a pour but de mieux cibler et coordonner les interventions du gouvernement face aux cyberincidents et aux cybermenaces; d'améliorer la coordination des activités en matière de cybersécurité du gouvernement; et d'accroître l'efficacité des échanges d'information entre le gouvernement et les partenaires du secteur privé.

91. La stratégie de 2018 comprend des initiatives liées à la protection de l'infrastructure essentielle du Canada. Dans le cadre du plan d'action sur cinq ans de la stratégie, le CCC doit renforcer ses partenariats avec les responsables et les exploitants de l'infrastructure essentielle dans les secteurs des finances et de l'énergie pour permettre l'échange de connaissances et de capacités en matière de cybersécurité et ainsi assurer une meilleure défense contre les cybermenaces avancées[137]. De son côté, Sécurité publique Canada doit mettre en place une approche de gestion du risque exhaustive permettant aux responsables et aux exploitants de mieux sécuriser leurs systèmes et leurs informations. Enfin, la stratégie prévoit du financement pour que le SCRS augmente le nombre d'activités de collecte du cyberrenseignement et d'évaluation des cybermenaces afin de mieux comprendre la situation en matière de cybersécurité et de fournir des conseils au gouvernement concernant les questions pertinentes sur le plan de la cybersécurité[138].

92. Le cadre du gouvernement entourant les activités de cyberdéfense continue d'évoluer. En juin 2019, la *Loi sur le Centre de la sécurité des télécommunications* a reçu la sanction royale, entraînant d'importants changements au mandat, aux pouvoirs, aux immunités et à la surveillance du CST, y compris dans les domaines directement liés à la cyberdéfense. En avril 2020, le Conseil du Trésor a publié sa Politique sur les services et le numérique, établissant les règles selon lesquelles le gouvernement doit gérer la prestation des services, l'information et les données, les technologies de l'information et la cybersécurité à l'ère numérique. Ces changements seront abordés dans les prochaines parties sur le SCT et le CST, respectivement.

---

[136] CST, « Presentation to Col. Peyton », 10 avril 2018.
[137] Sécurité publique Canada, « Plan d'action national en matière de cybersécurité 2019-2024 », 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntl-cbr-scrt-strtg-2019/ntl-cbr-scrt-strtg-2019-fr.pdf.
[138] Sécurité publique Canada, « Plan d'action national en matière de cybersécurité 2019-2024 », 2019, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntl-cbr-scrt-strtg-2019/ntl-cbr-scrt-strtg-2019-fr.pdf.

Partie III : Intervenants, autorités et activités clés en matière de cyberdéfense

93. La cybersécurité est une responsabilité partagée dans l'ensemble du gouvernement. Chaque ministère est responsable de la sécurité de ses biens de technologie de l'information, mais trois organisations ont des obligations et offrent des services précis à l'ensemble du gouvernement, y compris en ce qui a trait au mandate particulier de la cyberdéfense. L'équipe tripartite chargée de la sécurité des technologies de l'information du gouvernement du Canada est formée du Secrétariat du Conseil du Trésor du Canada (SCT), qui relève du Conseil du Trésor, de Services partagés Canada et du Centre de la sécurité des télécommunications.

94. Les paragraphes qui suivent examinent en détail les rôles, les responsabilités, les fonctions et les activités liées à la cyberdéfense de l'équipe tripartite chargée de la sécurité des technologies de l'information. Ils présentent les responsabilités de chaque ministère en ce qui concerne la cybersécurité en adoptant une vision large de la portée des entités qui constituent le gouvernement du Canada. Une analyse des régimes législatifs, des politiques administratives et des autres pouvoirs des organisations tripartites en ce qui concerne la fourniture de services de cyberdéfense à des organismes gouvernementaux détermine les organismes qui peuvent recevoir des services de cybersécurité et de cyberdéfense, et dans quelle mesure. Cette approche permet d'obtenir une compréhension générale des responsabilités, des activités et de la fourchette de protection du cadre de cyberdéfense du gouvernement.

Conseil du Trésor du Canada et le Secrétariat du Conseil du Trésor du Canada

95. Créé sous forme de comité du Cabinet en 1869, le Conseil du Trésor du Canada joue un rôle fondamental dans le cadre de cyberdéfense du Canada. Le Conseil du Trésor prescrit les politiques, les normes et les directives en matière de cyberdéfense et détermine les organisations auxquelles les exigences s'appliquent. La loi habilitante du Conseil du Trésor, à savoir la *Loi sur la gestion des finances publiques* (LGFP), précise les rôles et les responsabilités des principaux représentants de l'ensemble du gouvernement et établit de façon générale un certain nombre des piliers stratégiques, administratifs et en matière de responsabilisation du cadre de cyberdéfense du gouvernement.

96. Le Conseil du Trésor est investi d'un vaste mandat pour l'ensemble du gouvernement. En vertu de la LGFP, il est garant de la responsabilisation ministérielle et de la gestion financière du gouvernement, de même que de la surveillance réglementaire des programmes et des services du gouvernement; il est également le principal employeur du gouvernement du Canada. La LGFP établit les exigences concernant un certain nombre de représentants clés et permet au Conseil du Trésor, par l'intermédiaire du Secrétariat du Conseil du Trésor du Canada (SCT), d'émettre des politiques, des directives, des normes et des lignes directrices sur la gestion et l'administration de la majorité des organisations fédérales. Le Conseil du Trésor

est également responsable de surveiller les pratiques de gestion ministérielles et des résultats de programme, y compris dans les domaines de la politique de sécurité. Même si, historiquement, le Conseil du Trésor a joué un rôle nominatif en ce qui concerne les questions de sécurité nationale, ses fonctions concernant la gestion et l'administration du gouvernement en font un acteur central dans le cadre de cyberdéfense.

97. La LGFP définit des rôles et des responsabilités généraux; notamment pour le président du Conseil du Trésor, le secrétaire du Secrétariat du Conseil du Trésor du Canada (l'administrateur général du ministère) et le dirigeant principal de l'information du Canada (DPI du Canada). Leurs rôles et responsabilités clés comprennent les suivants :

- **Président du Conseil du Trésor** : il est le président du Conseil du Trésor et détermine le programme du gouvernement en ce qui concerne les personnes, l'argent et les technologies. Le président est également responsable du SCT en tant que ministère et détermine l'orientation stratégique de l'organisation.
- **Secrétaire du SCT du Canada** : il est l'administrateur général du Secrétariat et est nommé par le gouverneur en conseil. Le Conseil du Trésor peut déléguer tout pouvoir ou fonction au secrétaire qu'il a le droit d'exercer en vertu d'une loi fédérale ou d'un décret du gouverneur en conseil. Le secrétaire fournit des conseils sur l'interprétation des politiques, des directives ou des normes prescrites par le Conseil du Trésor.
- **DPI du Canada** : il détient des responsabilités pangouvernementales particulières en matière de leadership aux fins de l'orientation, de la surveillance et du renforcement des capacités en ce qui a trait à la gestion de l'information, aux technologies de l'information, à la sécurité du gouvernement et à la prestation de services gouvernementaux, ce qui inclut la surveillance des pratiques de gestion ministérielles et l'établissement de rapports sur la mise en œuvre des objectifs et de l'orientation stratégique pour l'ensemble de l'entreprise, notamment dans les domaines de la cybersécurité. Le Conseil du Trésor peut également déléguer au DPI du Canada tout pouvoir ou fonction qu'il a le droit d'exercer en vertu d'une loi fédérale ou d'un décret du gouverneur en conseil en ce qui concerne les technologies de l'information[139]. Pour accomplir ce mandat, le Bureau du DPI du Canada compte environ 195 employés et dispose d'un budget d'environ 31 millions de dollars, dont 21 pour cent est alloué précisément aux besoins stratégiques en matière de politique et de cyberespace[140].

98. Pour leur part, les administrateurs généraux des organisations fédérales doivent s'assurer que leurs ministères réalisent les priorités et le mandat du gouvernement tout en veillant à l'intégrité des programmes et des services. En ce qui a trait à la cyberdéfense, cela comprend l'obligation de s'assurer que les systèmes et les réseaux ministériels sont sécurisés.

---

[139] *Loi sur la gestion des finances publiques*, L.R.C. (1985), ch. F-11, https://laws-lois.justice.gc.ca/fra/lois/f-11/ et SCT, examen de la cyberdéfense : séance d'information à l'intention du CPSNR, comparution devant le CPSNR, 27 novembre 2020.

[140] SCT, mot du DPI du Canada, comparution devant le CPSNR, 27 novembre 2020; SCT « NSICOP Review – TBS Comments on Draft Final Report (9-July-2021) », p. 2, 9 juillet 2021; et SCT, *Politique sur les services et le numérique*, 1er avril 2020, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603.

Définition des organisations gouvernementales

99. Le Conseil du Trésor dénombre 169 organisations fédérales et 100 organisations « d'intérêt » fédéral[141]. Il est essentiel de comprendre la façon dont le gouvernement définit sa taille et sa portée afin de pouvoir déterminer et évaluer les organisations assujetties aux politiques du Conseil du Trésor et leurs obligations en matière de sécurisation des systèmes et des réseaux, et ultimement, la mesure dans laquelle elles sont protégées au sein du cadre de cyberdéfense.

100. La LGFP répartit la plupart des organisations fédérales en catégories précises, appelées « annexes », en fonction de leur mandat, de leurs responsabilités et de leur relation avec le gouvernement. Les six annexes de la LGFP sont directement pertinentes, puisque le Conseil du Trésor s'en sert pour déterminer l'applicabilité des politiques, des normes et des lignes directrices en matière de cybersécurité et de cyberdéfense.

- **L'annexe I** comprend les « ministères », qui sont créés par voie législative. Leur mandat couvre de nombreux secteurs de politiques publiques dont sont chargés un ou plusieurs ministres du Cabinet. Ils sont financés par des crédits parlementaires. Entre autres exemples notables, on compte le ministère de la Sécurité publique et de la Protection civile, le ministère des Affaires étrangères, du Commerce et du Développement du Canada et le ministère de la Défense nationale.
- **L'annexe I.1** comprend les « organismes » et les « agents du Parlement ». En général, le mandat de ces organisations est défini plus étroitement, et elles exercent leurs activités avec divers degrés d'autonomie. Entre autres exemples notables, on compte le Centre de la sécurité des télécommunications, le Service canadien du renseignement de sécurité et Services partagés Canada.
- **L'annexe II** comprend les « établissements publics » et les « organismes de services ». Les établissements publics comprennent des organismes qui fournissent des services hautement opérationnels qui n'engagent généralement aucune concurrence dans le secteur privé. Ils ont divers degrés d'autonomie et diverses structures de gestion. Entre autres exemples notables, on compte l'Agence des services frontaliers du Canada, la Commission canadienne de sûreté nucléaire et le Bureau de la sécurité des transports du Canada. Les organismes de service comptent trois organismes spécialisés établis par voie législative et financés par des crédits parlementaires et certains frais d'utilisation : l'Agence du revenu du Canada, l'Agence canadienne d'inspection des aliments et Parcs Canada.
- **L'annexe III** comprend les « sociétés d'État ». Ces organisations mènent leurs activités selon un modèle propre au secteur privé, mais elles ont généralement des objectifs stratégiques qui sont à la fois commerciaux et publics. Les sociétés d'État sont des sociétés qui relèvent directement du gouvernement du Canada. Parmi les exemples

[141] SCT, Infobase du GC, Répertoire des organisations et intérêts fédéraux, 16 juin 2021, https://www.tbs-sct.gc.ca/ems-sgd/edb-bdd/index-fra.html#igoc/instc_form.

notables, on compte la Société canadienne d'hypothèques et de logement, Exportation et développement Canada et VIA Rail Canada. Il y a neuf autres sociétés d'État mère non énumérées dans cette annexe de la LGFP qui ont des modèles de gouvernance distincts créés en vertu de lois[142].

- Les **annexes IV et V** comprennent d'autres « Secteurs de l'administration publique centrale » et des « Organismes distincts ». Il s'agit d'organisations auxquelles la partie I du *Code canadien du travail* ne s'applique pas ou pour lesquelles le ministre, le Conseil du Trésor ou le gouverneur en conseil a le droit d'établir des conditions d'emploi. Entre autres exemples notables, on compte les commissariats à l'information et à la protection de la vie privée (annexe IV) et l'Agence du revenu du Canada (annexe V, mais annexe II également). Même si un certain nombre de ces organismes pourraient être inclus dans les annexes précédentes, les annexes IV et V comprennent d'autres entités fédérales autonomes qui n'ont pas été mentionnées auparavant[143].

En vertu de la LGFP, un ministère est un organisme inclus dans les annexes I, et I.1 (ci-dessus), toute société d'État et diverses autres organisations et effectifs[144]. Le Conseil du Trésor utilise également cette définition pour déterminer l'applicabilité de certains instruments de politique en matière de cyberdéfense. Comme on le mentionnera plus tard, les entités incluses à l'annexe III ne sont pas assujetties aux instruments.

101. Le gouvernement détient une participation dans un certain nombre d'autres organisations en plus de celles qui sont énumérées dans la LGFP. En général, ces « intérêts » incluent des organisations dans lesquelles le gouvernement détient des intérêts ou participe à la gestion et à la surveillance, mais qui ne font pas officiellement partie du gouvernement[145]. Voici des exemples d'intérêts fédéraux : Institut canadien d'information sur la santé, Administration portuaire de Halifax et Autorité aéroportuaire du Grand Toronto. Il importe de souligner que la Chambre des communes et le Sénat ne sont pas considérés comme étant des entités gouvernementales et, par conséquent, ne sont pas assujettis aux politiques de la LGFP ou du Conseil du Trésor. ***.

---

[142] Les neuf organisations sont la Banque du Canada, le Conseil des arts du Canada, l'Office d'investissement du régime de pensions du Canada, la Société Radio-Canada, la Fondation canadienne des relations raciales, le Centre de recherches pour le développement international, la Société du Centre national des Arts, l'Office d'investissement des régimes de pensions du secteur public et Téléfilm Canada.

[143] L'information utilisée pour décrire les six annexes provient du SCT, *Aperçu des organisations et intérêts fédéraux*, 16 août 2016, https://www.canada.ca/fr/secretariat-conseil-tresor/services/etablissement-rapports-depenses/inventaire-organisations-gouvernement/apercu-types-institutions-definitions.html; et la *Loi sur la gestion des finances publiques*, L.R.C. (1985), ch. F-11, https://laws-lois.justice.gc.ca/fra/lois/f-11/.

[144] Cette dernière catégorie comprend les commissions d'enquête créées en vertu de la *Loi sur les enquêtes*; le personnel de la Chambre des communes, du Sénat et de la Bibliothèque du Parlement; le Bureau du conseiller sénatorial en éthique, le Commissariat aux conflits d'intérêts et à l'éthique, le Bureau du directeur parlementaire du budget et le service de protection parlementaire. *Loi sur la gestion des finances publiques*, L.R.C. (1985), ch. F-11, https://laws-lois.justice.gc.ca/fra/lois/f-11/.

[145] SCT, *Aperçu des organisations et intérêts fédéraux*, 16 août 2016, https://www.canada.ca/fr/secretariat-conseil-tresor/services/etablissement-rapports-depenses/inventaire-organisations-gouvernement/apercu-types-institutions-definitions.html.

Politiques fondamentales en matière de cyberdéfense

102. En vertu de la LGFP, le Conseil du Trésor a mis en place deux principaux instruments de politique ainsi qu'un plan stratégique afin de jeter les bases administratives de la position du gouvernement en matière de cybersécurité et de cyberdéfense. Il s'agit de la Politique sur la sécurité du gouvernement et de la Politique sur les services et le numérique ainsi que du Plan stratégique des opérations numériques[146]. Ces instruments de politique et leurs composants secondaires s'appliquent à un éventail d'organisations fédérales. Dans cette structure administrative, les administrateurs généraux et les ministères sont responsables de la sécurisation de leurs systèmes et de leurs réseaux conformément aux politiques. Dans les cas où les ministères ne se conforment pas à ces politiques, les administrateurs généraux peuvent appliquer des mesures administratives, allant de la persuasion (p. ex. poursuivre le dialogue avec le ministère non conforme) à la restriction (p. ex. réorganiser une administration ou mettre fin à un emploi)[147]. Le Comité a observé des cas de non-respect des directives du SCT, mais le SCT n'a donné aucun exemple de mesures administratives imposées pour la non-conformité aux instruments de politiques susmentionnés. Comme le DPI du Canada l'a souligné pendant une comparution devant le Comité, [traduction] « les administrateurs généraux sont ultimement responsables de satisfaire aux attentes décrites dans nos politiques [du Conseil du Trésor]. Il leur incombe notamment d'assurer la protection et la confidentialité de l'information et des biens des ministères[148]. »

Politique sur la sécurité du gouvernement

103. La politique sur la sécurité du gouvernement a deux principaux objectifs. Le premier consiste à « gérer de manière efficace les mesures de sécurité gouvernementales à l'appui de la prestation fiable des programmes et des services du gouvernement ainsi qu'à l'appui de la protection des renseignements, des personnes et des biens ». Le second objectif consiste à « donner à la population canadienne, aux partenaires, aux organismes de surveillance et aux autres intervenants une assurance à l'égard de la gestion de la sécurité au sein du gouvernement du Canada[149] ». La version actuelle de la Politique a été mise en œuvre le 1er juillet 2019 et s'applique à 110 organisations fédérales[150].

104. La Politique prescrit un ensemble d'exigences pour les ministères et les responsables. Elle confie au Conseil du Trésor les responsabilités qui suivent : établir une approche pangouvernementale en matière de gestion de la sécurité et effectuer la surveillance connexe; fournir un leadership, des conseils et une orientation stratégique en matière de sécurité au

---

[146] SCT, « Cyber Defence Review: Briefing for National Security and Intelligence Committee of Parliamentarians », présentation, comparution devant le CPSNR, 27 novembre 2020.
[147] Conseil du Trésor, « Cadre stratégique sur la gestion de la conformité », 2009, http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=17151.
[148] SCT, Mot du DPI du Canada, comparution devant le CPSNR, 27 novembre 2020.
[149] SCT, Politique sur la sécurité du gouvernement, 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578.
[150] La Politique sur la sécurité du gouvernement s'applique aux organismes énumérés aux annexes I, I.1 (colonne I), II, IV et V de la LGFP.

gouvernement; et assurer la surveillance et la coordination stratégique dans la gestion des événements liés à la sécurité qui peuvent entraîner des incidences sur l'ensemble du gouvernement[151]. Pour les organisations fédérales, la Politique oblige les administrateurs généraux à nommer un dirigeant principal de la sécurité chargé de fournir de la direction, de la coordination et de la supervision à l'égard des activités liées à la sécurité ministérielle.

105. En vertu de la Politique, les administrateurs généraux doivent approuver un plan triennal en matière de sécurité qui décrit une stratégie permettant de satisfaire aux exigences ministérielles de sécurité. Le plan doit prévoir huit contrôles de sécurité, à savoir des mesures administratives, opérationnelles, techniques, physiques ou juridiques de gestion des risques en matière de sécurité. Parmi les huit contrôles, quatre portent directement sur la cybersécurité et la cyberdéfense :

- Les exigences, les pratiques et les mesures relatives à la **sécurité des technologies de l'information** sont définies, documentées, mises en œuvre, évaluées, surveillées et tenues à jour à chaque étape du cycle de vie des systèmes d'information, ce qui permet de fournir une assurance raisonnable que les systèmes d'information sont en mesure de protéger adéquatement l'information, sont utilisés d'une façon acceptable, et appuient les programmes, les activités et les services gouvernementaux.
- La **gestion de la continuité des activités** est menée de manière systématique et complète. Elle fournit une assurance raisonnable qu'en cas de perturbation, le ministère pourra garantir un niveau acceptable de prestation des services et des activités critiques, et qu'il sera en mesure de reprendre rapidement les autres services et activités.
- Les exigences, les pratiques et les mesures de **sécurité de la gestion de l'information** sont définies, documentées, élaborées, évaluées, surveillées et tenues à jour à chaque étape du cycle de vie de l'information afin de fournir une assurance raisonnable que l'information est adéquatement protégée d'une manière qui respecte les obligations juridiques et autres et pèse le risque de préjudice et de menaces avec le coût d'appliquer des mesures de protection.
- Les pratiques relatives à la **gestion des événements liés à la sécurité** sont définies, documentées, mises en œuvre et tenues à jour afin d'assurer la surveillance et le signalement des menaces, des vulnérabilités, des incidents et d'autres événements liés à la sécurité, de même que les interventions connexes, et de veiller à ce que de telles activités soient coordonnées de façon efficace au sein du ministère, avec les partenaires et dans l'ensemble du gouvernement, ce qui permet de gérer les incidences possibles, d'appuyer la prise de décisions et de mettre en œuvre de mesures correctives[152].

106. En plus de ces exigences générales, la Politique sur la sécurité du gouvernement façonne le cadre administratif du gouvernement en matière de cyberdéfense grâce à la création

[151] SCT, Politique sur la sécurité du gouvernement, 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578; et SCT, Mandat : Implications pour le SCT et Méthode de collecte, 31 août 2020.
[152] Le contenu des quatre puces provient du SCT, Politique sur la sécurité du gouvernement, 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578.

de directives, de normes et de lignes directrices secondaires détaillées. À titre d'exemple, la Directive sur la gestion de la sécurité découle de la Politique sur la sécurité du gouvernement. Parmi un éventail d'exigences, la Directive définit les rôles et les responsabilités en matière de sécurité du dirigeant principal de la sécurité, des cadres supérieurs, des spécialistes de la sécurité et des employés dans l'ensemble du gouvernement et inclut un certain nombre d'annexes détaillées qui précisent davantage les contrôles en matière de cybersécurité[153]. Une de ces annexes, intitulée Procédures obligatoires relatives aux mesures de sécurité des technologies de l'information, énonce les exigences et les pratiques en matière de technologie de l'information, les pratiques de gestion de projet, le cycle de vie et l'intégrité de la chaîne d'approvisionnement, les évaluations de la sécurité et les autorisations ainsi que la surveillance et les mesures correctives[154]. Bref, la Politique sur la sécurité du gouvernement et ses instruments secondaires aident à jeter les bases de la cybersécurité et de la cyberdéfense au gouvernement.

Politique sur les services et le numérique

107. La Politique sur les services et le numérique est le deuxième principal outil de politique du cadre de cybersécurité et de cyberdéfense du gouvernement[155]. Mise en œuvre le 1er avril 2020, elle constitue « un ensemble intégré de règles qui décrit la façon dont les organisations du gouvernement du Canada gèrent la prestation de services, l'information et les données, la technologie de l'information et la cybersécurité à l'ère du numérique »[156]. De concert avec sa directive secondaire sur les services et le numérique, elle regroupe et remplace un certain nombre de politiques et de directives antérieures[157]. Il importe de souligner que la Politique s'applique à 87 organisations fédérales, à savoir un domaine d'applicabilité plus étroit que celui de la Politique sur la sécurité du gouvernement[158]. Comme la Politique est entrée en vigueur récemment, ces organismes ont une période de mise en œuvre de deux années avant de devoir s'y conformer.

108. La Politique sur les services et le numérique comprend un certain nombre de pouvoirs délégués par le Conseil du Trésor à des fonctionnaires en particulier :

---

[153] SCT, Directive sur la gestion de la sécurité, 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32611.
[154] Pour en savoir davantage, voir la Directive sur la gestion de la sécurité et ses outils de soutien : https://www.tbs-sct.gc.ca/pol/doc-fra.spx?id32611.
[155] La Politique sur les services et le numérique est mise en œuvre en vertu de l'article 7 de la LGFP, comme on l'a mentionné auparavant, et l'article 31 de la *Loi sur l'emploi dans la fonction publique* (LEFP). Le pouvoir de mettre en œuvre la Politique en vertu de la LEFP découle du pouvoir du Conseil du Trésor en qualité d'employeur du gouvernement d'établir les normes en matière de qualification qu'il juge nécessaire pour le travail à accomplir en lien avec la Politique.
[156] SCT, Politique sur les services et le numérique, 2 août 2020, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603.
[157] Les politiques et directives remplacées sont le Cadre stratégique pour l'information et la technologie, la Politique sur la gestion des technologies de l'information, la Politique sur la gestion de l'information, la Politique sur les services, la Politique sur l'utilisation acceptable des dispositifs et des réseaux, la Directive sur la gestion des technologies de l'information, la Directive sur les rôles et responsabilités en matière de gestion de l'information et la Directive sur la tenue des documents.
[158] La Politique sur les services et le numérique s'applique aux organismes énumérés aux annexes I, I.1 (colonne I) et II de la LGFP.

- Le président du Conseil du Trésor a le pouvoir d'émettre, de modifier et d'annuler des directives liées à la Politique.
- Le DPI du Canada a le pouvoir d'émettre, de modifier et d'annuler des normes, des procédures obligatoires et d'autres annexes liées à la Politique, ainsi que d'améliorer le cadre du gouvernement en vue de défendre ses réseaux de toute cyberattaque.

109. La Politique sur les services et le numérique définit davantage les rôles et les responsabilités des principaux cadres supérieurs en ce qui concerne la gouvernance et l'administration de la cybersécurité et de la cyberdéfense. Le secrétaire du Conseil du Trésor est responsable d'établir et de présider le Comité des sous-ministres sur les priorités et la planification opérationnelles, un organe de haut niveau qui fournit des conseils et des recommandations sur un certain nombre de questions relatives à la technologie de l'information, y compris la cybersécurité[158]. Le DPI du Canada doit :

- définir les exigences en matière de cybersécurité pour s'assurer que les renseignements et les données, les applications, les systèmes et les réseaux gouvernementaux et ministériels sont sécurisés, fiables et dignes de confiance;
- gérer les risques en matière de cybersécurité pour le gouvernement et exiger « de l'administrateur en général la mise en œuvre d'une intervention particulière en réponse à des situations de cybersécurité, y compris de vérifier si une atteinte à la vie privée a eu lieu, de mettre en œuvre des mesures de sécurité et de veiller à ce que les systèmes qui causent des risques au gouvernement du Canada soient déconnectés ou retirés, lorsqu'il est justifié de le faire »;
- approuver un plan pangouvernemental annuel pour la gestion intégrée des données, des technologies de l'information et de l'information et de la cybersécurité. La version la plus récente de ce plan, à savoir le Plan stratégique des opérations numériques de 2018 à 2022, est examinée plus en détail ci-après[160].

110. La Politique sur les services et le numérique confie aux administrateurs généraux et aux ministères de nombreuses responsabilités à l'égard des technologies de l'information. Ils doivent préparer un plan stratégique annuel sur les technologies de l'information qui est harmonisé avec le Plan stratégique des opérations numériques du DPI du Canada (voir les paragraphes 119 à 124) et surveiller la conformité de l'organisation à la Politique sur les services et le numérique ainsi qu'à ses instruments de soutien. De plus, les administrateurs généraux ont des responsabilités clairement définies en matière de cybersécurité. Ils doivent établir une gouvernance et des exigences de production de rapports claires, ce qui comprend la nomination d'un agent responsable de mener la fonction ministérielle de gestion de la cybersécurité, à savoir l'agent désigné pour la cybersécurité. La Directive sur les services et le numérique (instrument secondaire) et la Ligne directrice sur les services et le numérique définissent les rôles et les responsabilités de cet agent désigné. Par exemple, l'agent désigné, en collaboration avec le dirigeant principal de l'information ministériel et le dirigeant principal de

[159] SCT, « Deputy Minister Committee on Enterprise Priorities and Planning Terms of Reference », sans date.
[160] SCT, *Politique sur les services et le numérique*, 2 août 2020, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32603.

la sécurité ministérielle fournit une direction, une coordination et une surveillance panministérielles aux fins de l'intégration des exigences en matière de cybersécurité afin de protéger les services de technologie de l'information[161]. L'agent désigné doit également établir les rôles et les responsabilités relatifs au signalement des événements de cybersécurité (à savoir un incident qui pourrait nuire à la sécurité du gouvernement, y compris les menaces, les vulnérabilités et les incidents de sécurité)[162].

111. Dans leur ensemble, la Politique sur les services et le numérique et ses instruments secondaires exigent des cadres supérieurs qu'ils améliorent la prestation de services en misant sur les nouveaux services et les nouvelles technologies tout en prescrivant des fonctions et des responsabilités clés en matière de cybersécurité et de cyberdéfense. Un exemple important est la récente Stratégie d'adoption de l'informatique en nuage et l'orientation connexe sur la cybersécurité et la cyberdéfense incluse dans l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage.

Utilisation et protection de l'informatique en nuage : orientation du DPI du Canada

112. Les services d'informatique en nuage permettent aux personnes et aux organisations d'utiliser des logiciels, du matériel et des services qui peuvent être hébergés à l'extérieur des installations d'une entité et gérés par des organisations du secteur privé[163]. Voici la description du SCT :

> On peut comparer l'informatique en nuage aux services publics utilisés pour livrer des produits, comme l'électricité. Au lieu d'acheter et d'exploiter l'infrastructure en tant que telle, une organisation achète les services informatiques auprès d'un fournisseur. Comme pour l'électricité qui circule dans nos maisons, l'informatique en nuage est offerte sur demande, et le consommateur paie la quantité consommée. Le coût de l'infrastructure utilisée pour fournir le service (stockage et services dans le cas de l'informatique en nuage; poteaux électriques et lignes de transport d'énergie dans le cas de l'électricité) est couvert par les frais facturés au consommateur.[164]

---

[161] SCT, *Ligne directrice sur les services et le numérique*, 3 février 2021, https://canada.ca/fr/gouvernement/systeme/gouvernement-numerique/ligne-directrice-services-numerique.html.
[162] SCT, *Ligne directrice sur les services et le numérique*, 3 février 2021 https://canada.ca/fr/gouvernement/systeme/gouvernement-numerique/ligne-directrice-services-numerique.html; et SCT, « Designated Officials for Cyber Security (DOCS): #SecureGCDigital Forum », présentation, 25 février 2021. La définition du terme « événement » provient du SCT, Politique sur la sécurité du gouvernement, 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16578.
[163] SCT, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.
[164] SCT, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html.

113. Il y a trois types de services d'informatique en nuage : public, privé et hybride. Pour ce qui est du modèle public d'informatique en nuage, une entreprise du secteur privé offre le matériel, le logiciel et tout autre dispositif réseau requis par Internet. Dans ce type d'informatique en nuage, les entités (y compris des organismes gouvernementaux) louent de l'espace comme « locataires » et partagent ces mêmes services et le même espace avec d'autres organisations[165]. Un nuage privé comprend la prestation des mêmes services (matériel, logiciel, dispositifs réseau) sur un réseau privé utilisé exclusivement par une seule organisation[166]. Ces services peuvent également être offerts dans les installations physiques du locataire du nuage. L'approche hybride est une combinaison des modèles public et privé. Parmi les fournisseurs de services notables au Canada, on compte Microsoft, avec ses plateformes Azure et Office365, et Amazon Web Services.

114. Les services d'informatique par nuage offrent plusieurs avantages. L'un des avantages peut être la rationalisation des coûts, puisque les organisations n'effectuent plus la gestion ou l'entretien des biens de technologie de l'information dans l'environnement infonuagique (les exigences en matière d'entretien et de gestion sont désormais la responsabilité du fournisseur de services infonuagiques). Un autre avantage, c'est que le montant payé dépend de l'évolution des besoins informatiques. Le SCT décrit les avantages des services publics d'informatique en nuage pour le gouvernement de la façon suivante :

- Qualité du service améliorée en raison des ressources informatiques adaptables et des niveaux de rendement découlant d'obligations contractuelles;
- Sécurité solide, puisque les fournisseurs de services infonuagiques offrent des accréditations reconnues à l'échelle internationale qu'une organisation unique aurait de la difficulté à obtenir;
- Innovation grâce à la mise en place de nouveaux outils et de nouvelles technologies disponibles par abonnement qui ne nécessitent pas de grand investissement en capital;
- Grande souplesse dans l'élaboration des programmes grâce au vaste éventail de ressources et de capacités offertes dans le nuage[167].

Les environnements infonuagiques ne sont pas sans risque, toutefois. Les données du gouvernement hébergées dans le nuage pourraient quand même être compromises ou volées, et les activités gouvernementales qui emploient des services infonuagiques pourraient quand même être perturbées par les activités d'une cybermenace. Comme c'est le cas dans les environnements informatiques traditionnels, les services infonuagiques nécessitent des

[165] Microsoft, « What are public, private and hybrid clouds? », sans date, https://azure.microsoft.com/fr-ca/overview/what-are-private-public-hybrid-clouds/.
[166] Microsoft, « What are public, private and hybrid clouds? », sans date, https://azure.microsoft.com/fr-ca/overview/what-are-private-public-hybrid-clouds/.
[167] SCT, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html.

contrôles de sécurité adéquats afin d'atténuer les risques d'atteinte à la vie privée, de perte de données et liés à la continuité des activités[168].

115. Depuis 2016, le gouvernement a mis en place une stratégie sur l'adoption infonuagique en vue de maximiser les avantages et d'atténuer les risques. Le SCT souligne que l'adoption de l'informatique en nuage « aidera [le gouvernement] à maintenir l'excellence des services de la TI [technologie de l'information] durant une période de demande croissante pour des services numériques, et à maintenir un accès en temps opportuns à des technologies émergentes[169]. » La stratégie se veut également une directive stratégique qui met l'accent sur un certain nombre d'exigences pour les organisations fédérales :

- une stratégie d'adoption « l'infonuagique d'abord » selon laquelle le nuage est l'option retenue pour offrir des services de technologie de l'information et le nuage public comme solution privilégiée pour le déploiement du nuage;
- une approche de gestion des risques pour la sécurité, qui sont associés à l'adoption de l'infonuagique, qui assure la protection des données et de la vie privée des Canadiens;
- un ensemble de principes pour éclairer les dirigeants principaux de l'information à mesure qu'ils adoptent les services infonuagiques;
- une vision permettant l'utilisation de nuages communautaires; plus précisément, un nuage communautaire pour le secteur public canadien, afin de réunir les acheteurs du secteur public canadien avec les fournisseurs de services infonuagiques publics offerts par l'entremise de courtiers et évalués sur le plan de la sécurité par le gouvernement du Canada[170].

Cette stratégie est harmonisée avec l'orientation du Conseil du Trésor incluse dans la Directive sur les services et le numérique et le Plan stratégique des opérations numériques. Ces documents établissent également les buts d'une prestation de service améliorée grâce à l'utilisation de services infonuagiques, et les ministères doivent les déterminer et les évaluer à titre de principale option de prestation de services[171].

---

[168] CST, « Avantage et risques liés à l'adoption des services fondés sur l'infonuagique pour votre organisation (ITSE.50.060) », 21 avril 2020, https://cyber.gc.ca/fr/orientation/avantages-et-risques-lies-ladoption-des-services-fondes-sur-linfonuagique-par-votre; et SCT, Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.

[169] SCT, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html.

[170] SCT, Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018, 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html.

[171] Voir le paragraphe 4.4.3.9 de la Directive sur les services et le numérique; et « Migration de la charge de travail et adoption de l'informatique en nuage », *Plan stratégique des opérations numériques de 2018 à 2022*.

116. En fonction des exigences selon lesquelles les ministères doivent accorder la priorité aux services infonuagiques, le DPI du Canada a émis l'Orientation sur l'utilisation sécurisée des services commerciaux informatiques en nuage le 1er novembre 2017. Cette orientation permet de veiller à ce que des considérations en matière de sécurité soient intégrées à l'approche d'un ministère grâce à des obligations de politique particulières[172]. Par exemple, les environnements infonuagiques peuvent seulement être utilisés pour stocker des informations correspondant à une catégorie de sécurité donnée ou à une catégorie inférieure[173]. Cette orientation s'applique à 110 organisations fédérales[174].

117. Lors de l'acquisition de services d'informatique en nuage, Services partagés Canada (SPC) joue le rôle de courtier pour le gouvernement. Cela signifie que SPC conclut des marchés avec des fournisseurs de services infonuagiques, accrédite leur utilisation à des fins ministérielles et fournit un modèle de libre-service qui permet aux organisations fédérales de gérer leurs ressources infonuagiques[175]. Néanmoins, les ministères (par l'intermédiaire de leurs administrateurs généraux) demeurent ultimement responsables de la gestion et de la protection de leurs renseignements, y compris dans le nuage, aux termes de la LGFP. Conformément à l'Orientation sur l'utilisation sécurisée des services commerciaux informatiques en nuage, les ministères ont les obligations suivantes :

- appliquer des mesures de protection progressives proportionnelles aux risques déterminés;
- utiliser l'accréditation d'un tiers pour la conception sécurisée de son espace infonuagique;
- effectuer des évaluations de sécurité avant que l'utilisation du service soit autorisée;

---

[172] SCT, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité », 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.

[173] Le gouvernement classe les informations en fonction du type de préjudice qui découlerait de sa divulgation non autorisée. Le niveau de classification le plus élevé pouvant être utilisé sur le nuage est Protégé B, et il s'applique à des informations « dont la divulgation non autorisée pourrait vraisemblablement cause un préjudice grave à des intérêts autres que l'intérêt national, par exemple, la perte de réputation ou d'un avantage concurrentiel ». Pour obtenir des renseignements sur d'autres catégories de sécurité, voir SCT, « Directive sur la gestion de la sécurité – Annexe J : Norme sur la catégorisation de sécurité », 1er juillet 2019, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32614.

[174] L'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage s'applique à tous les ministères inclus dans les annexes I, I.1, II, IV et V de la LGFP.

[175] SCT, « Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : mise à jour de 2018 », 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement-canada.html; et SCT, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité », 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.

- appliquer l'orientation distincte visant l'emplacement des données, qui oblige les ministères à stocker les données de nature délicate au Canada[176];
- gérer les vulnérabilités touchant les systèmes d'information (p. ex. en éliminant les vulnérabilités);
- établir des mécanismes adéquats afin de gérer les incidents en matière de sécurité et d'y répondre[177].

Pour appuyer davantage la mise en œuvre sécuritaire d'un nuage, un cadre d'opérationnalisation infonuagique (les mesures de sécurité infonuagique) a été établi en 2019 afin de fournir une direction et une orientation additionnelles. Ces mesures de sécurité ont réitéré les exigences énoncées dans l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité, notamment que le SCT peut désactiver l'accès au nuage d'un ministère, si ce ministère ne satisfait pas à ces exigences en matière de sécurité dans les 30 jours qui suivent l'établissement d'un environnement infonuagique[178].

118. En bref, la Stratégie d'adoption de l'informatique en nuage et l'orientation connexe sur son utilisation sécurisée visent à établir un équilibre entre les améliorations apportées aux technologies de l'information et les besoins correspondants en matière de cybersécurité et de cyberdéfense.

Plan stratégique des opérations numériques

119. Le troisième instrument de politique fondamental concernant la cyberdéfense est le Plan stratégique des opérations numériques. Établi conformément à la Politique sur les services et le numérique, le Plan stratégique des opérations numériques s'applique à 87 organismes[179]. De plus, conformément à la Politique sur les services et le numérique, le DPI du Canada doit produire un plan annuel prospectif en matière de technologie de l'information pour l'ensemble

---

[176] L'Orientation relative à la résidence des données électroniques : Avis de mise en œuvre de la Politique sur la technologie de l'information a été mise en œuvre le 13 mars 2018 et donne des directives aux ministères et aux organismes en ce qui concerne le contrôle, l'accès et la détention des données électroniques du gouvernement. L'exigence selon laquelle « l'emplacement des données » doit être le Canada vise à assurer un accès continu à ces données, à protéger ses données au moyen des lois canadiennes sur la protection de la vie privée, à protéger les renseignements de nature délicate dans l'intérêt de la sécurité nationale et d'appuyer des interventions plus rapides en cas de compromission des données. SCT, « Orientation relative à la résidence des données électroniques : Avis de mise en œuvre de la politique sur la technologie de l'information », 13 mars 2018, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-relative-residence-donnees-electroniques.html.

[177] SCT, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité », 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.

[178] SCT, DPI du Canada, comparution devant le CPSNR, 27 novembre 2020; et SCT, « NSICOP Review – TBS Comments on Draft Final Report (9-July-2021) », p. 3, 9 juillet 2021. Voir aussi « Government of Canada Cloud Guardrails » qui fait partie du « Cloud Operationalization Framework » au https://github.com/canada-ca/cloud-guardrails.

[179] Comme on l'a mentionné, la Politique sur les services et le numérique s'applique aux organismes inclus dans les annexes I, I.1, et II de la LGFP.

du gouvernement. Ces plans stratégiques établissent l'orientation pour les ministères relativement aux priorités en matière de gestion intégrée des services, de l'information, des données, des technologies de l'information et de la cybersécurité. Entre 2016 et 2019, le DPI du Canada a publié trois plans prospectifs : le Plan stratégique de gestion de l'information et de la technologie 2016-2020 du gouvernement du Canada, le Plan stratégique de gestion de l'information et de la technologie de l'information 2017-2021 et le Plan stratégique des opérations numériques 2018-2022 en vigueur. En raison de la pandémie, le DPI du Canada n'a pas préparé de plan en 2020, mais il a l'intention de publier une version pour la période allant de 2021 à 2024.

120. Le Plan stratégique des opérations numériques 2018-2022 s'appuie sur les deux versions antérieures. Il réitère l'énoncé de vision selon lequel le « gouvernement du Canada est une organisation ouverte et axée sur le service qui exploite et offre des programmes et des services aux particuliers et aux entreprises de manières simples, modernes et efficaces qui sont optimisées pour la voie numérique et disponibles n'importe quand, n'importe où et sur n'importe quel appareil »[180]. Du point de vue de la cyberdéfense et de la cybersécurité, le Plan rend obligatoire l'élaboration d'une approche approfondie à plusieurs niveaux qui utilise des points d'interconnexion fiables (surveillés) offrant une passerelle vers les services infonuagiques. Dans l'ensemble, la Stratégie comprend quatre grandes catégories de mesure ou d'initiatives qui traitent des principales lacunes ou préoccupations en matière de cyberdéfense et de cybersécurité; chacune des catégories a un échéancier différent au sein du calendrier du plan stratégique[181].

121. La première catégorie générale vise à **renforcer la consolidation, la connectivité et la sécurité du réseau**. Pendant qu'il effectue la consolidation de l'accès au réseau à des points de connexion externes dignes de confiance, le gouvernement veille à la protection adéquate de son périmètre de technologies de l'information. Dans le cadre de ces efforts, SPC réduira le nombre de connexions à Internet. De plus, il effectuera le regroupement de 50 réseaux étendus existants des partenaires de SPC dans un réseau organisationnel unique. De même, SPC effectuera la migration de 61 ministères et organismes qui n'utilisent pas le Service Internet d'entreprise de SPC vers le réseau organisationnel géré par SPC (qui utilise les services Internet de SPC exclusivement et bénéficie de la protection des mesures de cyberdéfense *** du CST), pour un total de 104 ministères d'ici 2024[182]. Dans le cadre de la Stratégie d'adoption de l'informatique en nuage, le gouvernement mettra en place des connexions réseau dédiées

---

[180] SCT, « Plan stratégique des opérations numériques de 2018 à 2022 », 29 mars 2019, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/plan-strategique-operations-numerique-2018-2022.html.

[181] Les quatre prochains paragraphes résument les principales initiatives découlant du Plan stratégique des opérations numériques. Pour obtenir des renseignements additionnels, voir SCT, *Plan stratégique des opérations numériques de 2018 à 2022*, 29 mars 2019, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/plan-strategique-operations-numerique-2018-2022.html. Voir également les paragraphes 142 à 147, qui fournissent des précisions sur les projets de cybersécurité de SPC, dont bon nombre appuient les initiatives décrites ici.

[182] Pour en savoir plus long sur le Service Internet d'entreprise de SPC, voir les paragraphes 139 à 141 et 149 à 150. Pour en savoir plus long sur les efforts déployés par SPC afin d'accroître le nombre de ministères qui utilisent le service (projet relatif aux petits ministères et organismes), voir le paragraphe 151.

avec les fournisseurs de services infonuagiques. Cela permettra d'assurer des canaux de communication sécurisés pour les données du gouvernement. De plus, le SCT, le CST et SPC établissent d'autres points d'interconnexion fiable entre le réseau du gouvernement et les partenaires externes. En définitive, ces mesures visent à consolider le périmètre du gouvernement en réduisant le nombre de points de contact externes, n'incluant qu'un nombre limité de connexions dignes de confiance et sûres.

122. La deuxième grande catégorie d'initiative vise à **protéger les dispositifs de points d'extrémité**. Les dispositifs de points d'extrémité comprennent normalement les ordinateurs portables, les ordinateurs de bureau, les téléphones intelligents, les tablettes et les serveurs, ou les biens de technologie de l'information utilisés par les employés du gouvernement. En consultation avec le SCT et le CST, SPC élaborera des procédures normalisées visant à configurer de façon sécurisée les systèmes d'exploitation et les applications des dispositifs de points d'extrémité. Cela comprend deux éléments clés : la mise en place d'un système de prévention des intrusions aux points d'extrémité afin d'automatiser la collecte de renseignements permettant de déceler toute activité malveillante et de prévenir la compromission du dispositif; et l'établissement de contrôles pour accéder aux applications qui permettront aux administrateurs de système de déterminer et d'exécuter les programmes permis. Les initiatives comprises dans cette catégorie appuieront également la mise en œuvre d'outils et de processus qui surveilleront en temps réel l'état et la configuration des dispositifs de points d'extrémité (p. ex. l'état des versions du matériel et du logiciel, la version des systèmes d'exploitation et de l'installation de rustines). Cette capacité permettra de compléter les capteurs de systèmes hôtes du CST (voir les paragraphes 198 à 200), de faciliter la compréhension des dispositifs des points d'extrémité et d'accroître la vitesse et la capacité du gouvernement en ce qui concerne la correction des vulnérabilités des dispositifs de points d'extrémité touchant l'ensemble de l'organisation. On prévoit de terminer cette initiative en 2024[183].

123. La troisième catégorie d'initiatives **améliorera le contrôle des accès et le développement des applications**. Ces améliorations concernent principalement les comptes pour les administrateurs de systèmes de technologie de l'information qui ont un accès privilégié aux systèmes de technologie de l'information ministériels. En 2019, le SCT, SPC et les ministères ont renforcé la gestion et le contrôle des privilèges administratifs afin d'empêcher l'utilisation à mauvais escient d'un compte ayant des privilèges accrus et pour s'assurer que ses comptes sont gérés, contrôlés et surveillés adéquatement. À l'avenir, le SCT améliorera la conception d'applications sécurisées en établissant un cadre de sécurité des applications. Les ministères mettront en œuvre ce cadre lorsqu'ils créeront et mettront en œuvre des services numériques. L'approche du gouvernement vise à assurer que la sécurité est un élément clé de la conception des applications dès le départ. Il s'agit d'une question permanente qui n'a pas d'achèvement.

---

[183] SCT, « Government of Canada: Endpoint Visibility, Awareness and Security (EVAS) – Requirements (version 1.1) », PDF, 25 avril 2019; et SCT, « Plan stratégique des opérations numériques de 2018 à 2022 », 29 mars 2019, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/plan-strategique-operations-numerique-2018-2022.html.

124. La quatrième catégorie générale vise à **accroître la sensibilisation aux cybermenaces et aux risques pour les systèmes et les réseaux du gouvernement**. Comme les autres mesures comprises dans le Plan stratégique des opérations numériques, cet ensemble d'initiatives vise à accroître la sensibilisation aux risques et aux menaces cybernétiques grâce à une gouvernance et à une formation améliorées tout en renforçant la capacité du gouvernement à intervenir en cas d'incident cybernétique. Conformément aux améliorations susmentionnées permettant de voir en temps réel et de façon centralisée les dispositifs de points d'extrémité, le SCT propose de mettre en place une capacité centralisée pour mener des activités de gouvernance et de gestion du risque et de la conformité. Cela permettra de mieux connaître l'environnement général de technologie opérationnelle et facilitera la détermination de la surface d'attaque et des secteurs vulnérables dans l'ensemble du système. À l'heure actuelle, le SCT n'a pas fixé d'échéance pour ce projet. Par ailleurs, le SCT et le CST élaboreront un cadre de divulgation des vulnérabilités du gouvernement qui permettra de cerner et d'atténuer rapidement les vulnérabilités. Sur le plan de la formation, le Centre canadien pour la cybersécurité (CCC) fera la promotion d'une approche pangouvernementale qui améliorera la cybersécurité de tous les employés. Ces efforts aideront à veiller à ce que tous les utilisateurs du système contribuent à la sécurité et à l'intégrité du système. Enfin, le SCT mettra à jour le Plan de gestion des événements de cybersécurité du gouvernement du Canada (voir les paragraphes 224 à 236), où l'on décrit « les intervenants et les mesures nécessaires pour veiller à ce que les événements de cybersécurité soient traités de façon uniforme, coordonnée et rapide »[184].

Résumé

125. Le Conseil du Trésor et le SCT jouent un rôle crucial pour assurer l'administration et la gestion adéquates du gouvernement. En ce qui concerne la cybersécurité et la cyberdéfense, le Conseil du Trésor prescrit des politiques et des directives que suivent la plupart (mais pas toutes) des organisations gouvernementales pour veiller à l'intégrité et à la sécurité de leurs biens de technologie de l'information et de ceux du gouvernement, à plus grande échelle. Quant aux différents ministères, ils sont ultimement responsables de l'assurance de la cybersécurité au sein de leur organisation et de la protection de l'information et des biens numériques. Selon ce modèle de responsabilité partagée, SPC et le CST jouent également des rôles cruciaux en offrant du soutien aux ministères pour qu'ils puissent respecter leurs obligations. Le Comité discute de ces organisations dans la section à venir.

[184] SCT, « Plan de gestion des événements de cybersécurité du gouvernement du Canada », 28 juillet 2020, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html.

Services partagés Canada

126. Services partagés Canada (SPC) est le deuxième membre du groupe tripartite sur la sécurité des technologies de l'information. SPC veille à ce que l'infrastructure de la technologie de l'information du gouvernement du Canada protège les biens technologiques du gouvernement et les données en sa possession[185]. La prochaine section traite de l'évolution du mandat de SPC, des services et des projets clés du SPC visant à renforcer la posture de cybersécurité générale du gouvernement et ceux se rapportant plus particulièrement à la cyberdéfense, ainsi que des partenaires et clients de SPC.

Mandat de SPC

127. Avant 2011, les ministères étaient considérés comme isolés en ce qui a trait à leurs propres exigences en matière de technologie de l'information. Par conséquent, l'uniformisation entre eux était presque absente : les ministères étaient chacun responsables de l'acquisition et de la gestion de leur infrastructure de technologie de l'information, des ordinateurs et appareils, et de la protection de leurs biens électroniques[186]. SPC a été créé en 2011 afin de changer fondamentalement cette approche. Le préambule de la *Loi sur Services partagés Canada* (Loi sur SPC) énonce comme objectif « uniformiser et regrouper, au sein d'une même entité de services partagés, certains services administratifs à l'appui des institutions fédérales; qu'il sera ainsi possible de fournir ces services plus efficacement et d'utiliser les fonds publics de façon optimale[187] ». En pratique, il s'agit de regrouper la prestation des services de courriel, de centre de données et de réseau vers un groupe central de ministères partenaires et de coordonner l'achat et la fourniture d'équipement de technologie de l'information pour le gouvernement[188]. Même si on estimait au départ que cette consolidation allait être une mesure permettant de couper dans les dépenses, l'étendue des changements requis a nécessité des investissements considérables dans les années qui ont suivi[189].

128. Les pouvoirs sur lesquels se fonde SPC ont évolué. SPC a été créé par décret en 2011. Le ministère a ensuite été fondé dans la loi le 29 juin 2012, lorsque la Loi sur SPC a reçu la sanction royale. La Loi sur SPC permet à un ministre d'être désigné comme responsable de SPC — à l'heure actuelle, le ministre responsable est le ministre d'État (gouvernement numérique)[190] — et donne au ministre le pouvoir de coordonner les services de

---

[185] SPC, « Cybersécurité et sécurité de la technologie de l'information », sans date, https://www.canada.ca/fr/services-partages/organisation/cybersecurite-securite-technologie-information.html.
[186] SPC, « Norme sur le renforcement de la sécurité de l'accès à distance », sans date, https://service.ssc-spc.gc.ca/fr/politiques_processus/politiques/distance.
[187] *Loi sur Services partagés Canada*, L.C. 2012, ch. 19, art. 171, Préambule, 29 juin 2012, https://laws-lois.justice.gc.ca/fra/lois/s-8.9/page-1.html.
[188] Comme les claviers, les logiciels et matériel informatique, et les écrans. Bureau du vérificateur général. « Automne 2015 – Rapports du vérificateur général du Canada : Rapport 4—Services partagés en technologies de l'information », 2015, https://www.oag-bvg.gc.ca/internet/Francais/parl_oag_201602_04_f_41061.html.
[189] En date de 2020, les investissements dans SPC uniquement totalisaient plus de 4 milliards de dollars.
[190] Le décret 2019-1366 a désigné le ministre d'État (Gouvernement numérique) comme ministre de SPC. Voir https://decrets.canada.ca/attachment.php?attach=36701&lang=fr. De 2012 à 2019, le ministre de Travaux publics et Services gouvernementaux était le ministre responsable.

télécommunications pour les ministères et organismes. SPC doit :

- déterminer et fournir des solutions et les services habituels de la technologie de l'information dans l'ensemble des organisations gouvernementales;
- planifier et élaborer des services consolidés, standardisés et axés vers l'avenir pour répondre aux besoins des ministères partenaires et clients;
- gérer et maintenir l'infrastructure de technologie de l'information actuelle, y compris tous les services permanents et le soutien de maintenance nécessaires;
- fournir les biens et les services assurant la prestation des services de technologie de l'information habituels aux ministères partenaires et clients;
- appuyer la gestion de l'information et la sécurité des technologies de l'information à l'échelle du gouvernement en partenariat avec le Centre de la sécurité des télécommunications (CST), y compris le Centre canadien pour la cybersécurité (CCC), et d'autres partenaires de la sécurité du gouvernement[191].

129. Au total, le gouvernement a fait passer 21 décrets pour modifier le mandat de SPC, nommer les présidents de l'organisation et augmenter le nombre d'organisations auxquelles SPC doit fournir des services ou pour lesquelles SPC doit intervenir pour fournir de l'équipement et des services[192]. Des 21 décrets, quatre sont particulièrement pertinents pour l'examen.

- En 2011, le gouvernement a promulgué deux décrets qui ont transféré six unités liées à la technologie de l'information de l'ancien Travaux publics et Services gouvernementaux Canada[193], ainsi que les unités de services de courriel, de centre de données et de réseau de 42 ministères à SPC, créant ainsi les 43 « partenaires » principaux de SPC[194].
- En 2012, le gouvernement a fait passer un décret qui a circonscrit le mandat de SPC en stipulant qu'il ne fournirait pas de services de courriel, de centre de données ou de réseau à un ministère autorisé à traiter des renseignements Très secret ou lorsque quatre organisations précises se servaient de systèmes particuliers pour opérer des

---

[191] SPC, « Shared Services Canada's Mandate, Authorities and Partners », présentation, exposé devant le Secrétariat du CPSNR, novembre 2020.
[192] SPC, « Shared Services Canada's Mandate, Authorities and Partners », présentation, exposé devant le Secrétariat du CPSNR, novembre 2020.
[193] « Décret 2011-0877 », 3 août 2011, https://decrets.canada.ca/attachment.php?attach=24554&lang=fr.
[194] SPC est l'un des 43 partenaires. Décret 2011-1297, 15 novembre 2011, https://decrets.canada.ca/attachment.php?attach=24978&lang=fr. Ce décret a fait en sorte que SPC devenait responsable de l'infrastructure de technologie de l'information de 42 organisations partenaires (budgets des serveurs, des centres de données, des ressources humaines et de la technologie de l'information), y compris 485 centres de données, 50 réseaux différents et environ 23 400 serveurs. Il s'agissait d'environ 95 pour cent des dépenses liées à l'infrastructure de la technologie de l'information du gouvernement, et les cinq pour cent restants étaient composés des autres plus petits ministères et organismes. SPC, « Décret – Approvisionnement », https://www.canada.ca/fr/services-partages/organisation/transparence/sommaire-documents/cahier-breffage-ministeriel/decret-approvisionnement.html.

navires, des aéronefs ou des véhicules ou pour soutenir des opérations dans les domaines de la défense nationale, de la sécurité nationale ou de la sécurité publique[195].

- En 2015, le gouvernement a fait passer un décret pour élargir le mandat de SPC au-delà des 43 partenaires principaux du départ afin d'inclure 40 « clients obligatoires » qui recevraient un sous-ensemble de services liés aux services de courriel, de centres de données et de réseau sur un principe de recouvrement des coûts. Le décret a aussi augmenté le nombre d'organisations gouvernementales qui devaient se procurer les appareils pour utilisateurs (comme les ordinateurs de bureau et les imprimantes) auprès de SPC, et a créé une catégorie de « clients facultatifs » qui peuvent obtenir des services de SPC sur un principe de recouvrement des coûts (la définition comprenait les sociétés d'État et d'autres paliers de gouvernement)[196].

130. En somme, la promulgation périodique de décrets a établi le mandat et la composition des clients du SPC et a précisé sa prestation de services relativement aux courriels, aux centres de données et aux réseaux, et la fourniture de dispositifs de technologie en milieu de travail pour les utilisateurs. À l'heure actuelle, SPC fournit ses services en partie ou intégralement à 160 des 169 organisations fédérales (le Comité explore plus loin la question des ministères en question). Voir le Tableau 1 pour obtenir un aperçu de la division des responsabilités entre SPC et chaque ministère.

<table>
<tr><th colspan="4">Services de technologie de l'information du gouvernement du Canada</th></tr>
<tr><td>Responsabilité</td><td>Courriels, centres de données et réseaux</td><td>Appareils finaux</td><td>Applications</td></tr>
<tr><td>Gestion et prestation de service</td><td rowspan="2">Services partagés Canada (obligatoire ou facultatif pour certains ministères comme précisé dans les décrets)</td><td colspan="2">Ministères</td></tr>
<tr><td>Approvisionnement</td><td>Services partagés Canada</td><td>Services publics et Approvisionnement Canada</td></tr>
<tr><td>Établissement de politiques et de normes</td><td colspan="3">Secrétariat du Conseil du Trésor du Canada</td></tr>
</table>

Tableau 1 : Distribution des responsabilités et secteurs de service pour les services de technologie de l'information du gouvernement du Canada[197]

[195] Les quatre organisations sont l'Agence des services frontaliers du Canada, le ministère des Pêches et Océans, le ministère de la Défense nationale et la Gendarmerie royale du Canada. « Décret 2012-0958 », 29 juin 2012, https://decrets.canada.ca/attachment.php?attach=26384&lang=fr.

[196] « Décret 2015-1071 », 16 juillet 2015, https://decrets.canada.ca/attachment.php?attach=31447&lang=fr.

[197] Adapté de : SPC, « Historique et responsabilités législatives de Services partagés Canada », 3 février 2016, https://www.canada.ca/fr/services-partages/organisation/transparence/sommaire-documents/cahier-breffage-ministeriel/historique-responsabilites-legislatives-services-partages-canada.html; et SPC, « Shared Services Canada's Mandate, Authorities and Partners », présentation pour le Secrétariat du CPSNR, novembre 2020.

Services et projets de SPC

131. SPC joue un rôle fondamental dans la protection des biens et de l'information numériques du gouvernement. Sa prestation de services de courriels, de réseau et de centre de données signifie qu'il fournit l'infrastructure qui héberge et transporte l'information importante appartenant aux Canadiens et au gouvernement. L'infrastructure soutient la prestation des programmes gouvernementaux, et les Canadiens comptent sur un service constant et fiable de ces programmes et en dépendent. La menace incessante de cyberattaque contre cette infrastructure signifie que la cybersécurité comporte un risque considérable. En effet, si les contrôles de sécurité techniques ou opérationnels sont inadéquats, ou si les vulnérabilités en matière de sécurité ne sont pas traitées, les systèmes du gouvernement restent vulnérables aux cyberactivités malveillantes[198]. Comme l'indique SPC, la sécurité de l'infrastructure de la technologie de l'information du gouvernement est donc « cruciale[199] ».

132. Le Comité considère que l'exercice des responsabilités de SPC est réparti en deux grandes catégories. La première est la protection continue des biens et des communications numériques du gouvernement grâce à la gestion appropriée des technologies de l'information (services de SPC). La deuxième est la mise en œuvre d'un plan d'infrastructure en matière de technologie de l'information qui s'applique à l'ensemble du gouvernement et qui vise à mieux protéger les systèmes gouvernementaux contre les menaces à la sécurité (projets de SPC)[200]. Le Comité aborde chaque point l'un après l'autre.

Cyberdéfense et services de SPC

133. La taille, la fonction et le mandat des réseaux et des données que SPC doit protéger varient grandement. Ces différences traduisent bien la variabilité dans la prestation de programmes et de services gouvernementaux. Certaines organisations possèdent peu de renseignements sensibles sur leurs réseaux et font donc face à relativement peu de menaces à la sécurité, tandis que d'autres conservent beaucoup de renseignements sensibles et sont confrontées à des menaces considérablement plus grandes[201]. Pour répondre à ces menaces et ainsi repérer les acteurs malveillants et les empêcher d'accéder aux réseaux gouvernementaux, SPC utilise une série de mesures de cybersécurité, y compris des services de coupe-feu, d'antivirus et d'antimaliciel, ainsi que des outils d'identification et d'authentification[202]. SPC est responsable de l'infrastructure du réseau Secret du gouvernement et collabore avec le CCC pour gérer le périmètre du réseau du gouvernement en exerçant une surveillance de sécurité spécialisée des points d'accès Internet (voir la section « Le Centre de la

---

[198] Outre la cybersécurité et la sécurité de l'information, le Plan de sécurité ministériel a cerné deux autres risques importants pour la sécurité : la sécurité de l'effectif, du lieu de travail, des installations et des biens de SPC, et la gouvernance des activités de SPC liées à la sécurité. SPC, « Departmental Security Plan 2019-2022 », 15 mai 2019. Des risques similaires étaient aussi relevés dans le plan de sécurité ministériel de SPC pour 2013-2016.
[199] SPC, « Departmental Security Plan 2019-2022 », 15 mai 2019; et SPC, « Shared Services Canada Network and Security Strategy (version 1.6) », 1er septembre 2020.
[200] SPC, « Mandat », https://www.canada.ca/fr/services-partages/organisation/mandat1.html.
[201] SPC, « Departmental Security Plan 2013-2016 », 17 juin 2013.
[202] SPC, « Cybersécurité et sécurité de la technologie de l'information », sans date, https://www.canada.ca/fr/services-partages/organisation/cybersecurite-securite-technologie-information.html.

sécurité des télécommunications ») qui ont amélioré la capacité du gouvernement de repérer et de prévenir les cyberactivités malveillantes[203]. Au total, SPC offre à ses partenaires et clients 34 différents services qui sont regroupés dans cinq catégories comportant au moins un service qui se rapporte au rôle de SPC dans la défense des réseaux gouvernementaux contre les cyberattaques. Les prochains paragraphes décrivent brièvement chacun des services et leur applicabilité à la cyberdéfense.

Services numériques

134. Les services numériques sont la plus grande catégorie de services qu'offre SPC. Des 12 services de ce domaine, quatre jouent un rôle dans la cyberdéfense. Les deux premiers sont la fourniture de comptes de courriels pour les employés du gouvernement et leur accès à distance au moyen de connexions sécurisées au réseau. Ces deux services sont assujettis aux contrôles de gestion de l'identité et des justificatifs d'identité, et surveillés en vue de la détection de virus et de pourriels. Le troisième service est la fourniture d'appareils mobiles (téléphones cellulaires) pour la connectivité téléphonique, courriel et Internet[204]. Le quatrième service est un système de validation de l'identité en vue d'assurer un contrôle et une gestion synchronisés et à l'échelle du système des justificatifs d'identité de l'utilisateur pour fournir un accès aux systèmes gouvernementaux et à l'information se trouvant sur les nuages et sur les réseaux habituels « sur place »[205].

Services de sécurité

135. Les services de sécurité de SPC authentifient les personnes afin qu'elles accèdent aux services et aux comptes gouvernementaux, sur les réseaux gouvernementaux internes et externes. Trois éléments de ce secteur de service se rapportent à la défense des réseaux gouvernementaux :

- **Gestion interne des justificatifs d'identité :** SPC gère l'infrastructure à clé publique qui facilite l'authentification de l'accès sécurisé aux applications et aux réseaux gouvernementaux[206]. Le service permet aux utilisateurs de s'envoyer des courriels chiffrés jusqu'à un certain niveau de classification et d'accéder de façon sécuritaire aux

---

[203] SCT, « Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2019 », https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html#toc6; Sécurité publique Canada, « Évaluation horizontale de la Stratégie de cybersécurité du Canada », 29 septembre 2017, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/vltn-cnd-scrt-strtg/index-fr.aspx#s331.

[204] SPC, « Au service du gouvernement : Courriel – pour les administrateurs », http://service.ssc-spc.gc.ca/fr/services/communication/courriel/admin; et SPC, « Au service du gouvernement : Appareils mobiles - pour les employés du GC », https://service.ssc-spc.gc.ca/fr/services/communication/appareils-mobiles-lignefixe/mobile-utils.

[205] SPC, « Au service du gouvernement : catalogue de services », https://service.ssc-spc.gc.ca/fr/services; et SPC, « Directory Credential and Access Management » analyse de rentabilisation (version 3.0), 8 septembre 2020.

[206] Une infrastructure à clé publique protège la confidentialité de l'information et authentifie électroniquement l'identité des personnes qui accèdent à l'information protégée. SCT, *Ligne directrice sur la gestion de l'infrastructure à clé publique au gouvernement du Canada*, https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=20008#appB.

applications qui traitent des renseignements personnels sensibles (comme l'information sur la paie)[207].

- **Gestion de l'accès sécurisé à distance :** Ce service utilise l'infrastructure à clé publique (ci-dessus) pour que les utilisateurs transmettent et reçoivent de l'information de façon sécurisée à partir de postes de travail à distance tout en maintenant la disponibilité, la confidentialité et l'intégrité des données[208].
- **Gestion externe des justificatifs d'identité :** SPC gère une infrastructure à clé publique qui fournit un service de cyberauthentification standardisé aux Canadiens, aux entreprises et à d'autres personnes afin de permettre des opérations en ligne sécurisées avec différents programmes et services gouvernementaux[209]. Ce service est obligatoire pour les ministères et organismes[210].

Services de matériel et de logiciel

136. SPC offre aux ministères des choix d'approvisionnement pour les appareils comme les ordinateurs et l'équipement d'impression, ainsi qu'un éventail de logiciels, y compris pour la connectivité, les appareils individuels et les besoins en matière de sécurité. Les services qui se rapportent à la cyberdéfense comprennent les suivants.

- **Approvisionnement et fourniture de matériel :** SPC fournit des appareils de technologie en milieu de travail (matériel) pour ses partenaires et clients, y compris des ordinateurs de bureau, des ordinateurs portatifs et des tablettes[211].
- **Approvisionnement et fourniture de logiciel :** SPC fournit des logiciels à ses partenaires et clients pour des appareils (comme des systèmes d'exploitation), des services (comme la configuration d'un logiciel de bureau), la connectivité (comme des services d'impression), la productivité (comme des navigateurs Web) et la sécurité (comme l'authentification des utilisateurs)[212].

137. Tous les services d'approvisionnement en matériel et logiciels sont assujettis à la *Norme d'intégrité de la chaîne d'approvisionnement* de SPC. Cette norme vise à définir et à évaluer tout processus d'approvisionnement qui « pourrait être compromi[s] ou utilis[é] pour compromettre la sécurité de l'équipement, des logiciels, des services ou de l'information du Canada » et à veiller à ce que le matériel et les logiciels demandés fassent l'objet d'une évaluation de sécurité (notamment par une communication avec le CST), que les contrats

---

[207] SPC, « Au service du gouvernement : maCLÉ – pour les utilisateurs », https://service.ssc-spc.gc.ca/fr/services/acces/macle/utils.
[208] SPC, « Au service du gouvernement : Accès à distance protégé – pour les administrateurs », https://service.ssc-spc.gc.ca/fr/services/acces/acces-distance-protege/admin.
[209] SPC, « Au service du gouvernement : catalogue de services », https://service.ssc-spc.gc.ca/fr/services; et SPC, « Au service du gouvernement : Matrice des responsabilités en matière de cybersécurité et de sécurité de la TI. Section 6 Gestion des identités et des accès », http://service.ssc-spc.gc.ca/fr/securiteit/RACI#.
[210] SPC, « Au service du gouvernement : Catalogue de services », https://service.ssc-spc.gc.ca/fr/services.
[211] SPC, « Au service du gouvernement : Micro-ordinateurs », https://service.ssc-spc.gc.ca/fr/services/mat-log/micro-ordinateurs/approv; et SPC, « Norme d'intégrité de la chaîne d'approvisionnement », novembre 2015.
[212] SPC, « Au service du gouvernement : Approvisionnement en logiciels », https://service.ssc-spc.gc.ca/fr/services/mat-log/approv-logiciels.

soient vérifiés et que les éléments définis comme représentant un risque élevé puissent être évités, rappelés ou retirés des systèmes du gouvernement[213].

Services de centre de données

138. SPC offre neuf services de centre de données. Bien qu'il s'agisse principalement de services d'infrastructure et d'hébergement de bases de données, ce service comprend deux éléments importants pour la cyberdéfense.

- **Service de courtage infonuagique :** Conformément à l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage de 2017 du Conseil du Trésor, SPC fournit un service de courtage aux ministères en vue de cerner les fournisseurs de services d'infonuagique appropriés avec lesquels SPC a conclu des contrats. SPC fournit ce service à ses 43 partenaires, à ses 23 clients obligatoires et à ses 15 clients facultatifs[214].
- **Infrastructure secrète du gouvernement du Canada :** SPC gère et entretient cette infrastructure afin de permettre la création, le traitement, l'entreposage et la communication d'information classifiée au niveau Secret. Ce service utilise le réseau étendu du gouvernement pour transmettre des données chiffrées entre les utilisateurs et les ministères. Les risques de la protection de l'information plus sensible de niveau Secret sont partagés entre SPC et le ministère ou l'organisme client; SPC est responsable du maintien de l'intégrité, de l'assurance et de l'efficacité des contrôles de sécurité pour les utilisateurs approuvés, et les ministères sont responsables de gérer l'accès des utilisateurs à leurs applications et données[215].

Services de réseau

139. Les services de réseau de SPC comprennent la fourniture de Wi-Fi, de services Internet et de connectivité satellite. Les services de réseau comportent huit éléments, dont les deux suivants sont essentiels au cadre de cyberdéfense du gouvernement.

- **Réseau étendu du gouvernement du Canada (RE du GC) :** Le RE du GC est un service de réseau entièrement administré qui relie les locaux des partenaires ou des

---

[213] SPC, « Norme d'intégrité de la chaîne d'approvisionnement », novembre 2015.
[214] SPC, « Au service du gouvernement : Service de courtage infonuagique », https://service.ssc-spc.gc.ca/fr/services/cd/infonuagique; SCT, « Stratégie d'adoption de l'informatique en nuage du gouvernement du Canada : Mise à jour de 2018 », https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/strategie-adoption-information-nuage-gouvernement.html; et SCT, « Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage : Avis de mise en œuvre de la Politique sur la sécurité (AMOPS) », https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/services-informatique-nuage/orientation-utilisation-securisee-services-commerciaux-informatique-nuage-amops.html.
[215] SPC, « Au service du gouvernement : Réseau et hébergement de l'Infrastructure secrète du gouvernement du Canada – pour les administrateurs », http://service.ssc-spc.gc.ca/fr/services/infrastructure/classifiee/gcsi. Par le passé, le gouvernement maintenait 34 réseaux Secret autonomes et gérés indépendamment au sein de 18 ministères. Le projet d'élargissement de l'Infrastructure secrète du gouvernement du Canada comprend des efforts visant à faire passer ces réseaux à l'architecture d'entreprise de SPC vers un système lié aux communications et aux données secrètes. Voir aussi, SPC, *Secret Infrastructure, 34 Legacy Networks*, sans date.

clients à l'échelle métropolitaine, régionale, nationale et internationale. Il connecte les utilisateurs et les ordinateurs entre eux et à Internet, et il soutient les communications vocales et vidéo et la communication de données en simultané, ainsi que la transmission d'information classifiée au moyen de méthodes de chiffrement appropriées. Les services du RE du GC sont jumelés à une surveillance de sécurité et à des protocoles de sécurité renforcés (comme des services de connexion et de détection des intrusions)[216].

* **Service Internet d'entreprise :** Le Service Internet d'entreprise de SPC fournit une connectivité sécurisée aux utilisateurs du gouvernement pour accéder à Internet et au public pour accéder aux sites Web du gouvernement. SPC fournit le Service Internet d'entreprise à toutes les organisations partenaires et selon un principe de rémunération des services pour ses clients. Le service demande une connexion au RE du GC et donne la protection la plus élevée, en raison de protocoles de sécurité renforcés et de la surveillance de sécurité intégrée fournis par l'intégration des mesures de cyberdéfense *** du CST aux passerelles du Service Internet d'entreprise. Le Comité se penche sur l'avantage de cette intégration dans la discussion sur le CST ci-dessous[217].

Dans l'ensemble, la création du Service Internet d'entreprise de SPC et son adoption progressive par les ministères ont joué un rôle de base dans le renforcement du cadre de cyberdéfense du gouvernement. Son évolution est décrite ci-dessous.

Connectivité Internet sécurisée : L'évolution vers le Service Internet d'entreprise

140. Les origines du Service Internet d'entreprise de SPC datent de 2002, lorsque le gouvernement a lancé le Réseau de la Voie de communication protégée pour que les organisations fédérales puissent offrir de façon sécurisée leurs services les plus utilisés en ligne[218]. Le Réseau de la Voie de communication protégée visait à réduire les coûts opérationnels et liés à la maintenance au moyen d'une infrastructure de réseau commune pour le gouvernement qui comprenait un accès à Internet surveillé, protégé et redondant[219]. En 2006, le Conseil du Trésor a instauré une directive rendant obligatoire l'utilisation du Réseau de la Voie de communication protégée et, en 2008, 75 ministères y avaient migré. En 2010 et en 2011, la Chine a mené des attaques à grande échelle contre de nombreux ministères, entraînant la perte d'une quantité considérable de données sensibles (voir l'étude de cas 1). En réponse, le dirigeant principal de l'information du Canada a publié à nouveau des directives demandant aux ministères de migrer au Réseau de la Voie de communication protégée pour :

> [traduction] réduire les risques auxquels nous faisons tous face en raison du nombre de cyberattaques externes qui ne cessent d'augmenter. L'approche

---

[216] SPC, « Au service du gouvernement : RE du RGC – pour les administrateurs », http://service.ssc-spc.gc.ca/fr/services/infrastructure/infra-reseau/re-rgc-admin.
[217] SPC, « Au service du gouvernement : Catalogue de services », https://service.ssc-spc.gc.ca/fr/services. Aussi SPC, « Au service du gouvernement : RE du RGC – pour les administrateurs », http://service.ssc-spc.gc.ca/fr/services/infrastructure/infra-reseau/re-rgc-admin.
[218] SPC, Discussion sur le mandat avec le Secrétariat du CPSNR – 24 février et suivis, 9 mars 2021.
[219] SPC, Discussion sur le mandat avec le Secrétariat du CPSNR – 24 février et suivis, 9 mars 2021.

> clé pour atténuer ces risques est de réduire le nombre de connexions Internet indépendantes des ministères et de les remplacer par un accès commun solide, hautement performant et très sécurisé pour [le gouvernement]. En diminuant le nombre de points d'accès Internet — et en protégeant ces points — on réduit le risque de sécurité global [de technologie de l'information] pour le gouvernement, ce qui facilite la prévention et la lutte contre les attaques visant à perturber nos opérations ou à voler de l'information sensible ou des renseignements personnels[220].

En 2012, le nombre de ministères utilisant le Réseau de la Voie de communication protégée était passé de 75 à 87[221].

141. En 2015, le Réseau de la Voie de communication protégée est devenu le Service Internet d'entreprise et le nombre de ministères qui l'utilisent est passé à 90. Tous les partenaires principaux de SPC sont passés au Service Internet d'entreprise (à l'exception du ministère de la Défense nationale, qui migrera en 2021-2022), comme de nombreux clients obligatoires et des clients facultatifs de SPC[222]. Cependant, l'adoption du Service Internet d'entreprise à l'échelle du gouvernement demeure un défi. En 2018, le Conseil du Trésor a réitéré sa directive aux ministères de migrer au Service Internet d'entreprise :

> Pour gérer les risques pour son réseau, le gouvernement normalise la protection et crée un périmètre pangouvernemental sécurisé qui protégera les données du gouvernement sur place et dans le nuage. Le SCT, le CST et SPC établiront des points d'interconnexion fiables entre le réseau [de base] du gouvernement et les partenaires externes afin : d'offrir une connectivité uniformisée et sécurisée avec des partenaires externes et à Internet; de faire office de porte d'entrée aux services d'informatique en nuage; [et de protéger les charges de travail en nuage contre les attaques directes provenant d'Internet]. Les ministères qui n'utilisent pas actuellement les services Internet de SPC effectueront une migration vers le réseau opérationnel géré par SPC, et recourront exclusivement aux services de ce dernier.[223]

Il est logique d'exiger cette migration. Comme il est indiqué plus en détail à la section sur le CST (paragraphes 1544 à 213), le CST et SPC gèrent un système très efficace de capteurs et d'outils de défense (classifiés et disponibles sur le marché) qui protègent les organisations gouvernementales au sein du Service Internet d'entreprise contre les menaces habituelles et, le plus important, contre les auteurs de cybermenaces les plus expérimentés. En date

---

[220] SSC, « SCNet Enterprise Internet – 2010 and 2011 », communiqué du BDPI du SCT, 24 février 2021.
[221] SPC, Discussion sur le mandat avec le Secrétariat du CPSNR – 24 février et suivis, 9 mars 2021.
[222] SPC, Discussion sur le mandat avec le Secrétariat du CPSNR – 24 février et suivis, 9 mars 2021. Le ministère de la Défense nationale *** fait l'objet d'une surveillance distincte par le CCC.
[223] SCT, « Plan stratégique des opérations numériques de 2018 à 2022 », Article 4.2, *Sécuriser le périmètre en évolution du réseau du gouvernement*, https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/plans-strategiques-operations-numeriques-gouvernement-canada/plan-strategique-operations-numerique-2018-2022.html.

d'août 2021, SPC fournit le Service Internet d'entreprise à 94 organisations[224]. Le Comité traite de la directive du Conseil du Trésor et du nombre de ministères qui utilisent le Service Internet d'entreprise de SPC dans son évaluation.

[224] SPC, Discussion sur le mandat avec le Secrétariat du CPSNR – 24 février et suivis, courriel, 9 mars 2021; et SPC, « Re: NSICOP Discussion on Mandate with Committee Secretariat », courriel, 30 avril 2021.

Étude de cas 1 : Un coup de semonce — consolidation des réseaux et des défenses dynamiques

[*** Quatre paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] En février 2010, le CST a déployé ses capteurs réseau passifs sur le Réseau de la Voie de communication protégée du gouvernement, soit la première fois que le CST utilisait cette ressource ailleurs que dans trois ministères : Affaires étrangères et Commerce international (maintenant Affaires mondiales Canada), le ministère de la Défense nationale et le CST lui-même[225]. Le CST a immédiatement découvert une compromission importante et de longue date des réseaux gouvernementaux par un acteur étatique chinois. L'acteur chinois était connu pour s'en prendre à des réseaux gouvernementaux du monde entier pour trouver des renseignements sur les ressources naturelles et l'énergie, la défense, les finances mondiales, la politique étrangère et le commerce. Le CST a déterminé que l'acteur cherchait à obtenir des documents, des notes de breffage et des stratégies sur la posture du Canada relativement à des négociations multilatérales liées à plusieurs organismes internationaux.

Entre août 2010 et août 2011, la Chine a ciblé 31 ministères, dont huit ont subi de graves compromissions. Les pertes d'information étaient considérables, notamment des communications par courriel de hauts dirigeants gouvernementaux; une exfiltration de masse d'information provenant de plusieurs ministères, y compris des notes de breffage, des documents de stratégie et de l'information de niveau Secret; ainsi que des mots de passe et des données de systèmes de classement. Le Secrétariat du Conseil du Trésor du Canada et le ministère des Finances étaient les plus touchés. En effet, ils ont perdu des ensembles complets de mots de passe de réseaux.

Le CST a lancé une réponse à trois volets. D'abord, il a fourni une surveillance passive continue des activités malveillantes au moyen de ses capteurs réseau. Ensuite, il a fourni des conseils et une orientation aux ministères afin d'améliorer la gestion et la sécurité des systèmes. Enfin, il a contribué à l'atténuation stratégique des compromissions, au moyen de ses informations afin de mieux comprendre les intentions et les moyens de l'attaquant. Pour leur part, le Secrétariat du Conseil du Trésor du Canada et le ministère des Finances ont été forcés à déconnecter leurs réseaux d'Internet afin d'atténuer la compromission.

L'incident a été un coup de semonce pour le gouvernement concernant l'étendue de sa cybervulnérabilité et le besoin de défenses proportionnelles. Avant cela, les réseaux gouvernementaux étaient une cible facile et précieuse pour les auteurs de menace étatiques chinois, puisqu'ils étaient essentiellement sans défense et servaient à entreposer de l'information classifiée en l'absence d'un moyen sécurisé. Le déploiement de capteurs réseau du CST dans ce réseau étendu a été un [traduction] « point tournant de l'histoire de la cyberdéfense au gouvernement » — il a confirmé le besoin de points d'accès regroupés à Internet qui peuvent être surveillés contre les menaces et d'un réseau d'entreprise unique à

[225] Ce résumé s'appuie sur les documents suivants: CST, *Analysis of Widespread Chinese Intrusions on Government of Canada Networks* du, avril 2010; CST, « Interdepartmental Assessment: The Chinese Cyber Threat to Government of Canada Networks – August 2010–August 2011 », sans date; CST, « DM Security and Intelligence: Update on January 2011 Cyber Intrusions », note de service pour le chef, CST, février 2011; et CST, « NSICOP Cyber Defence Review – Information Package #17 – Table of Contents », 11 mars 2021.

l'échelle du gouvernement pour bien protéger les systèmes gouvernementaux contre les cyberattaques[226].

Cyberdéfense et projets de SPC

142. La deuxième grande catégorie de responsabilités de SPC est la mise en œuvre d'un plan d'infrastructure de technologie de l'information à l'échelle du gouvernement visant à mieux protéger les systèmes gouvernementaux contre les menaces pour la sécurité, c'est-à-dire les projets de SPC. SPC utilise une approche de type « sécurisé dès la conception » pour intégrer ses activités de cybersécurité à ses tâches principales[227]. Par conséquent, les services et les activités de SPC sont conçus et élaborés de façon à incorporer les normes applicables de génie et de sécurité, et à respecter les politiques en matière de sécurité du gouvernement. En pratique, SPC dispose de ses propres instruments politiques internes en matière de sécurité, chacun servant de guide en vue de la mise en œuvre uniforme d'une norme de sécurité des technologies de l'information[228]. SPC dirige actuellement 12 projets de cybersécurité actifs, organisés en trois secteurs : identité et contrôle de l'accès, connectivité, et surveillance. Ces secteurs et leur pertinence à la cyberdéfense sont vus ci-dessous.

Identité et contrôle de l'accès

143. La vérification de l'identité d'un utilisateur et le contrôle de son accès aux éléments requis d'une infrastructure numérique ministérielle sont essentiels à la sécurité des systèmes numériques[229]. Les contrôles liés à l'identité et à l'accès visent à vérifier qu'un utilisateur est autorisé à accéder seulement aux ressources numériques dont il a besoin, selon son rôle au sein d'une organisation. Par le passé, le gouvernement a utilisé l'approche « château et douves », où l'objectif principal était de sécuriser le périmètre du réseau, authentifiant et accordant l'accès aux utilisateurs autorisés à des points d'entrée sécurisés, et superposant les systèmes de défense (comme des coupe-feux) pour filtrer l'accès au réseau. SPC l'a décrit comme étant [traduction] « une posture approfondie de défense employant une série de mécanismes superposés pour protéger les données et l'information d'intérêt. Si un mécanisme échoue, un autre passe à l'action pour contrecarrer immédiatement une attaque[230]. »

144. SPC indique que cette approche est de moins en moins viable dans un environnement numérique marqué par la prolifération d'appareils et d'options de connexion et les exigences accrues des utilisateurs en ce qui a trait à la mobilité. Par conséquent, il met en œuvre plusieurs projets en vue de moderniser les contrôles liés à l'identité et à l'accès. Ils reposeront sur des

---

[226] CST, « NSICOP Cyber Defence Review – Information Package #17 – Table of Contents, p. 1 », 11 mars 2021.
[227] SPC, *Departmental Security Plan 2019–2022*, 15 mai 2019.
[228] Les 16 normes de sécurité des technologies de l'information de SPC couvrent de nombreux secteurs, y compris la gestion des journaux des systèmes de sécurité, l'intégrité de la chaîne d'approvisionnement, la sécurité du périmètre, la gestion des correctifs pour les serveurs et les postes de travail, ainsi que l'accès au réseau et à Internet. Les normes de sécurité des technologies de l'information de SPC sont disponibles à l'adresse http://service.ssc-spc.gc.ca/fr/politiques_processus/politiques.
[229] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.
[230] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.

moyens de défense des périmètres efficaces permettant la vérification et l'autorisation continues des utilisateurs et des appareils. Voici les plus importants.

- **Authentification des appareils sur le réseau (Network Device Authentication) :** L'authentification des appareils sur le réseau sert à améliorer l'authentification d'appareils sur les réseaux gouvernementaux (par opposition à chaque utilisateur et à ses comptes). Le projet vise à améliorer les contrôles d'accès, les fonctions de vérification et l'analyse judiciaire des appareils qui accèdent à un réseau, le dernier représentant une lacune importante dans la réponse aux compromissions des systèmes gouvernementaux[231].
- **Modernisation de l'accès à distance sécurisé (Secure Remote Access Modernization) :** À l'heure actuelle, chaque ministère est chargé de l'accès sécurisé à distance aux réseaux gouvernementaux. Ce projet vise à migrer l'accès sécurisé à distance vers un système d'entreprise consolidé à l'échelle du gouvernement. Le projet améliorera les fonctions de cyberdéfense liées à la connectivité à distance, y compris les journaux de connectivité, l'analyse liée à la détection des menaces et la gestion du volume du trafic[232].
- **Service de contrôle de l'accès administratif (Administrative Access Controls Service) :** Les administrateurs de réseau partagent et réutilisent souvent des mots de passe, ce qui réduit le nombre d'obstacles que doivent franchir les cyberattaquants tentant d'obtenir un accès étendu à de multiples réseaux au sein d'un ministère et entre ministères. Le projet vise à éliminer cette pratique en normalisant et en appliquant la gestion des privilèges d'administration[233].
- **Gestion des comptes du répertoire des justificatifs d'identité (Directory Credential Account Management) :** Le projet est conçu pour accroître la collaboration des partenaires et des clients de SPC dans les environnements d'infonuagique en synchronisant les justificatifs d'identité des utilisateurs au moyen d'un service d'authentification des utilisateurs centralisé dans le nuage. Il permettra à SPC d'authentifier l'identité d'un utilisateur entre les lieux de travail sur nuage et hors nuage[234].
- **Service d'authentification centralisé interne (Internal Centralized Authentication Service) :** Le projet fournira des justificatifs d'identité (p. ex. les noms d'utilisateur et les mots de passe) standardisés à l'échelle du gouvernement, et un service d'authentification centralisé pour appuyer l'accès Web aux applications internes peu importe l'organisation. Il permettra la transition vers une technologie de sécurité par justificatifs d'identité plus robuste et la mise hors service de technologies de navigateur ayant des vulnérabilités liées à la sécurité[235].

---

[231] Pendant une cyberattaque, les représentants passent souvent beaucoup de temps à analyser les données judiciaires pour différencier l'activité légitime sur le réseau de l'activité de cyberacteurs malveillants.
[232] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.
[233] SPC, « Administrative Access Control Services. Project Proposal (version 1.7) », 12 septembre 2016, PDF. Ce projet répond au rapport du vérificateur général de l'automne 2015 sur les services partagés de la technologie de l'information au gouvernement du Canada.
[234] SPC, « Directory Credential Account Management (DCAM) – DCAM Overview (version 1.7) », 5 décembre 2019, PDF.
[235] SPC, « Internal Centralized Authentication Service (ICAS): Concept of Operations (Con-Ops) (version 1.1) », 8 octobre 2020.

Connectivité

145. La gestion de la connectivité numérique pour les utilisateurs et les systèmes du gouvernement représente un défi important en matière de cyberdéfense. Le réseau actuel du gouvernement est un mélange complexe de connectivité de télécommunications à environ 4 000 emplacements, 5 000 immeubles et des centaines de milliers d'appareils numériques fixes et mobiles pour les employés et les sous-traitants du gouvernement au Canada et à l'étranger[236]. Par le passé, les ministères exploitaient plus de 720 centres de données d'un bout à l'autre du Canada, sans infrastructure partagée, normes de configuration ou de connectivité de réseau, procédures d'exploitation ou niveaux de service standardisés en ce qui a trait à la redondance et à la disponibilité[237]. Pour s'attaquer aux nombreuses difficultés que cette situation représente, SPC prévoit de regrouper les centres de données patrimoniales en quatre points centraux régionaux, de mettre en œuvre une approche « sans-fil d'abord » pour la connectivité au sein d'un immeuble et d'adopter de nouvelles technologies (comme le 5G et l'utilisation élargie de la technologie mobile)[238]. L'évolution des mesures de connectivité de SPC demandera des mesures de sécurité proportionnelles pour protéger les réseaux, les centres de données et leurs utilisateurs. Les projets de connectivité de SPC dans ce domaine comprennent ce qui suit :

- **Sécurité du périmètre d'entreprise (Enterprise Perimeter Security) :** Le projet vise à améliorer la visibilité des cybermenaces qui ciblent les réseaux du gouvernement et leurs connexions aux environnements d'infonuagique ministériels. En tirant parti des projets sur l'identité et le contrôle de l'accès, ce projet permet une connectivité sécurisée à distance aux réseaux gouvernementaux, de n'importe où, y compris par l'entremise de liens de connexion physiques ou virtuels. Ce projet offrira également à SPC et au CCC une visibilité additionnelle sur les cybermenaces[239].
- **Mise en œuvre et défense d'un nuage sécurisé (Secure Cloud Enablement and Defence) :** Le projet offrira les contrôles de connectivité et de sécurité (points d'accès contrôlés et surveillés) nécessaires pour que les ministères accèdent aux informations sensibles sur les réseaux d'infonuagique et les y sauvegardent. Les contrôles comprendront une connexion et une surveillance centralisées afin de repérer et de gérer les événements liés à la sécurité qui touchent les données sur les nuages et les menaces aux réseaux gouvernementaux qui peuvent provenir d'un environnement d'infonuagique et cibler le réseau de base du gouvernement. Semblable au projet de sécurité du

---

[236] Il s'agit notamment des ministères dans les immeubles à locataires uniques ou multiples situés à différents endroits au Canada, utilisant une infrastructure filaire, une connectivité sans fil et des approches variées au déploiement, à la maintenance et à la sous-traitance de la technologie auprès de vendeurs et de fournisseurs de service de télécommunications.

[237] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.

[238] SSC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.

[239] SPC, « Networks, Security, and Digital Services and the Senior Assistance Deputy Minister, Project Management and Delivery. For Decision. Enterprise Perimeter Security (EPS) Authority to Operate (ATO) », note de service au représentant autorisé et au sous-ministre adjoint principal, sans date; et SPC, *Enterprise Perimeter Security (EPS)*, rapport d'évaluation de la sécurité, 7 avril 2020.

périmètre d'entreprise, ce projet augmentera la visibilité sur les cybermenaces pour SPC et le CCC[240].

- **Développement de l'infrastructure secrète (Secret Infrastructure Expansion) :** SPC gère une infrastructure consacrée à l'entreposage et à la transmission d'information classifiée Secret. À l'heure actuelle, 31 ministères profitent de l'infrastructure, et ce projet la développera pour en faire profiter certains nouveaux clients et augmentera les services offerts pour un certain nombre de ses clients[241]. Ce projet corrigera une importante lacune. En effet, par le passé, certains ministères traitaient des renseignements Secret sur leur réseau non classifié, entraînant la perte d'information classifiée au profit d'acteurs étatiques[242].
- **Téléphone intelligent pour réseau classifié (SmartPhone for Classified) :** Certains représentants gouvernementaux ont besoin de communiquer de façon sécurisée au moyen de leur téléphone et de données mobiles pour soutenir les opérations. Ce projet s'appuiera sur un principe de validation du CST pour offrir une capacité initiale de 2 000 utilisateurs du gouvernement au Canada et à certains emplacements à l'étranger, dont l'extensibilité peut atteindre jusqu'à 10 000 utilisateurs[243].

Surveillance

146. La surveillance relative à la sécurité de l'infrastructure de la technologie de l'information du gouvernement assure son rendement constant et fiable, et contribue à la poursuite des activités du gouvernement et à la prestation de services aux Canadiens. La surveillance des activités comprend le repérage d'événements liés à l'identification et à l'authentification des utilisateurs sur un réseau ou un appareil, la surveillance du trafic de réseau qui passe par une liaison de communications du gouvernement, et l'utilisation d'applications sur des appareils d'utilisateurs. Une surveillance proactive réussie permet aux administrateurs de repérer les événements de sécurité sur les appareils du réseau et de s'employer à les résoudre rapidement. Ce n'est pas la situation à l'heure actuelle. La surveillance relative à la sécurité des réseaux du gouvernement est incohérente; les réseaux sont parfois surveillés par SPC, les partenaires principaux de SPC ou des organisations qui n'ont pas de lien avec SPC. De plus, le propre système d'information de sécurité et de gestion des événements de SPC n'est pas standard pour tous ses clients[244]. D'une manière générale, SPC n'a pas une vue complète des

---

[240] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020; et SPC, « SSC Networks, Security and Digital Services: Cyber and IT Security Program », exposé devant l'Agence du revenu du Canada (ARC), 4 février 2020.

[241] SPC, « Government of Canada Secret Infrastructure Expansion (GCSI Expansion) », analyse de rentabilisation (version 2.2), 28 septembre 2020; SSC, « Government of Canada Classified (SECRET) Information Technology Convergence Update », 8 avril 2020; SPC, « Government of Canada Secret Infrastructure Expansion (GCSI Expansion), Project Management Plan », 28 septembre 2020; et SPC, « Secret Infrastructure: 34 Legacy Networks », sans date.

[242] Voir l'étude de cas sur la compromission de 2010-2011 des réseaux du SCT et du ministère des Finances par la Chine.

[243] SPC, « SmartPhone for Classified », analyse de rentabilisation de la mise en œuvre (version 0.13), 19 octobre 2020.

[244] Bien que SPC fournisse la plateforme électronique pour la gestion de l'information et des événements en matière de sécurité, le CCC est responsable de sa configuration et de son opération, ainsi que de la surveillance des événements.

réseaux gouvernementaux pour repérer les risques et répondre rapidement aux incidents, faisant en sorte que la responsabilité de la surveillance des réseaux de l'ensemble du gouvernement est incohérente[245].

147. Prenant appui sur le regroupement des centres de données du gouvernement, SPC met en œuvre trois projets pour centraliser sa surveillance relative à la sécurité en vue d'accroître sa connaissance des activités sur les réseaux du gouvernement et d'accroître la rapidité et la coordination des ressources de réponse aux incidents[246]. Ces projets :

- améliorent la connaissance en temps réel de SPC de la posture de sécurité des appareils de points finaux (p. ex. des ordinateurs portatifs, des ordinateurs de bureau, des tablettes et des serveurs)[247];
- améliorent la connaissance de SPC des vulnérabilités de sécurité dans les grands ensembles d'éléments de la technologie de l'information d'entreprise du gouvernement (p. ex. au sein des centres de données)[248];
- surveillent les communications de réseau en ce qui a trait aux événements qui peuvent indiquer un possible incident de sécurité et informer les utilisateurs de SPC qu'ils doivent prendre les mesures pour étudier le problème et y répondre au besoin[249].

Pour les trois projets, SPC se concentre sur l'automatisation de la surveillance des connexions réseau et des appareils déployés, ainsi que l'évaluation de leur posture de sécurité par rapport aux vulnérabilités connues et aux cybermenaces émergentes. Chaque projet est élaboré pour améliorer la connaissance de SPC de la situation et corriger les lacunes relevées quant à la sécurité du réseau du gouvernement (p. ex. le manque de connaissances sur les correctifs les plus récents pour les vulnérabilités en matière de sécurité). Dans le cas d'un cyberincident grave, les projets visent à accroître la capacité d'évaluer, en temps réel, les faiblesses du réseau d'entreprise et à réduire le temps nécessaire pour repérer un cyberincident, y répondre et s'en remettre.

---

[245] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020. Il convient de noter que les ministères sont aussi responsables de surveiller et de sécuriser leurs réseaux et points terminaux (voir les paragraphes 102 à 105).
[246] SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.
[247] SPC, « Endpoint Visibility Awareness and Security Project. Project Management Plan (version 1.0) », 30 mars 2020. Voir aussi SPC, « SSC Networks, Security and Digital Services: Cyber and IT Security Program », exposé devant l'ARC, 4 février 2020. Lorsqu'il sera entièrement mis en œuvre, le projet fournira une information automatisée sur près de 900 000 points finaux dans l'ensemble des réseaux gouvernementaux, regroupant les aperçus individuels des ministères en un portrait global pour tout le gouvernement.
[248] Le projet « Enterprise Vulnerability and Compliance Management », mentionné dans SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020.
[249] Le projet « Security Information and Event Management », SPC, « Security Information and Event Management », analyse de rentabilisation (version 1.1), 6 novembre 2018; et SPC, « SSC Networks, Security and Digital Services: Cyber and IT Security Program », exposé devant l'ARC, 4 février 2020. Voir aussi SPC, « Shared Services Canada: Network and Security Strategy (version 1.6) », 1er septembre 2020. Le CCC est maintenant responsable de ce projet.

Partenaires et clients de SPC

148. SPC fournit des services aux trois catégories de ministères et organismes suivantes. Les catégories déterminent le type de services fournis, la latitude de certaines organisations à choisir les services de SPC qu'elles utiliseront et la façon dont les coûts liés aux services sont répartis :

- **Partenaires principaux :** Depuis 2011, SPC est responsable de la gestion de l'infrastructure du réseau pour 43 ministères et organismes partenaires. À l'époque, ces organisations ont transféré leurs budgets et leur effectif respectifs pour les services de courriel, de centre de données et de réseau à SPC, et ont donc reçu tous les services de SPC sans coûts additionnels.
- **Clients obligatoires :** En 2015, le mandat de SPC a été élargi afin d'inclure des clients obligatoires. Ces organisations, qui comprennent de petits ministères et organismes, doivent utiliser certains services de SPC pour ce qui est des courriels, des centres de données, des réseaux et des appareils finaux, ou pour obtenir une autre infrastructure numérique. À l'heure actuelle, SPC compte 39 clients obligatoires qui paient les services de SPC selon un principe de recouvrement des coûts[250].
- **Clients facultatifs :** En 2015, le mandat de SPC a été élargi afin d'inclure des clients facultatifs. Ces clients peuvent demander les services de SPC selon un principe de recouvrement des coûts, et peuvent comprendre un gouvernement provincial ou une municipalité, un organisme d'aide canadien, une organisation de la santé publique, une organisation intergouvernementale ou un gouvernement étranger. SPC compte 78 clients facultatifs[251].

À l'heure actuelle, SPC fournit une partie ou la totalité de ses services à 160 des 169 organisations du gouvernement fédéral.

149. L'éventail des organisations qui reçoivent des services de SPC a de grandes incidences sur le cadre de cyberdéfense du gouvernement. Au fur et à mesure de son évolution, SPC a mis en place des mesures de plus en plus exhaustives pour protéger les infrastructures numériques (comme la réduction des points de connexion à Internet et l'introduction des capteurs et des moyens de défense pointus du CST dans les passerelles Internet de SPC) et, dans le cadre de ses projets visant à moderniser l'infrastructure numérique du gouvernement, a élaboré une approche de type « sécurisé dès la conception » aux solutions relatives aux courriels, aux centres de données et aux réseaux[252]. Même si cette évolution a comporté d'importantes difficultés pour SPC et ses organisations partenaires, les 43 partenaires

---

[250] SPC, « Improve the Internet Security Posture of Small Departments and Agencies », analyse de rentabilisation, 15 décembre 2020. Il y avait 40 clients en 2015. Voir aussi SPC, « Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20 », présentation, fournie au Secrétariat du CPSNR, 24 mars 2021.
[251] SPC, « Au service du gouvernement : Décret 2015-1071 : Questions et réponses », http://service.ssc-spc.gc.ca/fr/politiques_processus/decret2015-1071-qr. SPC fournit actuellement un service d'infrastructure à clé publique à deux organisations, le bureau d'un ministre du gouvernement de la Colombie-Britannique et la Police provinciale de l'Ontario, et un service de RE du GC au gouvernement de l'Ontario.
[252] SPC, « Re: NSICOP Discussion on Mandate with Committee Secretariat », courriel, 21 mai 2021.

principaux de SPC ont profité automatiquement des avantages en raison de leur statut à titre d'organisations qui reçoivent tous les services de SPC[253].

150. La situation ne s'applique pas aux clients obligatoires et facultatifs de SPC. Ces clients varient considérablement sur le plan de la taille, du mandat, de la complexité, de la modernité de leur infrastructure numérique et de leur budget lié à la technologie numérique et à la sécurité[254]. Certaines des organisations obtiennent des services de SPC par l'entremise de liens avec les partenaires principaux de SPC[255]; d'autres ont seulement recours à une sélection de services de SPC; d'autres obtiennent un mélange de services de technologie de l'information de SPC et de fournisseurs de services privés; et d'autres ne se connectent pas du tout à un réseau du gouvernement[256]. Bon nombre de ces organisations sont connues comme étant de petits ministères et organismes, définies comme ayant un effectif de moins de 500 employés et un budget annuel de moins de 300 millions de dollars. Ces ministères et organismes représentent un risque pour la sécurité des réseaux gouvernementaux pour trois raisons :

- leur connectivité aux points d'accès sécurisés à Internet de SPC et à l'accès infonuagique sécurisé fourni par courtage de SPC peut être absente. Dans de tels cas, les ministères et organismes ne profiteraient pas de la cybersurveillance de pointe du CCC;
- ils emploient différents services de connectivité à Internet, souvent en provenance de multiples endroits, et maintiennent une connectivité à d'autres ministères;
- ils possèdent des ressources limitées (personnel ou ressources financières) pour répondre aux problèmes de sécurité Internet, entraînant des mesures de cyberdéfense non uniformes[257].

Notamment, SPC a relevé quatre ministères et organismes qui représentaient des risques élevés ou critiques pour les réseaux du gouvernement en raison de leurs connexions simultanées aux réseaux du gouvernement et aux services Internet d'un tiers dont les mesures

---

[253] SPC a indiqué avoir hérité de nombreux systèmes disparates de ses ministères partenaires et que l'effort nécessaire pour concevoir et mettre en œuvre une approche de sécurité d'entreprise pour tous ses partenaires s'est avéré itératif. SPC, « Addendum to the Business Case for the Small Departments and Agencies Study », 30 novembre 2020. Il a été difficile pour certains ministères, comme la Gendarmerie royale du Canada, de faire reconnaître leurs exigences opérationnelles uniques par SPC.

[254] SPC, « Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20 », présentation fournie au Secrétariat du CPSNR, 24 mars 2021.

[255] Huit organisations, y compris le Conseil national des produits agricoles (sous l'égide d'Agriculture et Agroalimentaire Canada); le Tribunal d'appels des anciens combattants (sous l'égide d'Anciens combattants Canada); la Commission de l'assurance-emploi du Canada (sous l'égide d'Emploi et Développement social Canada); Services aux Autochtones Canada (sous l'égide de Relation Couronne-Autochtones et Affaires du Nord Canada); la Commission des libérations conditionnelles (sous l'égide du Service correctionnel du Canada); le Bureau de l'enquêteur correctionnel (sous l'égide du Service correctionnel du Canada); la Commission des débats des chefs (sous l'égide du Bureau du Conseil privé); et la Commission du droit d'auteur (sous l'égide d'Innovation, Sciences et Développement économique Canada). SPC, « Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20 », présentation, 24 mars 2021.

[256] SPC, « Mandatory Clients (MCs) IT Service Landscape Survey: As of Winter 2019-20 », présentation, 24 mars 2021.

[257] SSC, « Improve the Internet Security Posture of Small Departments and Agencies », analyse de rentabilisation, 15 décembre 2020.

de défense sont inexistantes ou faibles[258]. En résumé, ces organisations détiennent des données gouvernementales et ont souvent des liens électroniques avec les ministères, mais ne profitent pas nécessairement de l'éventail des mesures de cyberdéfense de SPC (et du CST) ni des projets « sécurisés dès la conception » de SPC visant à moderniser l'infrastructure numérique du gouvernement. (La situation s'applique aussi aux clients obligatoires qui n'utilisent pas le Service Internet d'entreprise de SPC.) Par conséquent, les cyberattaques contre des organisations (y compris la perte de données) peuvent passer inaperçues et le gouvernement pourrait ne pas être en mesure de réagir de façon efficace ou tout court aux cyberincidents sensibles. L'incapacité de ces organisations à se protéger adéquatement est un risque pour leur propre infrastructure numérique et potentiellement pour d'autres organisations gouvernementales.

151. En 2020, SPC a monté un projet sur quatre ans pour agir face aux problèmes causés par les organisations qui sont connectées aux réseaux du gouvernement du Canada sans devoir installer des moyens de cyberdéfense solides ou être l'objet de la surveillance de SPC ou du CCC. Le projet pour les petits ministères et organismes (Small Departments and Agencies Project) vise à faire passer le niveau de sécurité réseau de tous les petits ministères et organismes et des clients obligatoires (61 au total) au niveau maximum de la sécurité réseau de SPC en leur fournissant un accès au réseau de base du gouvernement (RE du GC), une sécurité réseau complète au même niveau que les partenaires principaux de SPC, une surveillance par le CCC et la mise en œuvre par SPC de toutes les améliorations à la sécurité réseau[259]. Le projet cible les objectifs principaux suivants :

- faire entrer tous les clients obligatoires et les petits ministères et organismes « à l'intérieur de l'enceinte de sécurité » afin qu'ils puissent se servir des points d'accès à Internet sécurisés de SPC, ce qui réduirait le nombre de connexions externes aux réseaux ministériels;
- regrouper les points de connexion à Internet au moyen des points centraux régionaux de communications de SPC, ce qui améliorerait la visibilité du trafic réseau de SPC et du CCC, et permettrait à ces derniers d'appliquer des mesures de cyberdéfense plus élevées en vue de repérer et de limiter les entrées non autorisées, l'exfiltration de données et d'autres activités malveillantes;
- améliorer la posture du gouvernement en matière de cybersécurité en éliminant différentes classes de sécurité réseau pour les partenaires et les clients obligatoires de SPC[260].

Nonobstant l'importance de ce projet, aucun budget ni calendrier n'y est associé[261].

---

[258] SSC, « Improving the Internet Security Posture of Small Departments and Agencies Study: Survey Report (version 1.0) », 15 décembre 2020.
[259] SSC, « Improve the Internet Security Posture of Small Departments and Agencies », analyse de rentabilisation, 15 décembre 2020.
[260] SPC, « Improve the Internet Security Posture of Small Departments and Agencies », analyse de rentabilisation, 15 décembre 2020.
[261] SPC, « SSC Comments », courriel au Secrétariat du CPSNR, 28 juillet 2021.

Gestion des événements de cybersécurité

152. Dans le cadre de ses responsabilités élargies, SPC coordonne avec ses partenaires les interventions face aux cyberincidents graves. SPC est responsable :

- de bloquer les activités de cybermenace ciblant les réseaux gérés par SPC et d'atténuer leurs répercussions;
- de répondre aux recommandations du CCC et de veiller à ce que les mises à jour et les mesures d'atténuation soient appliquées en temps opportun;
- de mettre en œuvre les efforts de prévention, d'atténuation et de reprise des activités (entre autres, il pourrait s'agir de fermer ou d'isoler des réseaux précis);
- de participer à l'identification des événements de cybersécurité au sein du gouvernement et à leur atténuation, à l'évaluation des risques, à la reprise des activités et aux analyses après événement;
- d'évaluer l'incidence à l'échelle du gouvernement des événements, des menaces et des vulnérabilités de cybersécurité sur la prestation des programmes et des services;
- d'établir des rapports après événement, y compris la chronologie des événements et une analyse des causes premières, et de les soumettre au CCC[262].

Comme il est indiqué, ces responsabilités sont coordonnées avec les partenaires principaux, notamment le CCC et le SCT (par l'entremise du dirigeant principal de l'information du Canada).

Résumé

153. SPC a été créé en 2011 afin de fournir des services de technologie de l'information à un groupe d'organisations fédérales qui représentaient la majorité des dépenses du gouvernement liées à l'infrastructure numérique. Au fil des années, le mandat de SPC a évolué, tout comme son offre de services de sécurité et de défense à ses partenaires et clients. Depuis sa création à titre d'organisation au service de 43 partenaires principaux, SPC a grandi et fournit maintenant des services à 160 différentes organisations au sein du gouvernement du Canada. Même si l'approche de type « sécurisé dès la conception » de SPC a facilité une posture de sécurité solide pour les organisations qui recevaient ses principaux services de cybersécurité et de cyberdéfense, les incohérences dans la prestation de service aux clients obligatoires et facultatifs ont présenté des difficultés et des risques de cybersécurité pour le reste du gouvernement. Le Comité reprend cette considération dans son évaluation.

[262] SCT, « Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) », 2019. Certaines de ces responsabilités ont été confiées au CCC depuis sa création en 2018.

Le Centre de la sécurité des télécommunications

154. Le Centre de la sécurité des télécommunications (CST) est une pièce maîtresse du cadre de cyberdéfense du gouvernement. Le CST recueille des renseignements sur les menaces qui pèsent sur les systèmes et les réseaux du gouvernement, gère un réseau sophistiqué de défense par couches au moyen de capteurs permettant de repérer et de bloquer ces menaces, et prodigue des directives ainsi que des conseils aux organisations gouvernementales (et de plus en plus aux Canadiens et aux organisations du secteur privé) pour les aider à renforcer leurs propres systèmes de sécurité des technologies de l'information. La présente section se penche sur les pouvoirs en vertu desquels le CST se charge de diriger ces activités et sur les mécanismes de gouvernance qui permettent d'assurer un contrôle sur ces activités ainsi que de veiller à ce que le CST rende des comptes au ministre de la Défense nationale. La section se poursuit en abordant les activités de cyberdéfense à proprement parler ainsi que le résultat de ces activités. Pour illustrer les principaux enjeux, le Comité fait référence à des études de cas fondées sur des cyberincidents qui ont réellement eu lieu.

Mandats et pouvoirs du CST en matière de cybersécurité

155. Le 18 décembre 2001, le Parlement a adopté la *Loi antiterroriste*[263]. Cette loi modifiait la *Loi sur la défense nationale* en y incluant la partie V.1, Centre de la sécurité des télécommunications. Pour la première fois, le pouvoir permettant au CST de diriger ses propres activités n'était plus fondé sur la prérogative de la Couronne, mais sur des dispositions législatives. En vertu de cette Loi, le mandat du CST comportait désormais trois volets :

a) l'acquisition et l'utilisation de renseignements étrangers en conformité avec les priorités du gouvernement en matière de renseignement;
b) la prestation d'avis, de conseils et de services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement;
c) la prestation d'assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

156. La Loi prévoyait bon nombre de mesures de contrôle et de responsabilisation. En outre, les activités menées au titre des mandats a) et b) ne doivent jamais viser les Canadiens ni les personnes se trouvant en territoire canadien, et le CST est tenu de mettre en place des mesures visant à protéger la vie privée des Canadiens lorsqu'il est question d'utiliser et de conserver des données interceptées. La Loi a également créé un système d'autorisations ministérielles permettant au CST d'intercepter des communications privées aux fins de collecte de renseignements étrangers et de protection des systèmes informatiques du gouvernement du

[263] *Loi sur la défense nationale*, L.R.C., 1985, ch. 95, paragraphes 273.64(1) et 273.64(2) (avant l'adoption du projet de loi C-59 et de la *Loi sur le Centre de la sécurité des télécommunications*), http://laws-lois.justice.gc.ca/fra/lois/n-5/20181218/p1TT3xt3.html.

Canada[264]. Il s'agissait là d'un changement crucial : avant d'obtenir ces autorisations, la capacité du CST à remplir ses mandats en matière de collecte de renseignements étrangers et de protection de l'information était constamment réduite en raison de l'élargissement fulgurant de l'infrastructure mondiale de l'information numérique. Pour être en mesure de mener certaines activités de protection des systèmes et des réseaux du gouvernement, le CST devait obtenir des autorisations ministérielles lorsque certaines conditions étaient respectées[265]. Le mandat en trois volets ainsi que les autorisations afférentes ont permis au CST de développer et de mener des activités de cyberdéfense novatrices sur les systèmes informatiques et sur les réseaux du gouvernement, notamment des activités de mise à l'essai de mécanismes actifs de sécurité réseau visant à *mesurer* l'état de sécurité de certains systèmes et réseaux gouvernementaux, de même que des activités de cyberdéfense visant à *protéger* certains systèmes et réseaux du gouvernement[266].

157. La *Loi sur le Centre de la sécurité des télécommunications* (Loi sur le CST) a reçu la sanction royale le 21 juin 2019. La Loi sur le CST a considérablement modifié la mission du CST sur plusieurs plans, à savoir le mandat, les pouvoirs, les immunités et la surveillance. La Loi a prescrit un mandat global à l'organisme faisant de celui-ci « l'organisme national du renseignement électromagnétique en matière de renseignement étranger et l'expert technique de la cybersécurité et de l'assurance de l'information »[267]. En outre, la Loi définissait cinq volets du mandat du CST : le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives, les cyberopérations actives et l'assistance technique et opérationnelle[268]. Les volets du mandat du CST qui s'avèrent les plus pertinents dans le cadre du présent examen sont, d'une part, la cybersécurité et l'assurance de l'information et, d'autre part, les cyberopérations défensives.

Cybersécurité et assurance de l'information

158. La Loi sur le CST *établit* le mandat du CST dans la sphère de la cybersécurité et de l'assurance de l'information. Ce mandat consiste à fournir des conseils, des avis et des services visant à protéger non seulement les informations électroniques et les infrastructures de

---

[264] La *Loi sur la défense nationale* (art. 273.69) précise que la partie VI du *Code criminel* ne s'applique pas à l'interception des communications privées, lorsque celles-ci sont autorisées par le ministre. Le régime des autorisations ministérielles s'applique également aux activités de renseignement électromagnétique du CST; ces activités ne sont pas abordées dans la présente.

[265] Ces conditions étaient les suivantes : l'interception est nécessaire pour identifier, isoler ou prévenir les activités dommageables visant les systèmes du gouvernement; les renseignements à obtenir ne peuvent raisonnablement être obtenus d'une autre manière; le consentement des personnes dont les communications peuvent être interceptées ne peut être obtenu; seuls les renseignements qui sont essentiels pour identifier, isoler ou prévenir les activités dommageables visant les systèmes du gouvernement seront utilisés ou conservés; des mesures satisfaisantes sont en place pour protéger la vie privée des Canadiens. *Loi sur la défense nationale*, L.R.C., 1985, ch. 95, paragraphes 273.65(1) à 273.65(4) (avant l'adoption du projet de loi C-59 et de la *Loi sur le Centre de la sécurité des télécommunications*), http://laws-lois.justice.gc.ca/fra/lois/n-5/20181218/p1TT3xt3.html.

[266] *Loi sur la défense nationale*, L.R.C., 1985, ch. 95, paragraphe 273.65(9), (avant l'adoption du projet de loi C-59 et de la *Loi sur le Centre de la sécurité des télécommunications*), http://laws-lois.justice.gc.ca/fra/lois/n-5/20181218/p1TT3xt3.html. La Loi réduit en termes explicites l'application du régime des autorisations ministérielles aux « institutions fédérales », tel qu'il est énoncé dans la *Loi sur les langues officielles*.

[267] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 15(1) et 15(2).

[268] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 15(1) et 15(2).

l'information des institutions fédérales, mais aussi celles des organisations non fédérales qui sont jugées comme étant importantes pour le gouvernement du Canada[269]. La loi *active* les mandats en matière de cybersécurité et d'assurance de l'information en autorisant le CST à acquérir, à utiliser et à analyser les données tirées de l'infrastructure mondiale de l'information (p. ex. Internet et les systèmes de communication mobiles) par voie d'autorisations ministérielles ou par d'autres sources (p. ex. informations accessibles au public), ce qui permet à l'organisme d'offrir des conseils, des avis et des services[270]. En termes pratiques, cela signifie que l'information acquise dans le cadre du volet du renseignement étranger du CST peut être utilisée pour soutenir les volets de la cybersécurité et de l'assurance de l'information du CST, notamment l'acquisition et l'utilisation de l'information provenant des réseaux et des dispositifs informatiques du gouvernement.

159. Les autorisations ministérielles sont des éléments clés de ce volet. Ces autorisations permettent au CST, nonobstant les dispositions des autres lois du Parlement, d'accéder à une infrastructure de l'information d'une institution fédérale ou d'une organisation non fédérale désignée comme étant d'importance pour le gouvernement, ou à acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin d'aider à protéger cette infrastructure (dans ce contexte, contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement)[271]. Pour ce qui concerne les organisations non fédérales, le CST est autorisé à accéder à leurs systèmes pour ces motifs, mais uniquement si lesdites organisations ont d'abord été désignées, par voie d'arrêté ministériel, comme étant d'importance pour le gouvernement du Canada, et lorsque les propriétaires ou les opérateurs de ces organisations non fédérales ont demandé par écrit l'assistance du CST.

Cyberopérations défensives

160. Les cyberopérations défensives sont distinctes des activités menées dans le cadre du mandat en matière de cybersécurité et d'assurance de l'information. D'ailleurs, ces opérations sont d'autant plus risquées en raison de leur nature invasive et potentiellement perturbatrice. Conformément à la Loi sur le CST, en ce qui a trait au volet de son mandat touchant les cyberopérations défensives, le CST mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger l'information électronique et les infrastructures de l'information d'importance des institutions fédérales et l'information électronique et les infrastructures de l'information désignées comme étant d'importance pour le gouvernement du Canada[272].

---

[269] Les références de la présente section renvoient aux organisations non fédérales considérées comme étant d'importance pour le gouvernement. Dès lors que le Comité emploie le terme « gouvernement » dans ce contexte, celui-ci renvoie au gouvernement du Canada.
[270] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, sous-alinéas 17a)(i) et a)(ii), et alinéa 17b).
[271] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 27(1) et (2); et *Code criminel*, alinéa 184(2)e).
[272] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, alinéas 18a) et b).

161. Ainsi, le CST peut mener des cyberopérations défensives pour protéger, contre les cyberattaques, un réseau du gouvernement ou le réseau d'une entité désignée par le ministre. De telles opérations peuvent comprendre ce qui suit :

- accéder à des portions de l'infrastructure mondiale de l'information;
- installer, maintenir, copier, distribuer, rechercher, modifier, interrompre, supprimer ou intercepter quoi que ce soit dans l'infrastructure mondiale de l'information ou par son entremise;
- prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète de l'activité;
- mener toute autre activité qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou des catégories d'activités visées par l'autorisation[273].

162. Les cyberopérations défensives sont menées au titre d'autorisations ministérielles. Ces autorisations permettent au CST, malgré toute autre loi fédérale ou loi d'un État étranger, de mener, dans l'infrastructure mondiale de l'information ou par son entremise, toute activité précisée dans l'autorisation, dans la réalisation du volet de son mandat touchant les cyberopérations défensives[274].

Activités autorisées, contraintes, limites et conditions

163. La Loi sur le CST établit un certain nombre de contraintes, de limites et de conditions visant le déroulement des activités menées dans la réalisation des volets du mandat du CST touchant la cybersécurité et l'assurance de l'information, ainsi que les cyberopérations défensives. Premièrement, la Loi sur le CST interdit au Centre de diriger ses activités contre des Canadiens, peu importe où ils se trouvent, ou contre quiconque se trouvant au Canada. Qui plus est, la Loi stipule que les activités du CST ne peuvent porter atteinte aux droits de ces personnes, tel qu'il est énoncé dans la *Charte canadienne des droits et libertés*[275].

164. Deuxièmement, pour ce qui a trait aux activités de cybersécurité et d'assurance de l'information ainsi qu'aux cyberopérations défensives, la Loi sur le CST permet au CST de mener les activités ci-après :

- acquérir, utiliser, analyser, conserver et divulguer de l'information accessible au public;

---

[273] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 31 [alinéas a) à d)].
[274] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 29(1).
[275] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 22(1). La même interdiction s'applique dans le cas des activités menées dans la réalisation des volets renseignement étranger et cyberopérations actives du mandat. Pour ce qui concerne le volet assistance technique et opérationnelle de son mandat (où le CST est appelé à fournir une assistance technique ou opérationnelle à un organisme fédéral chargé de l'application de la loi ou de la sécurité, aux Forces canadiennes ou au ministère de la Défense nationale), le CST doit respecter les limites que la loi impose à ces entités. Ces limites comprennent toute restriction imposée par un mandat applicable.

- acquérir, utiliser, analyser, conserver et divulguer de l'information sur l'infrastructure à des fins de recherche et de développement ou de mise à l'essai de systèmes, ou pour mener des activités de cybersécurité et d'assurance de l'information dans l'infrastructure à partir de laquelle celle-ci a été acquise — ce qui permet la collecte d'information descriptive sur un réseau (p. ex. sur le plan de la configuration) de sorte à favoriser le déroulement des activités de cybersécurité et d'assurance de l'information;
- mettre à l'essai ou évaluer des produits, des logiciels et des systèmes, notamment pour des vulnérabilités[276].

165. Troisièmement, dès lors qu'il est autorisé à mener des activités de cybersécurité et d'assurance de l'information sur un réseau, le CST est en mesure de découvrir ou d'isoler des logiciels malveillants et de les empêcher de causer des dommages ou d'atténuer ceux-ci. Le CST peut également analyser l'information afin d'être en mesure de fournir des conseils sur l'intégrité de la chaîne d'approvisionnement ainsi que sur la fiabilité des télécommunications, de l'équipement et des services[277].

166. Quatrièmement, les autorisations ministérielles ont un rôle important lorsqu'il s'agit d'autoriser le CST à mener des activités hautement risquées dans ces domaines. Par exemple :

- Une autorisation ministérielle est exigée pour les activités menées dans la réalisation du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information qui risquent de contrevenir à une loi fédérale; qui visent l'acquisition d'information à partir de l'infrastructure de l'information d'organisations fédérales ou d'organisations non fédérales désignées comme étant d'importance pour le gouvernement; qui porteraient atteinte à une attente raisonnable de protection de la vie privée des Canadiens ou d'une personne se trouvant au Canada, ou qui risquent de contrevenir aux dispositions de la *Charte canadienne des droits et libertés*[278].
- Toutes les activités menées dans la réalisation du volet du mandat du CST touchant les cyberopérations défensives doivent se dérouler au titre d'autorisations ministérielles valides, et de telles autorisations ne peuvent être délivrées que si le ministre a préalablement consulté le ministre des Affaires étrangères. De plus, la Loi sur le CST interdit de diriger des cyberopérations défensives contre tout segment de l'infrastructure mondiale de l'information se trouvant en territoire canadien[279].

Bien que les cyberopérations défensives doivent toujours être menées au titre d'une autorisation ministérielle, les autres activités (p. ex. la prestation de conseils ou d'avis à l'intention d'un ministère) n'exigent pas ce type d'autorisation, puisqu'elles ne comportent pas le même risque d'enfreindre des dispositions de la *Charte canadienne des droits et libertés* ou de

---

[276] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 23(1).
[277] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, alinéas 23(3)a) et b).
[278] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 22(4).
[279] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, alinéas 22(2)a) et b), et paragraphe 29(2).

lois fédérales. Au reste, le rôle des autorisations ministérielles est abordé dans de plus amples détails dans la section suivante, qui porte sur la gouvernance.

Gouvernance des activités de cyberdéfense du CST

167. La Loi sur le CST constitue la pierre d'assise des pouvoirs, des responsabilités et de la gouvernance du CST. Cette Loi énonce quatre grandes catégories d'instruments de gouvernance visant les activités du CST. Les plus pertinentes, pour ce qui a trait à la cyberdéfense, sont les autorisations ministérielles, les arrêtés ministériels ainsi que les politiques et les orientations opérationnelles internes du CST. Chacun de ces instruments est décrit ci-après.

Autorisation ministérielle

168. Les autorisations ministérielles font partie de l'architecture de gouvernance des activités du CST depuis 2001. En vertu de la Loi sur le CST, le ministre de la Défense nationale peut délivrer trois types d'autorisations s'appliquant à la cyberdéfense :

- **Autorisation de cybersécurité — infrastructures fédérales :** Ces autorisations permettent au CST d'accéder au réseau d'une organisation fédérale ainsi que d'acquérir et d'utiliser toute information se trouvant dans le réseau aux fins de protection de ces ressources contre les méfaits, les utilisations non autorisées et les perturbations. Le ministre a délivré deux autorisations en vertu de la Loi au cours des exercices 2019-2020 et 2020-2021[280].
- **Autorisation de cybersécurité — infrastructures non fédérales :** Ces autorisations permettent au CST d'accéder au réseau d'une entité non gouvernementale préalablement désignée par le ministre comme étant d'importance pour le gouvernement, ainsi que d'acquérir et d'utiliser toute information se trouvant dans ce réseau aux fins de protection des ressources qu'il comporte contre les méfaits, les utilisations non autorisées et les perturbations. Le ministre n'a délivré qu'une seule autorisation de ce type depuis l'adoption de la Loi sur le CST[281].
- **Autorisation de cyberopérations défensives :** Ces autorisations permettent au CST de mener toute activité — énoncée dans le texte de l'autorisation — sur l'infrastructure mondiale de l'information ou par l'entremise de celle-ci pour contribuer à la protection de l'information électronique et des infrastructures de l'information des institutions fédérales ainsi que de l'information électronique et des infrastructures de l'information désignées comme étant d'importance pour le gouvernement. À ce chapitre, le ministre a délivré deux autorisations ministérielles au cours des exercices 2019-2020 et 2020-2021. Dans

---

[280] Les termes « méfait », « utilisation non autorisée » et « perturbation » sont employés au sens entendu par l'alinéa 184(2)e) du *Code criminel*. Les deux autorisations sont : CST, *Cybersecurity Authorization for Activities on Federal Infrastructures*, autorisation ministérielle, 1er août 2019; et CST, *Cybersecurity Authorization for Activities on Federal Infrastructures*, 30 juin 2020.

[281] CST, *Cybersecurity Activities on Non-Federal Infrastructures*, autorisation ministérielle, 7 novembre 2019.

le cas de la première autorisation, aucune cyberopération défensive n'a été menée pendant sa durée (ce cas est abordé plus loin)[282].

169. Le ministre ne peut délivrer une autorisation que pour des activités qu'il juge raisonnables et proportionnelles, et si des mesures satisfaisantes sont mises en place pour protéger la vie privée des Canadiens. Conformément aux nouvelles obligations que la Loi sur le CST lui impose, le chef du CST doit soumettre une demande par écrit au ministre, laquelle doit exposer les faits et fournir des descriptions permettant au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions de sa délivrance sont respectées[283].

170. Toutes les autorisations ministérielles, y compris celles relatives à la cybersécurité et aux cyberopérations défensives, doivent comprendre des éléments d'information particuliers, à savoir :

- les activités ou les catégories d'activités que le CST est autorisé à mener, et lesquelles de ces activités contreviendraient par ailleurs à toute autre loi fédérale;
- les personnes ou les catégories de personnes autorisées à mener les activités énoncées dans l'autorisation;
- les activités autorisées sont raisonnables et proportionnelles compte tenu de la nature de l'objectif à atteindre et des activités à mener;
- les conditions ou les restrictions que le ministre estime souhaitables dans l'intérêt public ou pour assurer que les activités visées par l'autorisation sont raisonnables et proportionnelles;
- tout autre élément qui est raisonnable dans les circonstances et est raisonnablement nécessaire afin de faciliter l'exécution des activités ou catégories d'activités autorisées par l'autorisation[284].

171. Cinq conditions additionnelles doivent être respectées avant que le ministre approuve une autorisation pour la cybersécurité (ces conditions s'appliquent aux systèmes fédéraux ainsi qu'aux systèmes désignés comme étant d'importance) :

- l'information à acquérir ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire;
- dans le cas des systèmes fédéraux, le consentement des personnes dont l'information peut être acquise ne peut raisonnablement être obtenu et, dans le cas des systèmes non fédéraux, le propriétaire ou l'opérateur du système demande assistance par écrit;

---

[282] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, alinéas 18a) et b) et paragraphes 27(1), 27(2), 29(1) et (2), et 34(1). Les deux autorisations sont : CST, *** *Defensive Cyber Operations*, autorisation de cyberopérations défensives, 5 septembre 2019; et CST, *** *Defensive Cyber Operations*, autorisation de cyberopérations défensives, 25 août 2020.
[283] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 33(1).
[284] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, art. 35 [alinéas a) à i)].

- l'information à acquérir est nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information en question;
- les mesures que le CST a mises en place pour protéger la vie privée permettront d'assurer que l'information acquise sur les Canadiens ou sur une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle pour découvrir, isoler, prévenir ou atténuer des dommages aux informations électroniques ou aux infrastructures de l'information en question;
- les conditions ou les termes que le ministre juge nécessaires pour renforcer la protection de la vie privée des Canadiens et des personnes se trouvant au Canada.

Toutes les autorisations ministérielles pour la cybersécurité sont examinées par le commissaire au renseignement pour veiller à ce que les conclusions menant à leur autorisation soient raisonnables. Les autorisations ministérielles n'ont aucun poids juridique tant que le commissaire au renseignement ne les a pas approuvées par écrit[285].

172. Deux autres conditions doivent être respectées avant que le ministre approuve une autorisation pour les cyberopérations défensives :

- l'objectif de l'autorisation ne pourrait pas être raisonnablement atteint par d'autres moyens;
- l'information sera acquise strictement en conformité avec une autorisation existante en vertu de la Loi sur le CST pour le renseignement étranger, la cybersécurité ou une autorisation en cas d'urgence, tel qu'il est indiqué dans la Loi.

De plus, le CST est tenu de ne pas « causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci » et de ne pas « tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie »[286]. Comme les cyberopérations défensives pourraient impliquer des relations que le Canada entretient avec d'autres États, le ministre de la Défense nationale ne peut délivrer une telle autorisation qu'après avoir consulté le ministre des Affaires étrangères[287]. Le commissaire au renseignement n'est pas appelé à examiner les autorisations pour les cyberopérations défensives.

173. Les autorisations ministérielles sont valides pour une période maximale d'un an et peuvent être modifiées, sous réserve de certaines conditions[288]. Le ministre peut également délivrer une autorisation en cas d'urgence — dont la période de validité peut aller jusqu'à cinq

---

[285] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 28(1) et (2).
[286] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, alinéas 32(1)a) et b). La Loi indique également que le terme « lésions corporelles » s'entend au sens de l'article 2 du *Code criminel*, lequel décrit le terme comme suit : « blessure qui nuit à la santé ou au bien-être d'une personne et qui n'est pas de nature passagère ou sans importance ».
[287] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 29(2).
[288] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 36(1) à 36 (4), 37(1) à 37 (4), 38, et 39(1) et (2).

jours — pour des activités menées aux fins du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information, et doit informer le commissaire au renseignement de cette autorisation. Après cette période, le CST doit faire appel au ministre pour lui demander une autorisation conforme aux procédures normales — pour peu que le commissaire au renseignement examine et approuve la demande — dans les cas où la validité de l'autorisation doit être maintenue[289].

Directive ministérielle

174. Les activités du CST doivent être conformes aux directives du ministre, et ce, dans les secteurs de la cybersécurité et de l'assurance de l'information ainsi que dans le secteur des cyberopérations défensives. Avant l'adoption de la Loi sur le CST en 2019, le Centre avait reçu des directives ministérielles portant sur les secteurs suivants :

- les priorités du gouvernement en matière de renseignement;
- les obligations redditionnelles envers le ministre;
- la protection de la vie privée des Canadiens;
- la collecte et l'utilisation des métadonnées;
- la gestion des relations avec les organisations tierces;
- la prévention de toute complicité dans les cas de mauvais traitement infligé par des entités étrangères.

Hormis la Directive ministérielle sur les priorités du gouvernement du Canada en matière de renseignement, toutes les directives ministérielles délivrées en vertu de la *Loi sur la défense nationale* ont cessé d'être en vigueur dès lors que les dispositions de la *Loi sur la défense nationale* concernant le CST ont été abrogées, le 1er août 2019, et que la Loi sur le CST est entrée en vigueur. La seule directive ministérielle active à laquelle le CST est assujetti (pour ce qui a trait aux priorités du gouvernement du Canada en matière de renseignement) a été délivrée en 2019. Cette directive se fonde sur les priorités en matière de renseignement approuvées par le Cabinet et oriente les efforts du CST vers la collecte et l'échange de renseignements, ainsi que vers la collaboration avec d'autres parties. Elle exige que le CST fasse rapport annuellement au ministre sur les travaux réalisés pour favoriser les priorités. Les cyberopérations et les opérations disposant de cybercapacités constituent l'une des quatre priorités énoncées par la directive[290].

Arrêté ministériel

175. Le ministre de la Défense nationale peut délivrer deux types d'arrêtés ministériels au CST relativement aux activités de cyberdéfense :

---

[289] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphes 40(1) à 40(4), et art. 41 et 42.
[290] CST, *Ministerial Directive to CSE on the Government of Canada Intelligence Priorities for 2019-2021*, 21 juin 2019; et CST, *NSICOP Cyber Defence Report- CSE Feedback on First Draft*, p. 4, 9 juillet 2021.

- un arrêté désignant les appareils, les réseaux et l'information d'une organisation non fédérale, qui sont considérés comme étant d'importance pour le gouvernement du Canada;
- un arrêté désignant les entités avec lesquelles le CST est autorisé à échanger, s'il y a lieu, de l'information se rapportant à des Canadiens, à des personnes se trouvant au Canada ou à des entreprises canadiennes, dans le but de protéger l'information et les systèmes des organisations fédérales ou de l'infrastructure essentielle[291].

Désignation d'organisations non fédérales comme étant d'importance pour le gouvernement

176. La Loi sur le CST stipule que le ministre peut délivrer un arrêté ministériel visant à désigner comme étant d'importance pour le gouvernement du Canada toute information électronique ou toute infrastructure de l'information. Ce qui signifie que là où se trouvent de l'information électronique ou des infrastructures d'information ne faisant pas partie d'institutions fédérales (p. ex. un réseau de recherche ou un aspect de l'infrastructure essentielle), le ministre peut désigner ces informations et ces infrastructures comme étant d'importance pour le gouvernement du Canada, permettant ainsi au CST de leur offrir des services. Là où ces services risquent de contrevenir à une loi fédérale (p. ex. le *Code criminel*) ou d'enfreindre les dispositions de la *Charte canadienne des droits et libertés*, le CST doit obtenir une autorisation ministérielle lui permettant de mener des activités de cyberdéfense visant à protéger ces systèmes désignés[292].

177. Le ministre de la Défense nationale a délivré deux arrêtés visant à désigner certaines catégories d'information électronique et d'infrastructures de l'information comme étant d'importance pour le gouvernement : le premier en juillet 2019, abrogé puis mis à jour en août 2020. L'arrêté n'a aucune date d'expiration et comprend ce qui suit :

- les 10 secteurs de l'infrastructure essentielle du Canada : les gouvernements (fédéral, provinciaux, territoriaux, municipaux et autochtones), l'énergie et les services publics, les technologies de l'information et des communications, les finances, l'alimentation, la santé, l'eau, les transports, la sûreté et l'industrie;
- l'information relative au mieux-être des Canadiens et l'infrastructure qui la contient légalement;
- les entités qui prennent part à la protection de l'information électronique et des infrastructures de l'information d'importance pour le gouvernement;
- les organismes multilatéraux qui se trouvent en territoire canadien et dont le Canada est membre;

---

[291] CST, *Gouvernance*, sans date, https://cse-cst.gc.ca/fr/reddition-de-comptes/gouvernance.
[292] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragraphe 21(1).

- les partis politiques canadiens provinciaux, territoriaux et fédéraux qui sont enregistrés ainsi que leur information électronique et leurs infrastructures de l'information;
- les établissements d'enseignement postsecondaire[293].

178. L'arrêté n'*oblige* pas le CST à offrir des conseils, des avis ou des services aux entités faisant partie de ces secteurs. Le CST doit plutôt recevoir une demande d'assistance de la part de ces entités, puis il doit tenir compte de plusieurs facteurs avant de déterminer si l'entité demanderesse fait partie ou non de l'une des catégories désignées par le ministre[294]. Dès lors qu'il est en mesure d'établir qu'une organisation non fédérale constitue une entité faisant partie de l'une des catégories désignées par le ministre, le CST peut ensuite offrir des conseils, des avis et des services destinés à protéger ladite entité contre les cyberattaques. Or, s'il détermine que le déploiement de ses capteurs de cyberdéfense ou la conduite de cyberopérations défensives seraient nécessaires à la protection de l'entité en question (ou du secteur d'activité), le CST doit demander une autorisation ministérielle[295]. Au mois de mai 2021, le CST avait déployé, au titre d'une autorisation ministérielle, des capteurs de cyberdéfense pour une organisation non fédérale reconnue comme étant visée par le premier arrêté ministériel, et ce, pour défendre l'entité en question contre une attaque lancée par *** un acteur étatique (voir l'étude de cas n° 2).

---

[293] CST, *Overview Note for the Minister of National Defence. Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada*, 17 juin 2019; CST, arrêté ministériel, *Communications Security Establishment Canada. Electronic Information and Information Infrastructures of Importance to the Government of Canada*, 22 juillet 2019; et CST, arrêté ministériel, *Communications Security Establishment. Designating Electronic Information and Information Infrastructure of Importance to the Government of Canada*, 25 août 2020.

[294] Ces facteurs comprennent certains éléments, notamment, à savoir si l'entité offre des services dont dépend l'intégrité d'autres secteurs ou la nature des dommages résultant d'une perturbation des services fournis par ladite entité. La liste complète de ces facteurs est présentée dans CST, Electronic Information and Information Infrastructures of Importance to the Government of Canada, CST, arrêté ministériel, 22 juillet 2019.

[295] CST, *Overview Note for the Minister of National Defence. Ministerial Order Designating Electronic Information and Information Infrastructures of Importance to the Government of Canada*, 17 juin 2019.

Étude de cas nº 2 : Recours à un nouveau pouvoir

[*** Trois paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] En 2019, le CST a détecté des efforts déployés par un état en vue de compromettre le réseau d'une entreprise canadienne[226]. L'état était connu pour ses attaques poussées contre des cibles occidentales. Le CST a indiqué que l'entreprise était une organisation qui fournissait des services à un certain nombre de clients de l'infrastructure essentielle et a officiellement désigné l'entreprise comme constituant un système d'importance pour le gouvernement, conformément à l'arrêté ministériel du ministre.

Le CST a bloqué la cyberactivité de l'état sur tous les réseaux du gouvernement et a conclu que les ministères n'avaient pas été touchés. Le CST a informé l'entreprise de la compromission et, en réponse à sa demande d'aide, a travaillé avec l'entreprise pour mettre fin à l'attaque.

Cette étude de cas représente le premier recours à ce nouveau pouvoir que le CST avait acquis à peine quelques mois plus tôt. À ce stade, le Comité est réticent à tirer des conclusions définitives, mais il note tout de même deux difficultés. En premier lieu, cet incident montre que les pouvoirs doivent être assez souples pour permettre d'intervenir en cas de nouvelle difficulté. Le CST avait d'ailleurs noté que ce type de déploiement n'était pas prévu au moment où la loi a été rédigée; le pouvoir avait plutôt pour objet de donner lieu à une collaboration proactive sur le long terme avec les organisations non fédérales, particulièrement les entreprises de télécommunications. Néanmoins, le pouvoir en question a permis au CST de réagir à une attaque sophistiquée dirigée contre une entreprise qui fournissait de précieux services à l'infrastructure essentielle, y compris au gouvernement.

En second lieu, l'incident met en évidence l'importance de la rapidité d'intervention. Il s'est écoulé du temps entre le moment où le CST a détecté les cyberactivités douteuses et le moment où il a pu aider l'entreprise à appliquer les mesures de protection, puis obtenir l'approbation ministérielle d'aider. Le présent constat n'est nullement une critique : au reste, le seul fait que le CST a été en mesure de reconnaître l'attaque constitue une preuve qu'il exerce une surveillance accrue sur les menaces pouvant cibler le Canada. En revanche, force est de constater que de telles attaques nécessitent d'intervenir « à la vitesse du cyberespace ». Un auteur de menace perfectionné peut compromettre un système, voler des données ou miner les fonctionnalités d'un système à une vitesse inquiétante. Le gouvernement doit donc continuer d'envisager des moyens pragmatiques suivant lesquels le CST pourra répondre aux nouvelles cybermenaces tout en garantissant des contrôles ministériels rigoureux et une responsabilisation acceptable.

[226] Cette étude de cas est tirée de CST, ***, séance d'information pour le CPSNR, 26 février 2021; CST, ***, 2019; CST, *Application to the Minister of National Defence for Cybersecurity Activities on Non-Federal Infrastructure* ***, 2019; et CCC, exposé devant le CPSNR, 26 février 2021.

Désignation des destinataires d'informations nominatives se rapportant à des Canadiens ou à des entreprises canadiennes

179. La Loi sur le CST stipule que le ministre peut délivrer un arrêté visant des personnes et des catégories de personnes désignées auxquelles le CST peut communiquer de l'information qui pourrait être utilisée pour identifier un Canadien ou une personne se trouvant au Canada. Dans le contexte des activités de cyberdéfense, le CST peut procéder à cette communication dans la mesure où celle-ci est nécessaire à la protection de l'information électronique et des infrastructures de l'information des organisations fédérales ou des organisations non fédérales désignées par le ministre comme étant d'importance pour le gouvernement. En définitive, le CST peut divulguer de l'information si celle-ci a été acquise, utilisée ou analysée au cours d'activités menées dans le cadre du volet du mandat du CST touchant la cybersécurité et l'assurance de l'information, ce qui comprend les communications privées interceptées durant ces activités[297].

180. Le ministre de la Défense nationale a délivré deux arrêtés visant à désigner certaines catégories de personnes destinées à recevoir des informations communiquées par le CST et se rapportant à des Canadiens ou à des personnes se trouvant au Canada : le premier en juillet 2019, abrogé puis mis à jour en août 2020. L'arrêté n'a aucune date d'expiration et désigne plusieurs personnes et catégories de personnes à qui il est possible de communiquer des informations, à condition que la communication de ces informations soit nécessaire à la protection de l'informations électronique et des infrastructures de l'information des institutions fédérales ou de celles des systèmes désignés comme étant d'importance pour le gouvernement. Les entités visées par cet arrêté sont les suivantes :

- les propriétaires ou les administrateurs de systèmes ou de réseaux informatiques employés par le gouvernement ou par toute organisation non fédérale désignée comme étant d'importance pour le gouvernement;
- les personnes ou les catégories de personnes qui travaillent sous l'autorité d'institutions fédérales exerçant un mandat de coordination de la cyberdéfense ou d'atténuation, dans la mesure où ces personnes doivent, en considération de besoins opérationnels, disposer desdites informations (p. ex. SPC, le Service canadien du renseignement de sécurité, la Gendarmerie royale du Canada);
- les personnes ou les catégories de personnes autorisées faisant partie d'entités étrangères avec lesquelles le CST a conclu des ententes, y compris les partenaires du Groupe des cinq, *** ainsi que les équipes étrangères d'intervention en cas d'incident de sécurité informatique;
- les organisations étrangères ou nationales de cybersécurité qui contribuent à la protection de l'information électronique ou des infrastructures de l'information d'importance pour le gouvernement ainsi que les entités qui participent à la recherche et au développement en matière de cybersécurité, avec lesquelles le CST a conclu des partenariats[298].

---

[297] *Loi sur le Centre de la sécurité des télécommunications*, L.C. 2019, ch. 13, art. 76, paragr. 44(1) et (2), et art. 45.
[298] CST, *Disclosure of Information Related to Canadians and Persons in Canada (Cybersecurity and Information Assurance)*, arrêté ministériel pour le CST, 22 juillet 2019; CST, *Order. Communications Security Establishment. Designating Recipients of Information Related to a Canadian or a Person in Canada Acquired, Used, or Analyzed Under the Cybersecurity and Information Assurance Aspects of the CSE Mandate*, 25 août 2020.

Politiques opérationnelles internes

181. Les politiques opérationnelles internes du CST sont aussi désignées sous l'appellation « Ensemble des politiques sur la mission ». La section Cybersécurité de l'Ensemble des politiques sur la mission énonce les principes et les exigences stratégiques qui visent à guider les membres du personnel œuvrant sous le volet de la cybersécurité et de l'assurance de l'information du mandat du CST, pour qu'ils soient en mesure d'exercer leurs activités en toute légalité. Toute l'information que le CST acquiert sous le volet de la cybersécurité et de l'assurance de l'information de son mandat sont traitées conformément à l'Ensemble des politiques sur la mission[299].

182. Plus spécifiquement, la section Cybersécurité de l'Ensemble des politiques sur la mission régit l'acquisition, l'utilisation (analyse), la conservation et la communication de l'information dans le cadre des opérations du CST. La politique se penche également sur quatre secteurs cruciaux pour la réalisation des activités de cyberdéfense :

- l'autorisation du CST (et du CCC) à mener des activités touchant au volet de la cybersécurité et de l'assurance de l'information du mandat du CST;
- les principes stratégiques centraux que le CST est tenu de suivre lorsqu'il exerce ses activités touchant le volet de la cybersécurité et de l'assurance de l'information du mandat – légalité, nécessité et raisonnabilité, protection de la vie privée ainsi que transparence et responsabilisation;
- l'information électronique et les infrastructures de l'information d'importance (également désignées sous l'appellation « systèmes d'importance »);
- les exigences en matière de responsabilisation s'appliquant au personnel du CCC appelé à travailler en soutien au mandat de cybersécurité[300].

183. La section Cybersécurité de l'Ensemble des politiques sur la mission donne plus de détails sur les divers secteurs stratégiques, les obligations juridiques, ainsi que les procédures et les processus opérationnels que le CST doit suivre dans l'exercice de ses activités de cybersécurité et d'assurance de l'information. La politique a pour objet de renforcer les mesures de protection de la vie privée, de gérer les risques opérationnels, et d'accroître la raisonnabilité et la proportionnalité des activités du CST. Selon l'Ensemble des politiques sur la mission, plusieurs mesures de contrôle peuvent s'appliquer aux activités du CST, à savoir :

---

[299] CST, « Annex III: Relevant Policy Principles and Control Measures », *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale, 26 juillet 2019; CST, Ensemble des politiques sur la mission : Cybersécurité, 5 novembre 2020; CST, *End of Authorization Report for the Minister of National Defence. Cybersecurity Authorization for Activities on Federal Infrastructures, August 29, 2019 – July 30, 2020*, sans date; et CST, *Authorization Cybersecurity Activities on Non-Federal Infrastructures*, 7 novembre 2019.

[300] CST, *Ensemble des politiques sur la mission : Cybersécurité*, 5 novembre 2020; et CST, « Annex III: Relevant Policy Principles and Control Measures », *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale, 26 juillet 2019.

- **approbations de niveau supérieur** : employées en guise de mesures de contrôle des risques, les approbations de niveau supérieur pourraient être requises pour les activités de cyberdéfense pouvant poser des risques pour le gouvernement du Canada sur les plans juridique et opérationnel, et sur le plan de la protection de la vie privée, des partenariats et de la réputation;
- **marquage et suivi de l'information** : l'information acquise par le CST ou communiquée au CST est marquée pour en indiquer l'origine ainsi que les exigences concernant son accès, son utilisation et son traitement. Une fois marquée, l'information est suivie tout au long de son cycle de vie, dans le but d'en contrôler l'accès, la conservation et l'élimination, les limites relatives à l'utilisation, et la communication. De plus, le marquage et le suivi de l'information aident le CST à remplir ses obligations relativement à l'autorisation ministérielle.

La section Cybersécurité de l'Ensemble des politiques sur la mission établit également les périodes durant lesquelles le CST peut conserver l'information; fournit un guide pour les équipes du CST chargées de la conformité pour veiller à ce que le personnel opérationnel élimine les données conformément au calendrier de conservation et d'élimination; décèle les occurrences où les renseignements concernant un Canadien doivent être supprimés; et fournit des contrôles de la diffusion et des permissions visant à limiter l'accès à l'information particulièrement sensible (p. ex. rapports de cyberdéfense ou de renseignement fondés sur des sources hautement sensibles)[301]. L'Ensemble des politiques sur la mission exige aussi que le CST obtienne le consentement d'une institution fédérale ou d'une organisation non fédérale désignée comme étant d'importance pour le gouvernement avant de déployer ses capteurs au profit de ces entités. Toutes les exigences stratégiques énoncées dans l'Ensemble des politiques sur la mission sont inscrites dans les autorisations ministérielles remises au CST.

Activités de cyberdéfense du CST

184. Relevant du CST, le CCC constitue la source centrale faisant autorité en matière de cybersécurité au Canada. Le CCC a été créé en 2018 moyennant la fusion de trois entités : la Direction générale de la sécurité des technologies du CST, le Centre canadien de réponses aux incidents cybernétiques de Sécurité publique Canada et le Centre des opérations de sécurité de Services partagés Canada. Le CCC est chargé de diriger les interventions du gouvernement en cas d'événements de cybersécurité, et de garantir la protection ainsi que la défense des biens informatiques du Canada en donnant des conseils et des avis ciblés ainsi qu'en prodiguant de l'assistance directe[302]. Dans le cadre de ce mandat élargi, le CST et le CCC dirigent les activités relevant spécifiquement de la cyberdéfense. En voici un bref énoncé :

- fournir des conseils et des avis aux ministères du gouvernement et aux partenaires non gouvernementaux;

---

[301] CST, *Ensemble des politiques sur la mission : Cybersécurité*, 5 novembre 2020; et CST, « Annex III: Relevant Policy Principles and Control Measures », *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.
[302] CCC, « Au sujet du Centre pour la cybersécurité », https://cyber.gc.ca/fr/propos-du-centre-pour-la-cybersecurite.

- employer des capteurs de cyberdéfense sur les réseaux du gouvernement, y compris la surveillance, la détection et l'intervention liées aux cyberincidents;
- employer des capteurs de cyberdéfense sur les réseaux non gouvernementaux;
- diriger des cyberopérations défensives.

Les deux premiers éléments sont de loin les plus courants. En outre, l'installation de capteurs de cyberdéfense sur les réseaux non gouvernementaux et la direction de cyberopérations défensives découlent, quant à elles, des nouveaux pouvoirs conférés au CST en 2019, lesquels n'ont pas encore été largement utilisés. Chacune des activités est décrite ci-après.

Conseils et orientations

185. Les conseils et les orientations du CST se répartissent dans trois catégories. La première relève du rôle d'autorité dirigeante. En vertu de la Politique sur la sécurité du gouvernement du Conseil du Trésor, le CST constitue le principal organisme de sécurité ainsi que l'autorité nationale en matière de sécurité des communications. À ce titre, le CST donne des directives en matière de technologies de l'information aux ministères assujettis à la politique de mise en œuvre des normes et des pratiques garantissant la protection de l'information et des données classifiées, et permettant de sécuriser ou d'authentifier l'information provenant des télécommunications. Le CST a formulé 11 de ces directives entre 2012 et 2019[303]. Ces directives doivent être suivies et mises en œuvre par les ministères concernés.

186. La deuxième porte sur les alertes et les avis ainsi que les conseils personnalisés en matière de technologie de l'information à l'intention d'organisations. Ces alertes et ces avis sont fournis aux ministères, aux fournisseurs de services essentiels et aux entités du secteur privé. Ces documents couvrent une vaste gamme de sujets, notamment les avis de vulnérabilité des systèmes de contrôle de l'infrastructure essentielle, les avertissements de vulnérabilité des navigateurs Web et la diffusion des mises à jour non classifiées de l'appareil du renseignement concernant le ciblage des réseaux du gouvernement et de l'infrastructure essentielle par des auteurs de menace persistantes avancées qui sont parrainés par des États. Les organisations à qui sont destinés les alertes et les avis peuvent utiliser l'information pour appliquer des mesures concrètes visant à défendre leurs systèmes. Entre décembre 2013 et mai 2021, le CST a publié 1 721 alertes et avis publics[304].

187. La troisième catégorie de conseil et d'orientation consiste en des rapports de cyberdéfense et des évaluations de la menace. La portée, le sujet et le niveau de classification de ces documents peuvent varier. En outre, ces rapports et ces évaluations sont rédigés à l'intention de divers auditoires du gouvernement et du public dans le but d'accroître la sensibilisation à l'égard de l'environnement des cybermenaces. La nature de ces documents est

[303] CCC, « Directives », https://cyber.gc.ca/fr/directives. La plus récente directive est CCC, Atténuation obligatoire des menaces liées à l'informatique quantique au GC, https://cyber.gc.ca/fr/orientation/attenuation-obligatoire-des-menaces-liees-linformatique-quantique-au-gc-itsb-127.
[304] CCC, *Alertes et avis*, https://cyber.gc.ca/fr/alertes-et-avis.

également variable, dans la mesure où ils peuvent se décliner sous diverses formes, notamment les évaluations stratégiques (l'évolution de l'environnement des cybermenaces, les activités de certains États) ou les rapports opérationnels (aperçu des menaces posées par certains événements de cybersécurité ou par des vulnérabilités), dont l'objet est d'assister les ministères dans la gestion des mécanismes de défense de leurs systèmes[305].

Capteurs du CST pour la cyberdéfense

188. Le CCC a créé trois types de capteurs pour la cyberdéfense. Il s'agit des capteurs réseau, des capteurs sur l'hôte et des capteurs infonuagiques. Décrits en détail plus loin, ces capteurs constituent un complément aux mécanismes commerciaux comme les logiciels antivirus ou les coupe-feux et tiennent principalement deux rôles : reconnaître les cyberactivités malveillantes dirigées contre les réseaux du gouvernement et d'organisations non fédérales désignées comme étant d'importance pour le gouvernement, et défendre ces réseaux contre les cyberattaques[306]. Là où ils sont déployés, les capteurs du CST forment une couche défensive qui surveille constamment les systèmes et les réseaux informatiques à divers niveaux, bloque les menaces connues et reconnaît les anomalies. L'information sur les anomalies est saisie dans des systèmes d'analyse sophistiqués permettant de repérer les cybercomportements malveillants qui n'étaient pas encore connus. Cette information est ensuite réintroduite dans chacun des capteurs, comme nouveaux éléments de détection de cyberactivité malveillante[307].

189. Les capteurs du CST pour la cyberdéfense emploient *** méthodes pour la reconnaissance des activités de cybermenace, notamment [*** Deux puces ont été revues pour retirer l'information préjudiciable ou privilégiée. ***] :

- **Reconnaissance de la menace :** Lorsque les menaces sont détectées dans un réseau ou dans des données que le CST obtient par l'intermédiaire de ses capteurs, une alerte est générée. En fonction de la nature de l'alerte et du type de menace, une mesure d'atténuation peut être déclenchée ou encore, ce sont les analystes du CST qui peuvent procéder à une analyse supplémentaire visant à déterminer les prochaines étapes.
- **Détection de schème :** Le CST identifie les schèmes de comportement pouvant annoncer une cyberactivité malveillante en prenant note des activités particulières (dans le réseau, sur l'hôte ou dans le nuage) qui sont contraires aux comportements attendus ou normaux. Le CST peut appliquer des mesures défensives d'atténuation en fonction des comportements types détectés[308].

---

[305] CST, *Package 4: Table of Contents*, 22 septembre 2020. Cette liste descriptive accompagnant les rapports sur les cybermenaces porte sur l'évaluation des menaces et la mise à l'épreuve des vulnérabilités pour les systèmes du gouvernement du Canada, de même que sur les mesures d'atténuation appliquées dans le cadre des mesures d'intervention.

[306] Au moment de la rédaction du présent document, les trois types de capteurs avaient été déployés dans plusieurs ministères et agences. ***

[307] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.

[308] CST, *CSE Cyber Defence Activities: For Approval*, Note de breffage au ministre de la Défense nationale, 12 juin 2017.

190. Chaque capteur permet au CST de prendre des mesures d'atténuation visant à détecter ou à contrer une cybermenace. Les mesures d'atténuation peuvent être exécutées manuellement par un analyste du CST qui applique des contrôles interactifs, ou automatiquement grâce à des mécanismes de défense dynamique. En effet, après vérification, les déclencheurs configurés réagissent à la présence de cyberactivités. Les mesures d'atténuation peuvent se traduire par le blocage des connexions malveillantes à la passerelle ou par la suppression d'un maliciel sur un ordinateur[309]. L'information permettant de détecter de nouvelles menaces peut également être relayée par les partenaires et les clients du CST, qu'ils soient gouvernementaux ou non gouvernementaux.

191. Le déploiement de capteurs de défense se déroule en deux étapes. La première consiste à se faire octroyer l'accès au réseau. Conformément aux pouvoirs conférés aux diverses organisations en vertu de la *Loi sur la gestion des finances publiques*, le CST ne peut déployer ses capteurs que s'il a obtenu le consentement éclairé de la part du propriétaire du système ou du réseau. En accordant cet accès, le propriétaire de système donne au CST la permission d'accéder au réseau et aux informations électroniques qu'il contient.

192. La seconde étape consiste à acquérir l'information. Les capteurs du CST procèdent donc à l'acquisition de données sur les cybermenaces pouvant se trouver sur le réseau ou le système en question. Comme le CST ne connaît pas d'avance la nature des menaces qui pourraient peser sur les ressources à protéger, l'éventail des données à capter doit demeurer large et doit comprendre, notamment, le contenu du trafic passant par le réseau (p. ex. les courriels) et les métadonnées de ces communications (c.-à-d. les données sur la création, la transmission et la diffusion desdites communications). Ces données peuvent contenir des communications privées ou des renseignements personnels à l'égard desquels un Canadien ou une personne se trouvant au Canada pourrait s'attendre à ce qu'ils demeurent confidentiels. Ainsi, ce type de collecte nécessite une autorisation ministérielle (notion décrite plus haut)[310].

193. Chaque capteur de cyberdéfense du CST passe par une série d'étapes de perfectionnement technologique et par un déploiement servant de preuve de validation au CST, et doit enfin obtenir une approbation aux fins de déploiement dans les réseaux du gouvernement. La figure 2 illustre le calendrier de développement des capteurs de cyberdéfense au CST. La section subséquente donne de plus amples détails sur chacun de ces capteurs. [*** Un graphique a été revu pour retirer l'information préjudiciable ou privilégiée. ***]

---

[309] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.
[310] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.

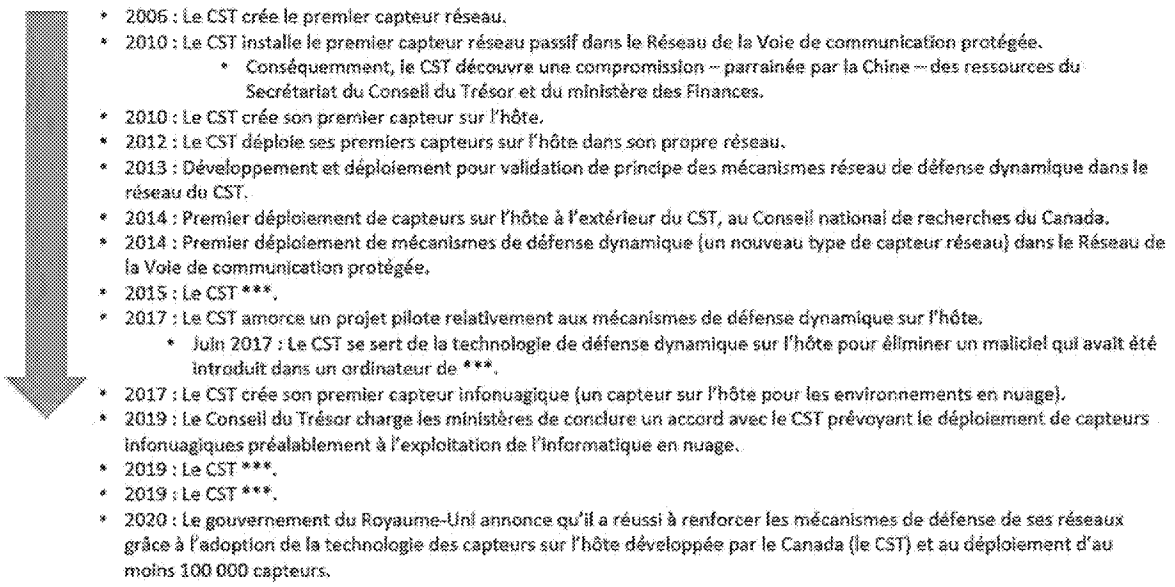


Figure 2 : Calendrier de développement des capteurs de cyberdéfense[311]

Capteurs réseau

194. Le développement des capteurs de cyberdéfense du CST a débuté en 2006 suivant la création des capteurs réseau ***. À cette époque, le CST employait ses capteurs en vertu d'une autorisation ministérielle visant plusieurs ministères. Ces capteurs devaient principalement surveiller les activités exercées par une poignée d'auteurs de cybermenace provenant surtout de la Russie et de la Chine[312]. En 2010, le CST a déployé ces capteurs *** dans le Réseau de la Voie de communication protégée, lequel reliait des dizaines d'organisations du gouvernement les unes aux autres. Quasi immédiatement, le CST a découvert la compromission des réseaux du SCT et du ministère des Finances par des auteurs malveillants parrainés par la Chine (voir l'étude de cas n° 1). C'est ainsi qu'en 2014, SPC a approuvé le déploiement de mesures de défense dynamique *** sur son Réseau de la Voie de communication protégée[313]. Cette réussite a permis au CST de commencer à appliquer des mesures d'atténuation automatisées (défense dynamique) conçues pour réagir aux importantes attaques dirigées contre les réseaux du gouvernement, y compris l'attaque de 2014 de la Chine sur le réseau du Conseil national de

---

[311] CCC, *Cyber Defence Activities*, présentation et commentaires pour le CPSNR, 2 octobre 2020; CST, *HBS [Host-Based Sensor] Deployment Priorities: Overview*, présentation, janvier 2020; CST, *TOC – Response Package 11– CSE Response to RFI 2 – 6. B*, courriel acheminé au Secrétariat du CPSNR, 15 janvier 2021; et R.-U. National Cyber Security Centre, « Introducing Host-Based Capability », sans date, https://www.ncsc.gov.uk/blog-post/introducing-host-based-capability-hbc.

[312] C'est en 2004 que le CST a commencé à demander des autorisations ministérielles permettant, pour l'occasion, de procéder à des tests spécialement conçus pour la sécurité réseau et à la surveillance réseau pour chacun des ministères demandeurs. Ces demandes faisaient suite à des compromissions et des tentatives de compromissions commises par la Chine (MDN en 2003) et la Russie (Affaires mondiales Canada en 2004). CST, *Protection of DND Computer Systems and Networks: Request for Ministerial Authorization*, note de breffage au ministre de la Défense nationale, 19 janvier 2004; et CST, *Protection of Government of Canada Computer Systems and Networks. Foreign Affairs Canada: Request for Ministerial Authorization*, note de breffage au ministre de la Défense nationale, 16 juin 2005.

[313] CCC, *Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation, 2 octobre 2020.

recherches du Canada et ses partenaires ministériels, ainsi que la vaste attaque par maliciels qui a également eu lieu en 2014 (voir les études de cas nos 3 et 4).

195. Le déploiement de mesures de défense dynamique *** par le CST s'est ensuite élargi lorsque SPC a remplacé son Réseau de la Voie de communication protégée par le Service Internet d'entreprise appelé à servir de principale passerelle d'accès à Internet pour le gouvernement. En mai 2021, *** institutions fédérales comptaient parmi les abonnés actifs du Service Internet d'entreprise de SPC et pouvaient conséquemment jouir de la protection offerte par les capteurs[314]. Le CST a également conclu des accords bilatéraux distincts visant à fournir des mesures de défense dynamique à plusieurs organisations ***[315].

196. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] Des mesures de défense dynamique sont disposées aux points d'entrée d'un réseau (couramment appelés « passerelles », ces points d'entrée permettent de relier le réseau à Internet) pour offrir un maximum de visibilité sur le trafic numérique et sur l'information qui entre et qui sort des réseaux des ministères. Ainsi, le CST peut reconnaître les menaces qui ciblent l'information et les réseaux des ministères et déterminer lorsque les systèmes ont déjà été compromis. Le CST ne décèle pas toutes les menaces : les cyberacteurs malveillants peuvent contourner le blocage du CST. Lorsque des menaces connues sont repérées, les mesures de défense dynamique du CST les bloquent automatiquement au périmètre du réseau. Tel qu'il était indiqué précédemment, les données suspectes sont réacheminées au CST, où elles sont soumises à une analyse sophistiquée visant à relever les comportements suspects ou inhabituels (anomalies)[316]. Une fois que de nouvelles menaces sont découvertes, les mesures de défense dynamique du CST sont aiguillées pour repérer et bloquer ces menaces à l'avenir. Ce système de mesures de défense dynamique est un élément central de la protection des réseaux du gouvernement, puisque l'information obtenue d'un ministère est appliquée proactivement pour défendre les autres ministères de façon continue afin de renforcer les cyberdéfenses du gouvernement[317].

197. L'une des particularités des capteurs du CST est qu'ils peuvent se renforcer mutuellement. [*** Deux phrases ont été revues pour retirer l'information préjudiciable ou privilégiée. Les phrases indiquaient que l'information recueillie par un capteur est analysée par le CST pour détecter les activités malveillantes et que les indicateurs de compromission connexes sont intégrés aux autres capteurs, qui, à leur tour, peuvent détecter les mêmes

---

[314] Voir le paragraphe 141.
[315] CST, *RFI-2 Item #3 – Provision of Cybersecurity Activities to Federal Institutions*, 23 décembre 2020.
[316] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020; et CST, *Cyber Defence Activities. A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation, 2 octobre 2020.
[317] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020; et CST, *Cyber Defence Activities. A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation, 2 octobre 2020.

activités malveillantes et déclencher les mesures d'atténuation dans les autres organisations. ***][318] Le rôle des capteurs sur l'hôte est abordé ci-après.

[318] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.

Étude de cas n° 3 : Mesures de défense et vulnérabilité HEARTBLEED

[*** Cinq paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] Le 8 avril 2014, les États-Unis ont révélé publiquement une vulnérabilité décelée dans des outils de chiffrement de source ouverte qui étaient employés pour sécuriser les communications circulant dans les réseaux informatiques et dans Internet. La vulnérabilité, appelée HEARTBLEED, permettait de soutirer de l'information confidentielle, notamment les certificats de sécurisation et de chiffrement des communications Internet, les mots de passe et les renseignements personnels[319]. Le CST et SPC ont examiné l'information et ont conseillé aux administrateurs des réseaux du gouvernement d'installer les correctifs permettant de neutraliser la vulnérabilité ou encore de mettre leurs systèmes hors service jusqu'à ce qu'ils soient en mesure d'installer lesdits correctifs.

Le 9 avril, l'Agence du revenu du Canada (ARC) a interrompu deux services fiscaux en ligne. Le 10 avril, le dirigeant principal de l'information du Canada a diffusé une directive dans l'ensemble du gouvernement voulant que les serveurs vulnérables soient mis hors ligne jusqu'à ce que les correctifs soient installés. Le 11 avril, SPC a approuvé l'installation, par le CST, de mesures de défense dynamique sur le Réseau de la Voie de communication protégée. En un mois, ces mesures de défense avaient bloqué de nombreuses occurrences de trafic malveillant HEARTBLEED, protégeant ainsi SPC, mais aussi les organisations gouvernementales qui s'étaient abonnées au service de passerelle sécurisée de SPC. Le CST a également transmis, aux fournisseurs de services de télécommunication, de l'information sur les façons de bloquer les attaques par HEARTBLEED.

Le Secrétariat du Conseil du Trésor du Canada a décrit cet incident comme étant l'un des plus graves à avoir touché le gouvernement. À ce moment, le gouvernement n'était pas en mesure de défendre convenablement ses réseaux contre les cyberattaques. Bien qu'il ait déployé des outils défensifs dans son propre réseau et dans ceux de SPC, d'Affaires mondiales Canada et du MDN, le CST n'avait pas encore déployé de mesures de défense dynamique et n'en était encore qu'aux premiers stades du développement de ses systèmes d'automatisation internes. Conséquemment, bon nombre d'auteurs malveillants ont utilisé cette vulnérabilité pour extraire de l'information des réseaux gouvernementaux. En tout, 12 ministères ont été la cible d'activités d'exploitation et d'exfiltration de données, y compris le vol d'au moins 900 numéros d'assurance sociale qui se trouvaient sur les serveurs de l'ARC et qui appartenaient à des contribuables canadiens.

Après l'attaque, le gouvernement a dressé une liste de difficultés qui, à ce jour, sont encore d'intérêt pour le Comité. Au nombre de ces difficultés, comptons le besoin d'établir une meilleure gouvernance en matière de gestion des incidents; d'améliorer les processus de cybersécurité dans l'ensemble du gouvernement (p. ex. la mise à jour des directives visant les vulnérabilités et la gestion des correctifs, les comptes à accès privilégié et la tenue d'un répertoire précis et automatisé des systèmes essentiels du gouvernement); et de renforcer le périmètre du réseau du gouvernement.

---

[319] Ce résumé se fonde sur les documents suivants : SCT, *HEARTBLEED: Government of Canada Lessons Learned and Management Response*, 24 septembre 2014; CST, *After Action Report HEARTBLEED*, mai 2014; CST, *Op HEARTBLEED: Timeline of events*, septembre 2015; et CCC, exposés devant le CPSNR, 27 novembre 2020 et 19 février 2021.

Plusieurs de ces problèmes ont été résolus dans le sillon des directives du Conseil du Trésor, grâce à des protocoles plus ciblés de gestion des incidents et suivant la création de SPC, ce qui a permis l'installation rapide et essentielle des correctifs de vulnérabilité. Toutefois — comme on le verra plus loin — certaines difficultés continuent de se manifester, notamment le fait que bon nombre de ministères se trouvent toujours en marge du périmètre sécurisé et ne jouissent aucunement de la protection offerte par les capteurs réseau du CST. Par conséquent, de l'information précieuse s'en trouve vulnérabilisée vis-à-vis des auteurs malveillants qui disposent de moyens sophistiqués, et crée des voies d'entrée potentielle vers les ministères se trouvant à l'intérieur du périmètre sécurisé. De plus, les directives du Conseil du Trésor, les configurations en matière de sécurité de SPC et les conseils du CST ne sont pas appliqués par tous. On en veut pour preuve ce cas où des lacunes sur le plan de la conformité ont entraîné des pertes de données qui auraient pu être évitées (voir l'étude de cas nº 6).

Capteurs sur l'hôte

198. Le CST a commencé le développement des capteurs sur l'hôte en 2010. En effet, le CST avait reconnu que les défenses périmétriques ne constituaient que la moitié de la solution et qu'un cadre de cyberdéfense avancée nécessiterait un outil capable de détecter la présence d'activités malveillantes hautement développées au niveau des serveurs et des postes de travail[320]. En 2012, le CST a déployé ses premiers capteurs sur l'hôte dans son propre réseau, en guise de validation de principe. En 2014, le Centre a installé ses premiers capteurs sur l'hôte à l'extérieur du CST, soit du côté du Conseil national de recherches du Canada et de ses partenaires du portefeuille de la science, à la suite d'une compromission des systèmes de l'organisme par la Chine (voir l'étude de cas nº 4). À la fin de 2014, le CST avait déployé ses capteurs dans 12 ministères[321]. En 2015, le CST a établi un ordre de priorités relativement au déploiement des capteurs sur l'hôte dans les réseaux d'autres ministères du gouvernement, en se fondant sur certains facteurs comme la probabilité que les ministères soient ciblés par des États étrangers et les cas où le déploiement permettrait de combler des lacunes en matière de surveillance réseau[322]. À la fin de 2020, le CST avait déployé des capteurs sur l'hôte dans *** ministères. En tout, plus de 500 000 capteurs sur l'hôte ont été installés[323]. À très court terme, le CST se propose de déployer ses capteurs dans *** ministères additionnels et dans *** autres institutions fédérales, dans le cadre d'efforts visant à étendre la couverture sur l'hôte dans les ministères. De fait, selon les prévisions du CST en matière de mobilisation des institutions fédérales, les capteurs sur l'hôte seront déployés dans *** organisations au total. L'échéancier de ces travaux variera d'un ministère à un autre, mais il sera toujours question d'établir l'ordre de priorité en fonction du degré de sensibilité de l'information que ces ministères traitent et

---

[320] Scott Jones, remarques présentées à Countermeasure 2020, notes d'allocution, fournies au Secrétariat du CPSNR, novembre 2020.
[321] Voir l'étude de cas nº 4. Voir également CST, *HBS Deployment Priorities: Overview*, présentation, janvier 2020. [*** La liste des ministères a été supprimée pour retirer l'information préjudiciable ou privilégiée. ***]
[322] CST, *HBS Deployment Priorities: Overview*, présentation, janvier 2020.
[323] CST, *HBS Deployment Priorities: Overview*, présentation, janvier 2020; CCC, *Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation et commentaires pour le CPSNR, 2 octobre 2020; et Scott Jones, remarques présentées à Countermeasure 2020, notes d'allocution, fournies au Secrétariat du CPSNR, novembre 2020.

conservent, de la posture de sécurité qu'ils affichent et de leurs besoins de combler des écarts permanents sur le plan de la surveillance réseau[324].

199. Les capteurs sur l'hôte sont déployés sur les ordinateurs, les postes de travail et les serveurs, que l'on désigne collectivement comme étant des dispositifs de destination. Ces déploiements permettent au CST d'acquérir (ou de recueillir) de l'information, puis de mettre en place des mesures d'atténuation visant à contrer les cybermenaces[325]. *** les mesures d'atténuation peuvent être automatisées avec les capteurs sur l'hôte, ce qui permet d'instaurer un mode de défense dynamique en temps réel sur chacun des dispositifs informatiques. [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases expliquaient l'installation des capteurs. ***] Les capteurs sur l'hôte assurent les fonctions suivantes :

- recueillir de l'information relative à l'hôte, laquelle est envoyée au CST par l'intermédiaire d'un lien Internet chiffré;
- analyser et traiter l'information recueillie pour détecter les activités suspectes ou anormales qui auraient pu avoir lieu dans le dispositif hôte;
- signaler les anomalies, les compromissions et les vulnérabilités touchant les ministères — fort de cette information, le CST est en mesure de fournir des recommandations relativement aux mesures d'atténuation (p. ex. application d'un correctif ou mise à jour des dispositifs informatiques au moyen de l'installation de nouveaux logiciels, de la réinitialisation de mots de passe ou du retrait d'une machine du réseau);
- supprimer les maliciels se trouvant sur un hôte : soit manuellement (par un analyste du CST), soit automatiquement ***;
- *** bloquer ou neutraliser un maliciel;
- ***

200. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] Les capteurs sur l'hôte recueillent plusieurs types d'information. Comme dans le cas des capteurs réseau, il peut arriver que de l'information recueillie soit liée à un Canadien ou à une personne se trouvant au Canada, lesquels seraient en droit de s'attendre au respect de leur vie privée. Par conséquent, les capteurs sur l'hôte sont exploités sous autorisation ministérielle[326].

---

[324] CST, *HBS Deployment Priorities: Overview*, présentation, janvier 2020; CCC, *Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation et commentaires pour le CPSNR, 2 octobre 2020; CST, *TOC - Response Package 11- CST Response to RFI 2 - 6. B*, 15 janvier 2021; CST, *HBS Deployment Priorities*, 22 octobre 2020; et CST, *RFI-4 Item #5 – Follow-up questions on prioritization of HBS deployments*, 11 juin 2021.

[325] CSE, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.

[326] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020.

Étude de cas nº 4 : Besoin d'accroître la protection des dispositifs de destination

[*** Quatre paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] Le 18 juin 2014, le CST a découvert une compromission du réseau du Conseil national de recherches du Canada (CNRC) commise par un auteur malveillant parrainé par la Chine[327]. On croit que l'auteur malveillant chinois avait été actif depuis *** et qu'il cherchait à mettre la main sur de l'information portant sur les relations et le commerce étrangers, la science et les technologies, l'énergie et les ressources naturelles, ainsi que les questions liées à l'environnement et aux changements climatiques.

Le CST a établi que la Chine avait obtenu l'accès au réseau du CNRC en envoyant des courriels de harponnage à des comptes de courrier électronique du CNRC, puis en mettant à profit son accès pour voler plus de 40 000 fichiers. Les fichiers volés contenaient des éléments de propriété intellectuelle, de l'information sur la recherche de pointe et des renseignements confidentiels d'entreprises partenaires du CNRC. La Chine a également tiré parti de son accès au réseau du CNRC pour infiltrer plusieurs organisations gouvernementales.

Au moment de l'attaque, le réseau du CNRC ne faisait pas encore partie du Réseau de la Voie de communication protégée de SPC. Ainsi, ni SPC ni le CST ne pouvaient recourir à leurs capteurs pour tenter de surveiller les activités de la Chine sur le réseau du CNRC. Pour dresser un portrait des activités qui pouvaient avoir lieu, le CST a déployé des capteurs sur l'hôte pour la première fois à l'extérieur du CST. Par la même occasion, le CST a mis à jour les mesures de défense dynamique, qu'il avait récemment déployées dans le Réseau de la Voie de communication protégée (en avril, en réaction aux attaques HEARTBLEED) dans le but de bloquer les attaques de la Chine sur les réseaux d'autres ministères. SPC a également bloqué la connexion entre le réseau du CNRC et celui des autres organisations fédérales.

Dans le cas de cet incident, l'intervention du gouvernement a été manuelle, vaste, coûteuse et longue (plusieurs mois), et a fini par s'étendre à plusieurs ministères. Le CNRC a informé ses clients que leurs données ont peut-être couru un risque. Le coût des mesures d'atténuation des dommages causés par cette attaque s'est élevé à environ 100 millions de dollars et a nécessité plusieurs années d'efforts de la part du CNRC, de SPC et du CST pour réaménager le réseau du CNRC de sorte qu'il dispose de mécanismes de protection qui soient intégrés dès l'étape de la conception du réseau.

Pendant cet incident, plusieurs problèmes ont été révélés relativement à la capacité du gouvernement de protéger ses réseaux contre les cyberattaques. Qui plus est, l'incident a mis en évidence la nécessité d'accroître le niveau de protection du périmètre du réseau du gouvernement; de réduire le nombre des points d'accès à Internet que les ministères utilisent en les regroupant; et d'accroître la protection aux points de destination (grâce aux capteurs sur l'hôte) à l'extérieur du CST. L'expérience a également rappelé certaines leçons tirées de l'incident impliquant HEARTBLEED relativement au besoin de perfectionner les modalités de gouvernance quant à la gestion des incidents et d'améliorer les processus liés à la cybersécurité dans l'ensemble du gouvernement (p. ex. installation des correctifs sur les applications vulnérables et accroissement des contrôles à l'égard des accès privilégiés).

[327] Cette étude de cas se fonde sur les documents suivants : CST, *** présentation et remarques afférentes devant le CPSNR, 19 février 2021; et SCT, *NRC Incident: Government of Canada Lessons Learned Report*, juillet 2015.

Étude de cas n° 5 : Attaque contre un réseau du ministère de la Défense nationale

[*** Trois paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] En 2017, le CST a découvert qu'un acteur étatique avait compromis un réseau du ministère de la Défense nationale (MDN). L'acteur a volé une quantité importante de données et a profité de sa présence pour infecter d'autres réseaux. Le MDN a isolé le réseau, le CST a mis à jour ses mesures de défense dynamique pour protéger les autres ministères, et les deux organisations ont coopéré avec Services partagés Canada pour supprimer la présence de l'acteur[328].

Cette étude de cas met en évidence des problèmes importants. Le réseau comportait plusieurs applications ainsi que des systèmes d'exploitation patrimoniaux qui n'étaient ni corrigés ni pris en charge, ce qui a constitué un vecteur d'entrée pour l'acteur. De plus, comme il n'était pas relié au Service Internet d'entreprise de SPC, le réseau n'était pas protégé par les mesures de défense du CST. Qui plus est, le réseau était relié à un certain nombre d'autres ministères, ce qui aurait en soi posé un risque de compromission pour l'ensemble de l'infrastructure gouvernementale si l'acteur avait été en mesure de se rendre jusqu'aux réseaux de ces organisations. En revanche, le CST a pu déployer ses mesures de défense et appliquer sur-le-champ des mesures d'atténuation en considération d'une autorisation ministérielle qui visait déjà les activités de cyberdéfense du MDN[329]. En définitive, cette étude de cas illustre parfaitement les dangers liés à la conservation de systèmes patrimoniaux qui n'ont pas été corrigés et qui ont accès à Internet par l'intermédiaire d'une liaison qui ne passe pas par le Service Internet d'entreprise de SPC. Au reste, elle met en évidence l'importance de disposer des autorisations appropriées permettant le déploiement rapide des cyberdéfenses requises.

---

[328] CST, *Executive Summary*, ***, 2017; et CST, ***, 2018. Voir également MDN, ***, 2017; MDN, ***, 2017; MDN, ***, 2018; MDN, ***, 2018; et MDN, ***, sans date.

[329] CST, *Cyber Defence Activities," 2017–2018*, autorisation ministérielle pour le CST, 22 juin 2017.

Capteurs infonuagiques

201. Tel qu'il était indiqué précédemment, le gouvernement s'en remet de plus en plus aux environnements infonuagiques, comme le prescrivent les plans de modernisation des systèmes et de l'infrastructure des technologies de l'information. En 2017, le SCT a émis l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage, suivant laquelle les ministères visés étaient tenus de se conformer à des mesures de sécurité avant même de recevoir une approbation permettant d'exploiter un système en nuage. En 2019, le SCT a obligé les ministères à adopter les capteurs infonuagiques dans le cadre de la mise en place de leur environnement infonuagique, alors que le CST et SPC commençaient à mobiliser les ministères pour ce qui a trait au déploiement des capteurs infonuagiques[330]. En outre, on a dû accroître le rythme de déploiement des capteurs infonuagiques en raison de la pandémie de COVID-19. En mai 2020, le SCT a établi des consignes de service pour Microsoft Office 365, alors que SPC a accéléré, en collaboration avec le SCT et le CST, la transition des ministères vers les services de courrier électronique et de collaboration infonuagiques, et ce, dans le but de répondre à l'explosion de la demande en télétravail. De fait, le CST et SPC ont collaboré de sorte à installer rapidement des capteurs infonuagiques dans les ressources de *** organisations. Conséquemment, le CST est désormais en mesure de fournir des services de surveillance à tous les ministères qui ont converti leur service de courrier électronique aux environnements infonuagiques identifiés par le service de courtage de SPC[331].

202. Le déploiement des capteurs infonuagiques a pour objet de protéger les activités des institutions fédérales qui sont menées dans les environnements infonuagiques et d'intensifier les services de protection fournis par les capteurs réseau et les capteurs sur l'hôte[332]. [*** Cinq phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Les phrases décrivaient des opérations du CST. ***]

- ***
- ***
- ***

Semblablement aux capteurs réseau et aux capteurs sur l'hôte, les capteurs infonuagiques pourraient recueillir de l'information liée à un Canadien ou à une personne se trouvant au Canada, lesquels seraient en droit de s'attendre au respect de leur vie privée. Conséquemment, les déploiements de capteurs infonuagiques sont réalisés en vertu d'une autorisation ministérielle.

---

[330] SCT, Remarques en cours de comparutions devant le CPSNR, 27 novembre 2020; CST, *TOC - Response Package 11- CSE Response to RFI 2 - 6. B*, 15 janvier 2021. Voir également les paragraphes 114 à 117 décrivant la Stratégie d'adoption de l'informatique en nuage du SCT et les exigences de sécurité énoncées dans l'Orientation sur l'utilisation sécurisée des services commerciaux d'informatique en nuage du SCT; et les Mesures de sécurité du nuage au gouvernement du Canada à https://github.com/canada-ca/cloud-guardrails.

[331] CST, *TOC - Response Package 11- CSE Response to RFI 2 - 6.B*, 15 janvier 2021.

[332] CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale (autorisation obtenue), 26 juin 2020; et CST, *Cyber Defence Activities: A Brief to the National Security and Intelligence Committee of Parliamentarians (NSICOP)*, présentation, 2 octobre 2020.

Étude de cas n° 6 : Un état attaque une société d'État et des systèmes du gouvernement

[*** Cinq paragraphes ont été revus pour retirer l'information préjudiciable ou privilégiée. ***] En 2020, le CST a découvert qu'un état avait compromis le réseau d'une société d'État. L'état a profité de sa présence sur le réseau de la société pour compromettre plusieurs ministères et en balayer de nombreux autres pour trouver leurs vulnérabilités. De plus, il y a tout lieu de croire que l'état a ciblé d'autres sociétés d'État. Le CST et SPC ont bloqué les liens entre la société d'État et le reste du gouvernement, et ont déterminé que l'état avait accédé à des quantités considérables d'information. L'attaque a été atténuée. Plus tard, le CST a découvert que l'état avait compromis un ministère et avait tenté d'en compromettre d'autres. Ces attaques ont également été atténuées[333].

Cette étude de cas met en évidence deux problèmes. D'abord, les capteurs de cyberdéfense sont efficaces, mais ils ne peuvent pas fonctionner s'ils ne sont pas déployés. La société d'État n'est pas assujettie aux directives du Conseil du Trésor, elle n'a pas utilisé le Service Internet d'entreprise de SPC et n'a pas encore mis en application les recommandations du CST à cet effet. De plus, il n'est pas suffisant qu'un ministère soit assujetti aux directives du Conseil du Trésor et de SPC; encore faut-il qu'il les suive. Trois mois avant la compromission par l'état, SPC avait décidé d'interrompre le service à faible authentification (un seul facteur) d'un ministère, mais cette décision a été infirmée par la haute direction du ministère, quoiqu'une solution renforcée eût été disponible dans les deux semaines. Il s'agit là d'un facteur clé de la cyberattaque.

[333] Ce résumé se fonde sur les documents suivants : CST, ***, 2020; CST, ***, 2021; CST, ***, 2020; SPC, ***, 2020; et CST, exposé devant le CPSNR, ***, 2020.

Cyberopérations défensives

203. Les cyberopérations défensives constituent l'un des nouveaux aspects du mandat en cinq volets du CST. Les opérations ont pour objet de protéger les informations électroniques et l'infrastructure des institutions fédérales ainsi que des organisations non fédérales désignées comme étant d'importance pour le gouvernement. À ce jour, le CST a reçu deux autorisations ministérielles d'une année chacune lui permettant de mener ces opérations, ***[334]. Concrètement, les opérations n'ont été menées ni dans un cas ni dans l'autre : au cours de la première année, les activités de cyberdéfense sont parvenues à atténuer les menaces, parant ainsi à la nécessité d'une opération distincte; au cours de la seconde année, les opérations planifiées ne sont pas parvenues au stade opérationnel[335]. En conséquence, le Comité se contentera de fournir une explication pour ce qui a trait à ces opérations et se propose de revenir sur le sujet ultérieurement[336].

204. Les cyberopérations défensives nécessitent une autorisation ministérielle. Sans une telle autorisation, les cyberopérations défensives risqueraient de contrevenir à une, voire à plusieurs lois fédérales (p. ex. le *Code criminel*). En effet, ces activités pourraient se traduire par des comportements illicites, la falsification de matériel ou d'information, le trafiquage de matériel informatique ou de logiciels sans en avoir obtenu la permission des responsables du système ou l'interaction avec des auteurs malveillants au moment où ceux-ci commettent leur forfait. Les opérations peuvent être employées dans trois situations :

- lorsqu'une cybermenace est si sophistiquée que ni les mécanismes de défense vendus dans le marché ni les capteurs classifiés du CST ne seraient suffisants pour la contrer;
- lorsqu'une compromission a atteint un stade d'avancement tel que les capteurs déjà déployés ne parviennent plus à en atténuer les effets;
- lorsqu'une compromission est d'une portée et d'une ampleur telles et qu'elle touche un si grand nombre d'institutions fédérales et d'entités non fédérales désignées comme étant d'importance pour le gouvernement, que le déploiement de capteurs ne pourrait pas être effectué à temps pour atténuer la menace[337].

205. La Loi sur le CST exige que les cyberopérations défensives soient menées dans certaines parties hors Canada de l'infrastructure mondiale de l'information, ne soient pas dirigées sur des Canadiens ou sur les personnes se trouvant au Canada, et n'enfreignent pas

---

[334] *** CST, *** *Defensive Cyber Operations*, autorisation pour des cyberopérations défensives du CST, 25 août 2020.

[335] [Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Elles décrivaient des opérations du CST. ***] CST, *** *Defensive Cyber Operations. September 6, 2019 – August 25, 2020, End of Defensive Cyber Operations authorization report for the Minister of National Defence*, sans date; et CST, *DCO MA Information Package for NSICOP*, courriel envoyé au Secrétariat du CPSNR, 14 juin 2021.

[336] Ce résumé se fonde sur les documents suivants : CST, *** *Defensive Cyber Operations : (For Approval)*, demande de la chef du CST auprès du ministre de la Défense nationale visant à obtenir une autorisation en vertu du paragraphe 29(1) de la Loi sur le CST, 4 septembre 2019; et CST, séance d'information pour le Secrétariat du CPSNR, 28 mai 2021.

[337] CST, *** *Defensive Cyber Operations: (For Approval)*, demande de la chef du CST auprès du ministre de la Défense nationale visant à obtenir une autorisation en vertu du paragraphe 29(1) de la Loi sur le CST, 4 septembre 2019.

les dispositions de la *Charte canadienne des droits et libertés*. Ces opérations nécessiteraient *** en vue d'installer, d'entretenir, de copier, de distribuer, de chercher, de modifier, de perturber, de supprimer ou d'intercepter quoi que ce soit ou encore d'interagir avec des personnes dans le but de réaliser les objectifs en matière de protection des réseaux du gouvernement et des réseaux appartenant aux entités désignées comme étant d'importance pour le gouvernement. Concrètement, le CST peut :

- ***
- ***
- ***
- ***
- ***

206. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. Le paragraphe décrivait des techniques du CST. ***] En vertu de l'actuel régime des autorisations ministérielles, les cyberopérations défensives ont pour objet d'atteindre certains objectifs, mais n'ont pas pour but de recueillir des informations.

- ***
- ***
- ***
- ***

Résultats

207. Le CST mesure la réussite et la valeur de son programme de cyberdéfense en établissant la mesure dans laquelle son programme de capteurs parvient à limiter ou à prévenir les dommages pouvant être causés aux informations électroniques et aux infrastructures des institutions fédérales ou à celles des organisations non fédérales désignées comme étant d'importance pour le gouvernement. À cet effet, des données sont fournies annuellement au ministre de la Défense nationale dans les demandes d'autorisations ministérielles et dans les rapports ultérieurs. Un aperçu de ces données est fourni dans le Tableau 2.

Année	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020
Capteurs sur l'hôte déployés (ministères)	161 012 (***)	313 781 (***)	345 160 (***)	404 891 (***)	583 809 (***)
Capteurs réseau déployés (ministères) [336]	Les données complètes n'étaient pas disponibles durant cette période[335].				*** (***)

[335] [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Elles indiquaient le nombre de ministères protégés par les cyberdéfenses du CST. ***]
[336] [*** Deux phrases ont été supprimées pour retirer l'information préjudiciable ou privilégiée. Elles indiquaient le nombre de ministères protégés par les cyberdéfenses du CST. ***]

Capteurs infonuagiques déployés (ministères)	S.O.	S.O.	S.O.	*** (***)	*** (***)
Trafic malveillant bloqué (quotidiennement)	282 millions	474 millions	693 millions	1,6 milliard	1,3 milliard
Compromissions (menaces persistantes avancées)	*** (***)	*** (***)	*** (***)	*** (***)	*** (***)
Compromissions avec exfiltration de données	***	***	***	***	***
Rapports de cyberdéfense	961	1 110	2 070	1 193	4 379

Sources : Données tirées des documents suivants issus du CST, *Ministerial Authorization Year End Report: 2015–2016*, sans date; CST, *Ministerial Authorization Year End Report: 2018–2019*, sans date; CST, *Interim Ministerial Authorization Year End Report: May 2019 – October 2019*, sans date; CST, *End of Authorization Report for the Minister of National Defence – Cybersecurity Authorization for Activities on Federal Infrastructures: August 29, 2019–July 30, 2020*, sans date; CST, *HBS Deployment Priorities*, 22 octobre 2020; CST, *CSE Cyber Defence Activities*, note de breffage au ministre de la Défense nationale, 12 juin 2017; CST, *Cyber Defence Activities*, note de breffage au ministre de la Défense nationale, 30 mai 2016; CST, *CSE Cyber Defence Activities*, note de breffage au ministre de la Défense nationale, 11 juin 2018; et CST, *Activities on Federal Infrastructures*, demande d'une autorisation ministérielle de cybersécurité auprès du ministre de la Défense nationale, 26 juillet 2019.

Tableau 2 : Capteurs de cyberdéfense : mesure des résultats

208. Les capteurs de cyberdéfense du CST couvrent une part importante des réseaux du gouvernement. En date du 10 novembre 2020, le CST avait fourni certains, voire tous les types de capteurs de cyberdéfense à *** institutions fédérales, dont certaines sont membres du Service Internet d'entreprise de SPC, alors que d'autres, notamment plusieurs organismes ou sociétés d'État non assujettis aux directives du Conseil du Trésor[340], ont plutôt conclu des accords bilatéraux. Par conséquent, [traduction] « au nombre des réseaux étatiques mondiaux », ceux du gouvernement canadien ont l'avantage de miser sur les mesures de cybersécurité les plus avancées[341].

209. Néanmoins, plusieurs organisations gouvernementales ne tirent pas avantage des mesures de protection déployées par le CST, puisqu'elles n'y sont pas tenues. Le nombre total d'organisations fédérales est de 169. De ce nombre, on compte divers types d'organisations allant des ministères les plus connus (p. ex. Affaires mondiales Canada) aux agences comme le Service canadien du renseignement de sécurité ou le CST, en passant par les entités de services (p. ex. l'Agence des services frontaliers du Canada), les sociétés d'État (p. ex. Exportation et développement Canada) et les organismes autonomes (notamment le

[340] [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée. Elle énumérait les sociétés d'État protégées par le CCC. ***] CST, *RFI-2 Item #3 – Provision of Cybersecurity Activities to Federal Institutions*, 23 décembre 2020.

[341] CST, *Cybersecurity Authorization for Activities on Federal Infrastructures. August 29, 2019 – July 30, 2020*, rapport d'échéance d'autorisation à l'intention du ministre de la Défense nationale, sans date.

Commissariat à l'information du Canada et le Commissariat à la protection de la vie privée du Canada). Certaines organisations, dont le Secrétariat du présent Comité, reçoivent leurs services de technologie de l'information par l'intermédiaire d'une organisation protégée par SPC et le CCC. Certaines autres doivent plutôt recourir aux technologies de l'information et aux accès Internet fournis par des entreprises du secteur privé. Cette façon de procéder se justifie pour diverses raisons, notamment le souci d'indépendance vis-à-vis du gouvernement et le coût du service. En revanche, elle laisse bon nombre d'organisations dans un état de vulnérabilité inquiétant qui les expose aux pertes de données ou qui pourrait constituer le vecteur caché d'une intrusion dans les systèmes protégés du gouvernement, et ce, par l'entremise des liaisons électroniques qui sont maintenues entre les ministères fédéraux, ce qui pose un risque considérable pour les données du gouvernement. Le Comité aborde ces enjeux dans son évaluation.

210. Aux fins des rapports qu'il prépare à l'intention du ministre de la Défense nationale, le CST fait le suivi du nombre d'occasions où il a utilisé, conservé ou divulgué des communications privées ou des communications protégées par le secret professionnel des avocats qui auraient été incidemment recueillies pendant les activités permises par voie d'autorisation ministérielle. Or, la façon dont le CST fait le décompte de ces occurrences a considérablement changé au fil des ans. Loin de constituer une simple question de méthodologie, ces changements mettent plutôt en évidence des éléments importants concernant le risque qui pèse sur l'attente raisonnable des Canadiens à l'égard de la protection de leurs renseignements personnels pendant le déroulement des activités de cyberdéfense du CCC.

211. Avant 2018, le CST surveillait et enregistrait automatiquement la collecte de courriels dont au moins une des parties était privée et se trouvait au Canada. En conséquence, le CST devait faire rapport au ministre relativement à la conservation de centaines de milliers de communications[342]. En mars 2015, le commissaire du CST a réalisé un examen combiné des activités de cyberdéfense que le CST avait menées au titre d'autorisations ministérielles délivrées entre 2009 et 2012. En l'occurrence, on a découvert qu'une très large majorité des communications personnelles accidentellement interceptées par le CST ne contenaient que du code malveillant et des efforts visant à personnaliser un message afin d'inciter la cible à en ouvrir le contenu. Le commissaire a donc conclu que les communications privées qui avaient été interceptées ne contenaient ni informations dommageables ni renseignements personnels et que, par conséquent, ces communications ne devraient pas être considérées comme étant des « communications privées » au sens du *Code criminel*[343].

212. [*** Une phrase a été supprimée pour retirer l'information préjudiciable ou privilégiée.***] D'ailleurs, le CST a redéfini la notion de communication privée dans le contexte des autorisations ministérielles de cybersécurité : le nombre des communications privées

---

[342] CST, *Ministerial Authorization Year End Report: 2018–2019*, sans date.
[343] Commissaire du CST, *Subject: Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization*, 29 mars 2019.

rapportées par le CST est désormais inférieur à 100 par année[344]. De l'avis du commissaire du CST, la méthode appliquée antérieurement donnait une idée déformée des risques que posent les activités de cyberdéfense pour la vie privée, alors que la nouvelle méthode [traduction] « devrait donner une mesure plus précise et plus significative des effets des activités du CST sur la vie privée[345] ». Le fait que les activités de cyberdéfense du CST ne posent que de faibles risques pour la vie privée des Canadiens ou des propriétaires de systèmes et de réseaux dotés de capteurs du CST devrait représenter un facteur digne d'attention pour les organisations qui invoquent l'indépendance comme motif de refus de s'intégrer au cadre gouvernemental de cyberdéfense. Au reste, il s'agit là d'un enjeu sur lequel le Comité se penche dans son évaluation.

Résumé

213. Le CST est au centre du cadre de cyberdéfense du Canada. Il recueille des renseignements sur les menaces pour les systèmes et les réseaux du gouvernement, dirige un réseau de défense perfectionné et en couches de capteurs qui trouvent et bloquent ces menaces, et fournit des directives et des conseils aux organisations gouvernementales (et de plus en plus aux Canadiens et aux organisations du secteur privé) pour renforcer leur propre sécurité en matière de technologie de l'information. Les moyens de cyberdéfense du CST ont évolué pour contrer les cybermenaces de plus en plus perfectionnées, et alors qu'ils ont été déployés à un nombre croissant d'organisations fédérales, ils ont joué un rôle de plus en plus prépondérant dans la capacité du gouvernement de défendre ses réseaux de cyberattaques. La présente section traite du pouvoir du CST de mener des activités de cyberdéfense, décrit le développement et l'utilisation de chacun des capteurs de cyberdéfense du CST, et présente les mécanismes de gouvernance interne utilisés pour régir ces activités et pour veiller à la responsabilisation du CST devant le ministre de la Défense nationale. La prochaine section du rapport décrit les mécanismes de gouvernance en place visant à gérer la tenue des activités de cyberdéfense dans l'ensemble du gouvernement.

---

[344] En guise d'éclaircissement, le CST indique qu'une communication reconnue comme étant privée contient [traduction] « des contenus substantiels [...] qui sont envoyés sans intention malveillante, mais pourraient contenir du matériel malveillant. Par exemple, un courriel envoyé par un destinateur qui n'est pas mal intentionné, mais qui ignore que son courriel contient du matériel malveillant (comme un lien malveillant ou du code malveillant intégré) pourrait toujours comporter du contenu reconnu comme étant substantiel, suscitant ainsi des attentes sur le plan de la protection de la vie privée ». CST, *Ministerial Authorization Year End Report: 2018–2019*, sans date.
[345] Commissaire du CST, *Subject: Annual Review of the Communications Security Establishment's Cyber Defence Activities under the 2017-2018 Cyber Defence Activities Ministerial Authorization*, 29 mars 2019.

Partie IV : Gouvernance de la cyberdéfense

214. La cyberdéfense est un sport d'équipe. Le gouvernement dispose de plusieurs mécanismes de gouvernance interministériels qui assurent une administration appropriée, des programmes et des opérations efficaces ainsi que la responsabilisation en matière de cyberdéfense. Lorsque survient une cyberattaque, le gouvernement a recours à des comités précis afin de coordonner son intervention selon la gravité et la portée de l'attaque. La présente section porte sur le rôle joué par divers comités en ce qui a trait à l'élaboration des politiques stratégiques sur la cyberdéfense, au soutien à la gestion efficace des initiatives liées à la sécurité des technologies de l'information touchant l'ensemble des opérations du gouvernement ainsi qu'à l'intervention en cas d'incidents de cybersécurité. On y décrit ensuite le Plan de gestion des événements de cybersécurité, le mécanisme principal utilisé par le gouvernement pour déterminer les rôles et les responsabilités ministériels concernant l'intervention en cas d'incidents de cybersécurité. On y précise entre autres comment le gouvernement détermine les niveaux d'intervention en cas de cyberattaques, les rôles de diverses entités de gouvernance ainsi que les étapes du processus.

Considérations stratégiques

215. Le Comité des sous-ministres sur la cybersécurité (CSM sur la cybersécurité) est la principale entité responsable de la coordination de la cybersécurité, des politiques et des objectifs stratégiques en matière de cybersécurité. Coprésidé par Sécurité publique Canada et le Centre de la sécurité des télécommunications (CST), il a pour mandat de mettre au point les politiques et les opérations de cybersécurité du Canada et de les diriger pour appuyer les priorités économiques et sociales du gouvernement. L'objectif du CSM sur la cybersécurité est le suivant :

- cerner les occasions en matière de politiques, de lois et de programmes pour veiller à ce que l'économie numérique du 21e siècle au Canada soit fondamentalement sécurisée dès la conception et que le leadership du Canada quant aux questions de cybersécurité soit reconnu à l'échelle internationale;
- superviser la progression de la mise en œuvre de la Stratégie nationale du Canada en matière de cybersécurité[346].

Le CSM sur la cybersécurité est essentiellement formé des sous-ministres de 14 organisations, y compris ceux dont les responsabilités sont liées aux opérations et aux politiques en matière de cybersécurité (CST, Secrétariat du Conseil du Trésor du Canada – SCT, et Sécurité publique Canada), les principaux organismes de sécurité (Bureau du Conseil privé, Service canadien du renseignement de sécurité – SCRS, ministère de la Défense nationale et les Forces armées canadiennes — MDN/FAC, et Gendarmerie royale du Canada — GRC), les secteurs liés aux infrastructures essentielles (Santé Canada, Ressources naturelles Canada, et

[346] Canada, mandat du Comité des sous-ministres sur la cybersécurité, 2019.

Transports Canada) ainsi que des sous-ministres issus de la sphère économique qui exercent des pouvoirs au sein des secteurs liés aux infrastructures essentielles du Canada (ministère des Finances, et Innovation, Science et Développement économique Canada).

216. Le CSM sur la cybersécurité remplace un comité précédent (voir la section sur l'évolution de la cyberdéfense de 2010 à 2018, paragraphe 86) et s'en distingue de façon importante. D'abord, le mandat révisé du CSM sur la cybersécurité consiste à améliorer la collaboration entre les secteurs de la sécurité, de l'économie et des infrastructures essentielles, étant donné que les questions de cybersécurité concernent de multiples niveaux de responsabilités ministérielles. Ensuite, la direction du comité, qui relevait de l'ancien sous-ministre de Sécurité publique Canada a été étendue au chef du CST, à titre de coprésident, illustrant la création du CCC et son rôle central au sein de la cyberdéfense[347]. Le nouveau comité a tenu ses deux premières réunions en juin et en septembre 2020 pour discuter de la collaboration entre les secteurs de la sécurité, des finances et des infrastructures essentielles; des cyberopérations et des cybermenaces; et de la Stratégie nationale sur la cybersécurité. Depuis, le Comité a tenu des réunions toutes les huit semaines.

217. Le CSM sur la cybersécurité est appuyé par un Comité des sous-ministres adjoints sur la cybersécurité (CSMA sur la cybersécurité). En tant que comité de soutien, le mandat du CSMA sur la cybersécurité est analogue à celui du CSM : élaborer les politiques sur la cybersécurité du Canada, et diriger les opérations de cybersécurité pour appuyer les priorités économiques et sociales du gouvernement. Il coordonne ces questions dans les secteurs et prépare des questions à soumettre à l'examen du CSM, aux fins de décision. L'objectif du CSMA sur la cybersécurité est le suivant :

- orienter les politiques et les opérations liées aux questions de cybersécurité;
- mettre au point des priorités relatives à la cybersécurité à l'intention des ministères et organismes membres;
- surveiller la progression de la mise en œuvre de la Stratégie nationale du Canada sur la cybersécurité;
- étudier les questions émergentes en matière de cybersécurité et de cybermenaces;
- examiner et préparer des questions à l'intention du CSM sur la cybersécurité.

Le CSMA sur la cybersécurité est coprésidé par le sous-ministre adjoint principal, Secteur de la sécurité nationale et de la cybersécurité de Sécurité publique Canada, et le chef adjoint du CST. Sa composition est essentiellement semblable à celle du CSM sur la cybersécurité. Il est appuyé par le Comité des directeurs généraux sur la cybersécurité et son sous-groupe opérationnel, le Comité des directeurs généraux sur les cyberopérations[348]. Le CSMA sur la cybersécurité se réunit aux dix semaines ou au besoin[349].

---

[347] Canada, *Mandat du Comité des sous-ministres sur la cybersécurité*, 2019.
[348] Sécurité publique Canada, *Comité des sous-ministres sur la cybersécurité*, 2019; et Sécurité publique Canada, *Mandat du Comité des directeurs généraux sur les cyberopérations*, 16 novembre 2018.
[349] Sécurité publique Canada, *Comité des sous-ministres sur la cybersécurité*, procès-verbal de la discussion, 13 août 2020.

218. Le Comité des sous-ministres sur les priorités et la planification intégrées est une autre entité de gouvernance qui assume des responsabilités liées aux considérations stratégiques en matière de cybersécurité à l'échelle du gouvernement. Comme énoncé dans la Politique sur les services et le numérique, le CSM sur les priorités et la planification intégrées agit à titre d'entité principale chargée d'améliorer le service à la clientèle et les opérations du gouvernement, et ce, par la gestion stratégique des services gouvernementaux, des informations, des données, des technologies de l'information et de la cybersécurité[350]. Alors que le CSM sur la cybersécurité susmentionné se penche sur le renforcement de la coopération au sein de l'appareil de la sécurité et du renseignement et avec les secteurs de l'économie et de l'infrastructure essentielle, le CSM sur les priorités et la planification intégrées œuvre principalement à la gestion des technologies de l'information et de la prestation de services.

219. Lorsque la politique du Conseil du Trésor sur les services et le numérique a été approuvée, le CSM sur les priorités et la planification intégrées a créé de nouveaux mandats qui représentent mieux l'importance d'aborder les questions sur un plan horizontal, et de mettre l'accent sur l'amélioration de la prestation de services à la population canadienne[351]. Conformément à la Politique sur les services et le numérique, l'objectif du CSM sur les priorités et la planification intégrées relativement à la cybersécurité est le suivant :

- établir les priorités en ce qui concerne les services et les biens partagés ainsi que les investissements et les acquisitions liés aux technologies de l'information qui touchent l'ensemble du gouvernement ou qui requièrent le soutien de Services partagés Canada (SPC);
- appuyer les ministères et leur permettre d'adopter des solutions organisationnelles pour des services courants;
- examiner et approuver le plan d'investissement et de travail de SPC, et formuler des recommandations concernant les initiatives de transformation de SPC;
- formuler des conseils et des recommandations stratégiques sur des questions liées à la gestion et à la prestation de services gouvernementaux aux particuliers et aux entreprises;
- souscrire à l'architecture organisationnelle et aux normes des technologies de l'information à l'échelle du gouvernement.

220. Le Comité des sous-ministres sur les priorités et la planification intégrée est coprésidé par le secrétaire du Conseil du Trésor et la chef de l'exploitation pour Service Canada. Il est formé de huit membres de la haute direction au gouvernement, y compris le dirigeant principal du CST, le président de SPC, le dirigeant principal de l'information du Canada et le greffier adjoint du Conseil privé[352].

---

[350] SCT, Politique sur les services et le numérique, article 4.1.1.1.
[351] SCT, « Notes d'allocution du Comité des sous-ministres sur les priorités et la planification intégrées », 22 août 2019.
[352] SCT, *Mandat du Comité des sous-ministres sur les priorités et la planification intégrées*, sans date.

Opérations, politiques et programmes

221. Le Comité des SMA tripartite sur la sécurité des technologies de l'information (Tripartite des SMA) est l'entité principale responsable de la gouvernance des initiatives de sécurité interministérielles liées aux technologies de l'information. Il est présidé par le dirigeant principal des technologies du SCT et se compose de sous-ministres du CST, de SPC et du SCT, et de ministères invités. Il oriente et surveille son comité de soutien tripartite des directeurs généraux sur la sécurité des technologies de l'information.

222. Le mandat du Tripartite des SMA se divise en deux parties. D'abord, à titre d'entité responsable de la prise de décisions, elle appuie la création, la prestation et la gestion efficaces des initiatives prioritaires en matière de sécurité des technologies de l'information qui touchent les systèmes internes du gouvernement, et l'ensemble de ses opérations. Conformément à cette partie de son mandat, le Tripartite des SMA doit :

- fournir des conseils afin d'établir la direction des stratégies et des politiques dans le domaine de la sécurité des technologies de l'information;
- orienter et conseiller le Comité tripartite des directeurs généraux (décrit ci-après) afin que les priorités stratégiques en matière de sécurité des technologies de l'information correspondent à la direction organisationnelle établie par le Tripartite des SMA;
- soumettre des initiatives et des recommandations clés aux comités de la haute direction aux fins de considération ou de décision.

La seconde partie du mandat du Tripartite des SMA consiste à gérer des événements majeurs liés à la cybersécurité, lesquels seront abordés ci-après. Ce comité ad hoc a tenu quatre réunions depuis 2016.

223. Le Comité tripartite des directeurs généraux soutient activement le Tripartite des SMA. Son mandat consiste plus précisément à :

- harmoniser les priorités stratégiques en matière de sécurité des technologies de l'information avec la direction organisationnelle établie par le Tripartite des SMA ou le CSMA sur les priorités et la planification intégrées;
- conseiller, orienter, surveiller et diriger le CST, le SCT et SPC afin de cerner les problèmes et les obstacles majeurs pouvant ralentir la progression des initiatives de sécurité organisationnelles liées aux technologies de l'information;
- surveiller l'état et la progression d'initiatives et de projets horizontaux précis du CST, du SCT et de SPC liés à la sécurité des technologies de l'information des organisations à l'échelle du gouvernement;
- fournir au Tripartite des SMA une orientation stratégique en matière de cybersécurité et produire des rapports sur l'état, les risques et les questions concernant les initiatives à l'échelle du gouvernement en matière de sécurité des technologies de l'information du CST, SCT et SPC.

Le Comité tripartite des directeurs généraux est présidé par le SCT et comprend des représentants du SCT, du CCC, de SPC et des invités. Il se réunit environ dix fois par an. Le 9 juillet 2021, on a informé le CPSNR qu'en mars 2021, le Tripartite des SMA ainsi que trois autres comités au niveau du sous-dirigeant avaient été fusionnés pour former le nouveau Comité quadripartite des SMA. Le Comité tripartite des directeurs généraux soutient ce nouveau comité[353].

Intervention en cas d'incident

224. Le Plan de gestion des événements de cybersécurité est le mécanisme principal régissant les rôles et les responsabilités en ce qui a trait aux interventions en cas d'incident de cybersécurité. Il sert de cadre opérationnel pour la gestion des événements de cybersécurité qui nuisent ou qui risquent de nuire à la capacité du gouvernement d'assurer la prestation de programmes et de services à la population canadienne. Conformément à la politique sur la sécurité du gouvernement, le SCT a publié le plan pour la première fois en 2015 et l'a mis à jour en 2019. À l'heure actuelle, le SCT révise le plan afin que les rôles et les responsabilités du nouveau CCC soient clairement définis[354]. Le Plan de gestion des événements de cybersécurité s'applique à tous les ministères et les organismes assujettis à la Politique sur la sécurité du gouvernement (110 ministères et organismes, à ce jour)[355].

Niveaux d'intervention du Plan de gestion des événements de cybersécurité

225. Le plan comporte quatre niveaux qui dictent l'intervention du gouvernement en cas d'événement de cybersécurité ciblant ses systèmes et ses réseaux. Les niveaux d'intervention se fondent sur deux facteurs : la gravité et la portée. On mesure la gravité d'un incident de cybersécurité au moyen d'évaluations ministérielles normalisées du préjudice, y compris les dommages causés à la santé et à la sécurité des particuliers; des pertes financières ou des difficultés économiques touchant des particuliers, des entreprises ou l'économie; de l'incidence sur les services et les programmes gouvernementaux, sur l'ordre civil ou sur la souveraineté nationale; des atteintes portées à la réputation de particuliers, d'entreprises ou du gouvernement ainsi qu'aux relations fédérales-provinciales et internationales. La portée d'un événement est mesurée selon le nombre de personnes, d'organisations, d'installations, de systèmes et de secteurs géographiques touchés par l'événement ainsi que la durée anticipée du préjudice. En se basant sur leur analyse, les ministères rapportent au CCC les conséquences attendues d'une compromission. Celles-ci peuvent être mineures (p. ex. dommages physiques ou difficultés financières touchant un particulier, légère nuisance à la prestation de services d'un ministère) comme elles peuvent être très graves (grave préjudice

---

[353] SCT, *Mandat du Comité tripartite des directeurs généraux sur la sécurité de la TI*, février 2021; SCT, « Ébauche du mandat du Comité des sous-ministres quadripartite », 3 mars 2021; et SCT, *NSICOP Review– TBS Comments on Draft Final Report (9-July-2021)*, p. 6, 9 juillet 2021.
[354] CCC, comparution devant le CPSNR, 30 octobre 2020.
[355] La politique du Conseil du Trésor sur la sécurité du gouvernement s'applique aux organisations répertoriées aux annexes I, I.1 (colonne 1), II, IV et V de la LGFP.

à la sécurité publique, à la sécurité nationale ou à l'économie, perte de confiance envers le gouvernement).

226. En se basant sur cet apport ministériel, le CCC et le SCT ont recours à une matrice normalisée afin de déterminer le niveau d'intervention global du gouvernement[356]. Cette matrice tient compte de la probabilité qu'une compromission ait une incidence sur un ou plusieurs programmes ou services gouvernementaux internes, si des services externes sont touchés, et s'il est possible que le préjudice s'étende davantage. Le CCC et le SCT se fondent sur ces valeurs pour déterminer le niveau d'intervention requis, qui s'échelonne du niveau 1 (ne requiert qu'une coordination minime du gouvernement) au niveau 4 (requiert une coordination maximale). Voici les quatre niveaux d'intervention du gouvernement :

- **Niveau 1 :** La mise en application du plan n'est pas requise. De tels événements ne nécessitent qu'une intervention ministérielle et un niveau de coordination gouvernementale normal. Les ministères interviennent conformément aux procédures internes normales, appliquent les mesures préventives habituelles et communiquent avec le CCC pour obtenir des directives et des conseils.
- **Niveau 2 :** La gravité et la portée de l'événement de cybersécurité sont supérieures au niveau 1, et le plan doit être appliqué : une intervention limitée à l'échelle du gouvernement est requise. Tous les intervenants principaux se tiennent à un palier d'alerte accru quant aux cyberactivités. Cela consiste à surveiller les capteurs ministériels à l'échelle du gouvernement (p. ex. capteurs réseau et capteurs sur l'hôte) pour vérifier si l'événement a eu des répercussions sur d'autres ministères, et faire en sorte que toute incidence réelle ou potentielle soit maîtrisée et atténuée. On fait appel aux intervenants spécialisés lorsque la menace ou l'incident a trait au crime, au terrorisme ou à la défense nationale.
- **Niveau 3 :** La gravité et la portée de l'événement de cybersécurité sont supérieures au niveau 2 et requièrent une intervention immédiate et exhaustive à l'échelle du gouvernement. L'intervention lors d'un incident de ce niveau est coordonnée à l'aide de la structure de gouvernance du plan, dans le cadre de laquelle les ministères et organismes reçoivent en continu des directives sur la marche à suivre.
- **Niveau 4 :** La gravité et la portée de tels événements relèvent du niveau maximal. On les considère comme des « événements graves et catastrophiques » qui ont une incidence sur de nombreuses institutions, sur la confiance envers le gouvernement ou sur d'autres aspects de l'intérêt national. On fait alors appel au Plan fédéral d'intervention d'urgence de Sécurité publique Canada, qui établit les mécanismes et les processus permettant d'harmoniser l'intervention du gouvernement fédéral en cas d'urgence[357]. À ce jour, on ne rapporte aucun cyberincident de niveau 4[358].

---

[356] SCT, *Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC)*, 2019.
[357] Sécurité publique Canada, « Plan fédéral d'intervention en cas d'urgence », 2011, www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-fr.pdf.
[358] CST, Breffage au Secrétariat du CPSNR, 11 mars 2021.

Les événements de cybersécurité sont dynamiques, et leur préjudice et leur portée peuvent s'aggraver ou s'atténuer à mesure qu'ils se déroulent. Ainsi, au cours d'un événement de cybersécurité donné, le gouvernement peut augmenter ou diminuer son niveau d'intervention. Les décisions relatives à l'augmentation ou à la diminution du niveau d'intervention du gouvernement sont prises par des entités de gouvernance de plus en plus haut placées, décrites ci-dessous.

Entités de gouvernance liées au Plan de gestion des événements de cybersécurité

227. Le Plan de gestion des événements de cybersécurité fait appel à trois catégories d'intervenants. Le SCT et le CCC agissent à titre d'intervenants principaux et sont mobilisés lors d'événements de niveaux 2 et 3. Le CCC fournit aussi des conseils et des directives dans le contexte des événements de niveau 1. En tant qu'intervenants spécialisés, Sécurité publique Canada, SPC, la GRC, le SCRS et le MDN/FAC sont mobilisés lorsque surviennent des incidents ou des menaces de cybersécurité confirmés, selon leur mandat et leurs champs d'expertise. Le plan répertorie aussi d'autres intervenants jouant divers rôles liés à la cyberdéfense, y compris le Bureau du dirigeant principal de l'information du Canada, le Centre des opérations du gouvernement, le Bureau du Conseil privé, le Comité canadien chargé des systèmes de sécurité nationale du CST (responsable de la gouvernance et de la protection des systèmes Très secret)[359], le Comité des directeurs généraux sur l'intervention en cas d'incident et des partenaires externes, tels que des fournisseurs du secteur privé et d'autres niveaux de gouvernement.

228. Le plan établit les trois entités de gouvernance chargées d'accorder la priorité aux interventions du gouvernement en cas de cyberincidents graves et de gérer l'augmentation du niveau d'intervention en cas d'événements de cybersécurité :

- **Équipe de coordination des événements :** Ce groupe d'intervenants de niveau opérationnel est coprésidé par le SCT et le CCC. Il est mobilisé lors d'événements de niveau 2, ou lorsque d'autres entités de gouvernance font appel à lui dans le contexte d'événements de niveaux 3 ou 4. L'équipe de coordination des événements collabore avec des intervenants afin de recommander des voies à suivre et de veiller à ce que l'équipe de direction (ci-dessous) soit informée de la situation.
- **Équipe de direction :** Ce comité au niveau des directeurs généraux est coprésidé par le SCT et le CCC. Il intervient lors d'événements de niveau 3. L'équipe de direction fournit une orientation stratégique à l'équipe de coordination des événements et veille à ce que les représentants principaux du gouvernement soient informés de la situation.
- **Tripartite des SMA :** Ce comité des sous-ministres adjoints est présidé par le dirigeant principal des technologies du SCT. On fait appel à lui lors d'événements de niveau 3. Il oriente l'intervention de l'équipe de direction et la prise de mesures d'atténuation. En outre, il lui incombe de s'assurer que les sous-ministres sont informés de la situation.

---

[359] CST, *Comité canadien chargé des systèmes de sécurité nationale*, bulletin, première édition, mars 2018.

Dans l'éventualité d'un incident de niveau 4, le Tripartite des SMA appuierait au besoin le Comité des sous-ministres adjoints sur le Plan fédéral d'intervention en cas d'urgence. C'est le sous-dirigeant du CCC et le sous-ministre adjoint de SPC, Réseaux, sécurité et services numériques qui coprésident ce comité.

Les trois entités de gouvernance peuvent faire appel à d'autres ministères au besoin. Par exemple, lorsqu'un événement est lié à des préoccupations en matière de sécurité nationale ou pourrait être de nature criminelle, toutes les équipes de gouvernance peuvent avoir recours à des représentants du SCRS et de la GRC, respectivement. Les ministères qui sont directement touchés par des menaces ou des incidents précis sont invités à participer aux discussions relatives à la gouvernance.

Les étapes du processus de gestion des événements de cybersécurité

229. Le processus de gestion des événements de cybersécurité comporte quatre étapes : la préparation; la détection et l'évaluation; l'atténuation et la reprise; et les activités post-événements.

230. Lors de la préparation, une série d'étapes doit être suivie afin que le gouvernement soit prêt à intervenir en cas d'événement de cybersécurité. Celles-ci comprennent l'établissement des rôles et des responsabilités, la mise à l'essai des plans et des procédures, la formation des employés et l'application de mesures de protection et de prévention au niveau des systèmes hôtes, des applications et des réseaux des systèmes d'information du gouvernement. Dans le cadre de cette étape continue, tous les intervenants du Plan de gestion des événements de cybersécurité, y compris les ministères et les organismes visés par le plan, sont responsables de la mise en œuvre de telles mesures au sein de leur secteur de responsabilité respectif. Pour sa part, le SCT est chargé d'élaborer et d'entretenir le plan, de coordonner régulièrement des exercices avec tous les intervenants participants et d'examiner les rapports de leçons à retenir concernant des événements antérieurs afin de guider les changements de politiques. Il incombe au CCC de faire en sorte que les ministères et les organismes reçoivent les directives et les conseils requis pour atténuer les cybermenaces et les vulnérabilités et ainsi prévenir les incidents de cybersécurité.

231. La seconde étape, celle de la détection et de l'évaluation, consiste en la surveillance des événements de cybersécurité émergents et l'évaluation de l'incidence potentielle ou réelle sur la prestation de services gouvernementaux, les opérations gouvernementales ou la confiance envers le gouvernement. Dans le cadre de cette étape, le CCC est chargé de surveiller les sources et l'information techniques rapportées par d'autres intervenants; le périmètre du gouvernement et tous les points d'entrée visibles au CCC; les environnements infonuagiques; les réseaux et les sources de renseignement du gouvernement; et l'information issue de sources intérieures ou étrangères. Le MDN/FAC est responsable de la surveillance de tous les réseaux gérés par le MDN. Pour leur part, la GRC et le SCRS sont respectivement chargés de

surveiller l'information issue de sources de surveillance du crime et de sources de renseignement.

232. Le Plan de gestion des événements de cybersécurité engage un certain nombre de responsabilités générales et particulières. De manière générale, les organisations sont tenues de mettre en œuvre des paramètres de sécurité conformes à la Politique sur la sécurité du gouvernement. En outre, elles doivent aviser les autorités appropriées lorsqu'un événement s'inscrit dans le champ de la sécurité nationale ou de l'application de la loi. Plus précisément, les principaux intervenants spécialisés sont tenus de signaler les événements de cybersécurité au SCT et au CCC, et, lorsqu'ils ont trait au crime, au terrorisme ou à l'armée, à la GRC, au SCRS et au MDN, respectivement. Quand le CCC reçoit de l'information concernant un événement de cybersécurité potentiel ou réel, il détermine le niveau d'intervention initial du gouvernement après consultation avec le SCT, et d'autres partenaires, au besoin.

233. La troisième étape du plan consiste en l'atténuation et la reprise. L'objectif de cette étape est d'atténuer les événements avant qu'ils donnent lieu à des incidents, et de maîtriser et de minimiser les répercussions des incidents qui sont survenus afin d'assurer un retour rapide aux opérations normales. Les interventions peuvent se traduire par l'installation de rustines, la maîtrise et l'atténuation d'un incident, le recours à des plans de continuité organisationnelle et de reprise à la suite d'une catastrophe, ou la fermeture temporaire des services vulnérables.

234. Les rôles et les responsabilités des ministères visés en matière d'atténuation et de reprise sont établis dans le plan. En ce qui concerne les événements de niveau 3 (et certains événements de niveau 2 selon la décision des intervenants participants), le SCT se charge de la coordination stratégique, y compris de l'orientation stratégique des ministères pour ce qui est de minimiser l'incidence des événements de cybersécurité à l'échelle du gouvernement. Le Centre des opérations du gouvernement s'acquitterait de ce rôle dans l'éventualité d'un événement de niveau 4. Pour sa part, le CCC est responsable de la coordination des opérations lors d'événements de tout niveau, y compris de l'orientation technique et de la prestation de conseils aux ministères en ce qui a trait à l'atténuation et aux mesures de maîtrise de l'événement. Dans le cadre du plan, tous les principaux intervenants spécialisés fournissent des conseils et des directives selon les renseignements obtenus de leurs sources respectives. Enfin, les ministères et organismes doivent mettre en œuvre les directives fournies par le CCC et le SCT dans le respect des échéances fixées.

235. En ce qui concerne tous les événements de niveaux 3 et 4 (et certains événements de niveau 2 selon la décision des intervenants participants), le CCC dirige l'élaboration et la mise en œuvre d'un plan de maîtrise de l'incident à l'échelle du gouvernement, et organise une intervention ciblée. De plus, il mène des examens et des analyses judiciaires des systèmes de technologies de l'information en collaboration avec les ministères touchés. Les ministères et organismes ainsi que les fournisseurs de service mettent en œuvre le plan de maîtrise de l'incident, et SPC travaille à cerner et à signaler les systèmes touchés ou vulnérables.

236. La quatrième étape du Plan de gestion des événements de cybersécurité se rapporte aux activités post-événements. Les ministères mènent alors des analyses à la suite de l'événement et déterminent les leçons à retenir afin d'améliorer le processus de gestion des événements de cybersécurité. Dans le cadre de cette étape, les ministères et organismes touchés doivent produire un rapport sur les leçons à retenir et un plan d'action, et contribuer aux activités post-événements au besoin. Le CCC compile les constats des ministères et produit un rapport post-événement, qui comprend un échéancier des événements et une analyse de l'origine. En ce qui concerne les événements de niveau 3 (et certains événements de niveau 2 selon la décision des intervenants participants), le SCT doit produire un rapport sur les leçons à retenir et un plan d'action au nom du gouvernement. Il doit également surveiller la mise en œuvre des recommandations. Le Centre des opérations du gouvernement doit produire un rapport sur les leçons à retenir et un plan d'action semblables dans l'éventualité d'un événement de niveau 4. Enfin, tous les autres intervenants doivent appuyer la création de rapports sur les leçons à retenir à l'échelle du gouvernement et mettre en œuvre des mesures de suivi au sein de leur secteur de responsabilité respectif[360].

[360] SCT, *Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC)*, 2019.

Partie V : Évaluation du Comité sur le cadre de cyberdéfense

237. Le gouvernement du Canada a jeté les bases d'un cadre rigoureux et résilient de cyberdéfense. Alors que d'autres états ont été victimes d'attaques de cyberexploitation et de rançongiciels, le Canada a soit bloqué les attaques, soit limité les répercussions les plus graves. Cela n'a pas toujours été le cas. Il y a moins de dix ans, le Canada a subi de multiples cyberattaques néfastes contre certaines de ses institutions gouvernementales principales. La compréhension du Canada sur la nature de la menace était limitée, ses moyens de cyberdéfense étaient faibles dans certains ministères et bons dans d'autres, et la gouvernance payait pour une coordination centrale bancale et une responsabilisation compartimentée. Le Centre de la sécurité des télécommunications (CST), l'expert technique principal du Canada en matière de cyberdéfense, déployait ses capteurs de défense seulement à l'extérieur d'une poignée d'organisations gouvernementales et n'avait pas encore conçu le type de mesures de défense dynamique automatisées nécessaires pour lutter contre les attaques incessantes des auteurs de cybermenaces qui caractérisent l'environnement moderne de cybermenace.

238. En 2020, toutefois, le Canada était devenu un chef de file mondial en défense de ses réseaux contre les cyberattaques. Le changement a été apporté par une leçon en trois temps : l'importance de maximiser les autorités devant le changement; de répondre aux crises non seulement dans le but de les résoudre, mais aussi pour préparer l'avenir; et de veiller à ce que les pouvoirs et les organisations soient adaptés à leurs rôles. Cela ne signifie pas que le Canada est parfait : le gouvernement doit continuer de s'adapter devant les menaces changeantes et l'évolution de la technologie, et le Comité présente un certain nombre de recommandations à cette fin. Il fournit également son évaluation de ces changements ci-dessous.

L'évolution de la cyberdéfense au Canada : Un cycle vertueux, mais incomplet

239. Le CST est un élément central de cette histoire. Lorsqu'il a reçu ses pouvoirs conférés par la loi en 2001, les activités du CST visant à protéger les systèmes de données et de technologie de l'information se concentraient sur l'essai des systèmes et le chiffrement de pointe. L'idée de la cyberdéfense existait à peine. Durant plusieurs années, le CST était la seule organisation fédérale autorisée légalement à exploiter les systèmes qui risquaient d'intercepter les communications privées, comme les coupe-feux et la détection d'intrusion, et qui protégeaient un réseau gouvernemental. En s'appuyant sur ses connaissances en renseignements électromagnétiques, le CST a développé et déployé des capteurs de défense exclusifs aux organisations attaquées par des adversaires étatiques expérimentés : la Chine et la Russie. Ces activités auraient été impossibles si le gouvernement n'avait pas permis au CST d'utiliser ses pouvoirs singuliers, c'est-à-dire les autorisations ministérielles, de façon inattendue. Entre 2002 et 2007, le CST a testé de nouvelles approches et techniques tout en tâchant de protéger plusieurs ministères contre les cyberattaques. Ses efforts n'étaient pas

sans obstacle. En effet, en 2006, le CST a été forcé de mettre ses activités de cyberdéfense sur pause pendant plus d'un an parce qu'elles ne respectaient pas les obligations légales découlant de ces pouvoirs. Après avoir restructuré le programme d'autorisation ministérielle et son cadre stratégique, le CST a repris ses activités de cyberdéfense et a approfondi son expertise lui permettant de détecter et de bloquer les cybermenaces les plus poussées. Néanmoins, la réussite du CST à cibler les menaces et à collaborer avec des ministères en particulier pour mettre en œuvre des mesures d'atténuation aurait probablement encore été limitée par l'approche du gouvernement en matière de cyberdéfense pour chaque ministère.

240. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] Les cyberattaques importantes ont marqué un tournant. En 2010, le CST a déployé ses mesures de cyberdéfense sur le Réseau de la Voie de communication protégée du gouvernement, où 75 ministères avaient migré leur accès Internet sur un réseau unique géré par Travaux publics et Services gouvernementaux Canada. Ce déploiement avait révélé que la Chine avait pénétré les systèmes numériques de plusieurs organisations gouvernementales, notamment le Secrétariat du Conseil du Trésor du Canada (SCT) et le ministère des Finances, et avait volé d'importantes données. Par conséquent, le SCT a exigé à tous les ministères de joindre le Réseau de la Voie de communication protégée, à la suite de quoi plusieurs ministères ont migré leur accès Internet, ce qui a jeté les bases de l'évolution vers le Service Internet d'entreprise plusieurs années plus tard. En 2014, les réseaux du gouvernement ont été victimes de l'attaque HEARTBLEED et le Conseil national de recherches a subi une compromission critique et distincte entraînant un vol important d'information de recherches et de données scientifiques. Les deux incidents ont été marquants pour le gouvernement, révélant des vulnérabilités de système étendues et des faiblesses dans le cadre de cyberdéfense du gouvernement. Ils ont aussi poussé le premier déploiement par le CST de cyberdéfenses précises. Ces déploiements ont ouvert la voie à l'élargissement et à la modernisation plus amples de ces services. Ces attaques ont aussi révélé d'importants problèmes en ce qui a trait à la coordination et à la gouvernance interministérielles de cyberincidents majeurs. Le SCT a donc modernisé différentes politiques et directives en vue de préciser les rôles et les responsabilités, et les principaux ministères ont joué des rôles de direction de plus en plus importants dans l'intervention relative aux cyberincidents.

241. La création de nouveaux pouvoirs et de nouvelles organisations par le gouvernement était essentielle. En 2011, le gouvernement a formé une nouvelle organisation, Services partagés Canada (SPC), pour uniformiser et regrouper l'achat et l'approvisionnement de services et de technologies de l'information dans l'ensemble des ministères. Au départ, le gouvernement a mis l'accent sur les aspects d'économie de la création de SPC, mais lorsque l'étendue des difficultés a été reconnue (par exemple, SPC a hérité d'un vaste mélange d'infrastructures nouvelles et désuètes), le gouvernement a investi des sommes considérables pour moderniser son infrastructure de technologie de l'information. Entre autres, SPC intégrerait la sécurité aux initiatives ultérieures de modernisation de la technologie de l'information du gouvernement. D'un point de vue de cyberdéfense, les changements les plus importants découlant de la création de SPC étaient le regroupement de plus en plus marqué de ministères sous le Service Internet d'entreprise (vu plus en détail ci-dessous) et la fonction contraignante

qu'a joué SPC en obligeant les ministères visés à déployer des correctifs pour leurs appareils, systèmes et réseaux.

242. D'importants changements aux structures du gouvernement se sont poursuivis en 2018 avec la création d'un groupe au CST : le Centre canadien pour la cybersécurité (CCC). Résultat de la fusion de trois organisations, le CCC est la source consolidée et habilitée pour la cybersécurité au Canada. Il est responsable de protéger et de défendre les actifs électroniques du Canada au moyen de conseils, d'orientation et d'aide opérationnelle directe et, en collaboration avec le SCT, de diriger l'intervention du gouvernement face aux événements de cybersécurité. Il modifie continuellement son approche à la cyberdéfense, met à jour ses capteurs réseau afin de mieux détecter et bloquer le cybercomportement malveillant, crée de nouveaux capteurs sur l'hôte pour approfondir les couches de défense du réseau jusqu'au niveau des appareils personnels, et travaille à repérer les nouvelles menaces en accumulant et en analysant les nouveaux renseignements et les données relatives aux anomalies. L'adoption de la *Loi sur le Centre de la sécurité des télécommunications* en 2019 peut contribuer davantage à ces efforts en précisant les pouvoirs et immunités du CST, y compris l'ajout de cyberopérations défensives comme outil embryonnaire pour protéger les systèmes gouvernementaux dans des circonstances précises.

243. Au fil du temps, ces changements ont créé un cycle vertueux. Plus les ministères migrent vers le Service Internet d'entreprise de SPC, plus ils profitent du perfectionnement des mesures de défense dynamique du CCC. Plus les ministères adhèrent aux services de cyberdéfense du CCC pour les appareils finaux et les environnements infonuagiques, plus les systèmes et les données du gouvernement sont protégés contre les cybermenaces et le cybercrime de pointe. Plus le CCC obtient et analyse des données provenant de ses capteurs de cyberdéfense de plus en plus nombreux, plus il sera en mesure de repérer et de bloquer de nouvelles cybermenaces. Enfin, plus les rôles, les responsabilités, la gouvernance et l'intervention aux incidents sont définis clairement suivant la création de ministères et l'adoption de nouveaux pouvoirs et de nouvelles politiques et directives, plus le gouvernement sera en mesure d'agir rapidement et délibérément sur les menaces qui évoluent. En outre, la situation devrait demeurer inchangée pour le moment. Par exemple, le SCT a ordonné l'utilisation de capteurs infonuagiques dans le cadre des mesures de sécurité infonuagique, faisant en sorte que des mesures de sécurité rigoureuses sont intégrées dès la conception. Ces changements et leur évolution continue ont donné des résultats tangibles : le nombre d'incidents de pénétration de réseau, de perte de données ou de dommages qui touchent le Canada diminue de plus en plus.

Les organisations protégées : des opinions divergentes

244. Il est impossible que ce système atteigne la perfection : les menaces évoluent, des erreurs sont commises, les défenses échouent. Cependant, il est toujours possible de l'améliorer, mais il faut surmonter trois obstacles importants. Le premier obstacle est l'application non uniforme des politiques et des directives du Conseil du Trésor. Ces instruments déterminent l'étendue des services accordés aux ministères. La *Loi sur la gestion*

des finances publiques regroupe la plupart des organisations fédérales dans des annexes précises selon leur mandat, leur structure de gouvernance et leur niveau d'indépendance, et donne au Conseil du Trésor l'autorisation légale de publier des politiques et des directives. De cette façon, la normalisation des exigences en matière de responsabilisation pour les organisations de l'ensemble du gouvernement est standardisée. Toutefois, les trois principaux instruments du Conseil du Trésor pour la cyberdéfense n'ont pas la même portée d'application. D'un côté, la Politique sur la sécurité du gouvernement et ses directives de sécurité connexes, comme l'utilisation sécurisée des services infonuagiques commerciaux, s'appliquent à 110 organisations fédérales; tandis que la Politique sur les services et le numérique (et ses politiques dérivées) et le Plan stratégique des opérations numériques s'appliquent à 87 organisations fédérales. De façon plus générale, les éléments centraux du cadre administratif du gouvernement sur la cyberdéfense ne s'appliquent pas uniformément (ou dans certains cas, du tout) aux 169 organisations du gouvernement du Canada.

245. Le deuxième obstacle est la façon dont le mandat et les responsabilités de SPC relativement aux services de cybersécurité sont énoncés. Une série de décrets renvoie à des annexes précises de la *Loi sur la gestion des finances publiques* afin de définir les ministères auxquels SPC *doit* fournir ses services de courriel, de centre de données, de réseautage et de points terminaux, et ceux auxquels SPC *peut* fournir ces services. Le groupe de ministères et organismes (partenaires principaux de SPC) auquel SPC doit fournir des services est le mieux protégé, puisqu'il reçoit l'éventail complet des services de SPC. Pour le groupe auquel SPC peut fournir des services (clients obligatoires et facultatifs de SPC), SPC fournit des services essentiellement à la carte, c'est-à-dire qu'il fournit une partie ou l'ensemble de ses services selon un principe de recouvrement de coûts. Lorsque les organisations gouvernementales estiment que les coûts des services sont hors de prix, ils n'y souscrivent pas, rendant leurs données potentiellement vulnérables à l'exploitation. Malgré tout, ces organisations ont des liaisons électroniques avec l'infrastructure numérique d'autres organisations et peuvent donner accès par inadvertance à un cyberacteur malveillant et possiblement menacer la sécurité globale du gouvernement.

246. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] Le troisième obstacle est l'établissement d'un principe fondamental pour l'augmentation du nombre d'organisations gouvernementales qui bénéficient de la protection du programme de cyberdéfense du CST. Le mandat du CST en vertu de la *Loi sur le Centre de la sécurité des télécommunications* confère le pouvoir le plus complet de fournir une protection de cyberdéfense aux institutions fédérales. Cependant, aucun ministère n'est obligé d'utiliser au moins un capteur de cyberdéfense du CST. Bien que le CST fournisse actuellement au moins un capteur de cyberdéfense à *** pour cent des 169 organisations fédérales qui composent le gouvernement du Canada, *** pour cent des organisations fédérales ne sont pas protégées par un capteur de cyberdéfense du CST. Cette situation est problématique. Premièrement, elle limite la quantité d'activités de cybermenace ciblant les ministères que le CST peut observer. Deuxièmement, elle nuit à la capacité du CST de réagir rapidement lorsqu'un ou plusieurs ministères qui ne sont pas protégés sont compromis par une cyberattaque. De plus, ces organisations à l'extérieur de la zone de couverture des capteurs de cyberdéfense du CST ne

savent probablement pas elles-mêmes si elles sont attaquées. Une des avenues de protection possibles pour ces organisations est lorsque le programme du renseignement électromagnétique du CST, grâce à son suivi des cybermenaces mondiales, obtient une certaine indication de compromission et communique cette information au CCC. Comme le mentionne l'étude de cas 6 sur l'attaque contre une société d'État, une telle aide viendrait presque toujours après le vol de données et la compromission de l'intégrité du système de l'organisation. Pour l'avenir, il sera important de maximiser le nombre de ministères utilisant les trois types de capteurs (lorsque possible) pour protéger leurs réseaux afin de protéger davantage l'information sensible détenue par les organisations gouvernementales et de veiller à ce que les Canadiens puissent profiter des services gouvernementaux essentiels dont ils ont besoin.

La réussite et la faille : Sécuriser l'accès Internet au gouvernement

247. Le nombre d'organisations fédérales qui utilisent l'accès sécurisé à Internet du gouvernement est à la base des trois obstacles. La création du Service Internet d'entreprise de SPC et son adoption progressive par les ministères ont joué un rôle de base dans le renforcement du cadre de cyberdéfense du gouvernement. De plus, l'intégration des mesures de défense dynamique *** du CST dans les points d'accès à Internet du Service Internet d'entreprise est sans doute la mesure de défense la plus importante à l'heure actuelle dans le cadre de défense du gouvernement. Pour étendre ce cadre à toutes les organisations du gouvernement du Canada, il faut éliminer ces trois obstacles susmentionnés.

248. Premièrement, les ministères devraient appliquer les politiques et directives du Conseil du Trésor de façon cohérente. Depuis 2006, le Conseil du Trésor a publié à quatre reprises une directive « obligatoire » pour les ministères, les obligeant à utiliser des services Internet sécurisés, le plus récemment dans le cadre du Plan stratégique des opérations numériques en 2018. Cela donne à penser que les organisations gouvernementales ont encore toute latitude pour choisir les directives du Conseil du Trésor qu'elles acceptent et le moment où elles le font. En date d'août 2021, 94 des 169 organisations souscrivent au Service Internet d'entreprise. Il s'agit notamment de presque toutes les organisations assujetties aux politiques du Conseil du Trésor, portant le Comité à conclure que les directives du Conseil du Trésor dans ce secteur ont, éventuellement, porté leurs fruits. À l'heure actuelle, la faille du cadre de cyberdéfense du gouvernement se trouve parmi les 75 organisations fédérales qui *ne sont pas* assujetties à l'orientation du Conseil du Trésor dans ce domaine (plus de détails au paragraphe 251). Ces organisations demeurent à l'extérieur du périmètre sécurisé du gouvernement et de la protection offerte par les mesures de cyberdéfense du CST.

249. Deuxièmement, la série de décrets qui édictent le mandat et les responsabilités de SPC en matière de services de cybersécurité crée une couverture en mosaïque pour les organisations gouvernementales. Les 94 organisations qui reçoivent le Service Internet d'entreprise ou y souscrivent comprennent les 43 partenaires principaux, les 27 clients obligatoires et les 24 clients facultatifs de SPC. Pour les partenaires principaux de SPC, la

fourniture de l'éventail complet de services de SPC comprend le Service Internet d'entreprise, et SPC est obligé de le fournir. Les clients obligatoires et facultatifs de SPC qui reçoivent le Service Internet d'entreprise ont choisi de le recevoir. Pour résumer, ces organisations contribuent au cycle vertueux du cadre et en profitent, comme il est mentionné ci-dessus. En revanche, d'autres organisations fédérales restent à l'extérieur du périmètre sécurisé du gouvernement et de la protection offerte par les mesures de cyberdéfense du CST. En dépit de la vulnérabilité qui touche ces organisations, aucun fonds n'est consacré à intégrer certaines d'entre elles, comme les petits ministères et organismes, aux services de sécurité plus vastes de SPC, y compris le Service Internet d'entreprise. Cela revêt une importance considérable. Comme l'a entendu le Comité :

> [traduction] Les passerelles Internet et les connexions à Internet ont été regroupées, en commençant par seulement les 43 grands ministères et organismes sous le mandat de SPC. Tous les petits ministères et organismes ont été laissés à eux-mêmes. [...] Il est essentiel de les intégrer aux moyens de SPC et du CST pour les protéger. Ils ont besoin de ces services plus que quiconque[361].

250. Troisièmement et finalement, de toutes les organisations gouvernementales qui reçoivent la protection des capteurs de cyberdéfense du CST, la majorité est protégée parce qu'elle reçoit le Service Internet d'entreprise. En d'autres mots, il s'agit *du* moyen d'obtenir la protection avancée du CST. Des *** organisations fédérales qui reçoivent au moins un capteur de cyberdéfense du CST, *** d'entre elles profitent de la protection offerte par les mesures de défense dynamique ***. *** Quelques ministères ont conclu leur propre entente bilatérale avec le CST concernant le déploiement de capteurs réseau. Le Comité fait l'éloge des efforts de SPC et du CST visant à assurer une protection exhaustive pour les systèmes gouvernementaux. Pour le moment, la préoccupation est plutôt de mettre en place la cyberprotection du CST dans les organisations qui ne sont pas considérées comme étant des ministères et organismes, mais qui sont quand même liées numériquement au gouvernement fédéral.

Sociétés d'État et intérêts gouvernementaux

251. Les 75 organisations qui ne sont pas touchées par l'orientation du Conseil du Trésor et le Service Internet d'entreprise sont principalement des sociétés d'État et certains « intérêts » gouvernementaux. Ces sociétés et intérêts ont été créés par le gouvernement pour diverses raisons et leur mandat est défini de façon indépendante de l'orientation gouvernementale à certains niveaux. Certains ont une latitude considérable pour concevoir et protéger leur propre infrastructure de technologie de l'information, et bon nombre d'entre eux font affaire avec des entreprises du secteur privé pour obtenir leur infrastructure, héberger leurs données et protéger leurs systèmes. Néanmoins, ces organisations doivent, au bout du compte, se conformer aux exigences fiduciaires et de responsabilisation de la Couronne. Tout particulièrement aux fins du présent examen, ces organisations reçoivent, conservent et utilisent de l'information sensible de

[361] Représentants du SCT, comparution devant le CPSNR, 27 novembre 2020.

Canadiens et d'entreprises canadiennes, de l'information qui n'est pas à l'abri de la compromission par les cyberacteurs les plus expérimentés, y compris les états. Toutefois, elles n'ont pas à respecter les politiques du Conseil du Trésor visant à assurer la sécurité de leur infrastructure de technologie de l'information. Elles sont aussi exclues des sections exécutoires des décrets d'habilitation de SPC et la majorité n'obtient donc pas de services de cyberdéfense de SPC. Il en résulte que la plupart d'entre elles ne profitent pas de la protection du Service Internet d'entreprise du CST. Par conséquent, ces organisations risquent donc de manière inquiétante de perdre leurs propres données et, lorsqu'elles maintiennent des liaisons électroniques avec des ministères connexes, de devenir par inadvertance un vecteur vers les systèmes sécurisés du gouvernement, mettant en danger les données et les systèmes du gouvernement.

252. Le Comité reconnaît l'importance de l'indépendance pour les sociétés d'État et, le cas échéant, les intérêts gouvernementaux. L'indépendance du mandat est essentielle pour protéger l'intégrité d'aspects importants de l'ordre public, y compris l'administration de la justice ou des systèmes financiers et économiques du Canada. Le Comité tient à souligner deux points, par contre, pour déterminer si l'indépendance du mandat doit équivaloir à un contrôle exclusif des données, des systèmes et des réseaux. Premièrement, il est évident que les produits et les services disponibles sur le marché offrent une protection insuffisante contre les cybermenaces les plus pointues. La Chine et la Russie ont montré à maintes reprises qu'elles sont capables de pénétrer des systèmes et des réseaux bien défendus, particulièrement ceux qui ne sont pas protégés par des mesures de cyberdéfense aussi perfectionnées et appuyées par l'État. La protection offerte par le CST et SPC est peut-être imparfaite, mais la combinaison de leurs mesures de cyberdéfense offre la probabilité la plus élevée de protéger les données du gouvernement et l'intégrité de ses systèmes à l'avenir.

253. [*** Ce paragraphe a été revu pour retirer l'information préjudiciable ou privilégiée. ***] Deuxièmement, les sociétés d'État et d'autres intérêts gouvernementaux sont les cibles de cyberactivités étatiques et de cybercriminels, comme l'ont montré des incidents précis au cours des dernières années. De façon plus générale, la Russie, la Chine et d'autres états prennent pour cible des fournisseurs d'infrastructure essentielle, y compris ceux mentionnés dans le Rapport annuel de 2020 du Comité, et des fournisseurs américains de gaz naturel et d'électricité. Au Canada, certaines organisations de l'infrastructure essentielle sont des sociétés d'État. D'après les comportements connus liés aux cybermenaces étatiques les plus perfectionnées, il serait naïf de croire que ces organisations ne seraient pas éventuellement prises pour cible (ou ne sont pas *actuellement* des cibles), que ce soit à des fins d'espionnage ou de dégradation du système.

254. Dans le contexte que de telles organisations se trouvent dans la zone de protection de SPC et du CST, le Comité reconnaît que les organisations pourraient avoir des préoccupations sur le plan de la confidentialité au sujet du CST, en particulier la surveillance du trafic, des courriels ou de la navigation Web sur le réseau du système. À cet égard, le Comité prend note des conclusions du commissaire du CST, qui estime que les incidences liées à la confidentialité étaient très faibles en ce qui concerne les activités de cyberdéfense du CST menées au titre

d'une autorisation ministérielle, un facteur important à prendre en considération pour les organisations qui invoquent la confidentialité comme raison de rester à l'extérieur du cadre de cyberdéfense du gouvernement. Encore plus important pour le Comité est le choix auquel font face les sociétés d'État et les intérêts pertinents : se fier au gouvernement, au moyen d'un mécanisme règlementaire rigoureux doté de contrôles solides en matière de confidentialité et d'examen externe, pour protéger les données, les systèmes et les réseaux de l'exploitation et d'une dégradation possible, ou accepter la probabilité relativement élevée que des cyberacteurs perfectionnés compromettent les systèmes de ces organisations et volent les données qu'elles détiennent. Pour le Comité, les conséquences de ce choix sont claires : refuser les services de cyberdéfense du gouvernement équivaut à choisir de rendre les données et l'intégrité des systèmes vulnérables aux cybermenaces les plus avancées du monde.

Conclusion

255. Le gouvernement dépend grandement de son infrastructure numérique : elle lui permet de mener ses activités et de fournir des services à la population canadienne. Par conséquent, les systèmes et les réseaux du gouvernement contiennent d'importantes quantités de données qui intéressent les États étrangers, dont certains se servent de méthodes sophistiquées pour pénétrer dans les systèmes et voler les données. En outre, il se peut que certains de ces États ciblent de plus en plus l'intégrité même de ces systèmes en y installant des logiciels malveillants qui pourraient ensuite être activés afin de compromettre les systèmes ou les rendre inutilisables. Il s'agit d'une menace envers la sécurité nationale du Canada et la protection des renseignements personnels des Canadiennes et des Canadiens.

256. Au cours de la dernière décennie, le Canada a mis sur pied un système de cyberdéfense solide pour contrer cette menace. Ce système repose sur trois organisations : le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications. Ces organisations travaillent en étroite collaboration, entre elles et avec d'autres ministères, pour rendre la cyberinfrastructure du gouvernement plus sécuritaire et renforcer ses mesures de cyberdéfense. Sous sa forme la plus pure, le système peut se résumer en quelques éléments clés :

- les systèmes du gouvernement sont rassemblés à l'intérieur d'un seul périmètre;
- le périmètre comporte quelques points d'accès à Internet;
- ces points d'accès sont surveillés au moyen de capteurs avancés pouvant détecter et bloquer les menaces connues;
- des mécanismes de cyberdéfense sont superposés et comportent des capteurs spécialisés pouvant détecter et bloquer les menaces déployées sur des appareils personnels et des environnements infonuagiques;
- des anomalies relatives au trafic du réseau sont analysées en vue de cerner de nouvelles menaces, et cette information permet de continuellement mettre à jour les mesures de cyberdéfense*** qui servent à détecter et à bloquer les menaces;
- les ministères mettent continuellement à jour leurs appareils et leurs systèmes et y apportent des correctifs selon les directives, les conseils et l'orientation des trois organisations.

257. Le système de cyberdéfense en place n'a pas encore atteint cet idéal. Le fait que la gestion du système est de plus en plus horizontale et que les pouvoirs fondamentaux demeurent verticaux représente un obstacle global. Il en résulte donc d'importants écarts : les politiques du Conseil du Trésor visant à rendre les systèmes du gouvernement plus sécuritaires ne sont pas appliquées de manière uniforme; les ministères et les organismes conservent une certaine latitude à savoir s'ils adhèrent au cadre ou s'ils acceptent certaines technologies de défense; et un grand nombre d'organisations, notamment des sociétés d'État et possiblement des secteurs d'intérêt du gouvernement, ne respectent pas les politiques du Conseil du Trésor ou n'utilisent pas le cadre de cyberdéfense.

258. La menace que ces écarts présentent est indéniable. Les données des organisations qui ne sont pas protégées par le cadre de cyberdéfense courent un risque important. De surcroît, puisqu'on maintient une connectivité numérique avec les organisations faisant partie du cadre de cyberdéfense, les organisations qui ne sont pas protégées pourraient représenter un maillon faible des mesures de défense du gouvernement, créant un risque pour le gouvernement dans son ensemble. Le gouvernement connaît très bien ces obstacles. Le Comité s'attend à ce que son examen et ses recommandations contribuent à les résoudre.

Conclusions

259. Le Comité formule les conclusions suivantes :

C1. Les cybermenaces envers les systèmes et les réseaux du gouvernement présentent un risque important à la sécurité nationale et à la continuité des activités du gouvernement. Les États-nations constituent les auteurs de menace les plus sophistiqués, mais tout acteur ayant des intentions malveillantes et des capacités avancées expose les données et l'intégrité de l'infrastructure numérique du gouvernement à un risque. (Paragraphes 25 à 64)

C2. Le gouvernement a mis en place un cadre « horizontal » rigoureux dans le but de se défendre contre les cyberattaques. Le Secrétariat du Conseil du Trésor du Canada, Services partagés Canada et le Centre de la sécurité des télécommunications jouent un rôle essentiel dans ce cadre. Néanmoins, ce cadre horizontal semble de moins en moins compatible avec les pouvoirs « verticaux » en place de chaque ministère au titre de la *Loi sur la gestion des finances publiques*. (Paragraphes 95 à 213)

C3. Le gouvernement a établi des mécanismes de gouvernance clairs à l'appui de l'élaboration de politiques de cyberdéfense stratégiques, de la gestion efficace des initiatives liées à la sécurité des technologies de l'information qui touchent les activités de l'ensemble du gouvernement, ainsi que de l'intervention du gouvernement face aux cyberincidents. Le cadre a évolué au fil du temps en réponse aux changements apportés aux politiques, à l'appareil et à l'environnement de cybermenace du gouvernement. (Paragraphes 214 à 236)

C4. L'efficacité du cadre est affaiblie en raison de l'application non uniforme des responsabilités en matière de sécurité et de l'utilisation incohérente des services de cyberdéfense. Voici certaines des faiblesses :

- Les politiques du Conseil du Trésor relatives à la cyberdéfense ne sont pas appliquées de manière uniforme aux ministères et aux organismes. Par conséquent, les organisations n'exercent pas les mêmes responsabilités, exigences et pratiques, créant ainsi des lacunes dans la protection des réseaux du gouvernement contre les cyberattaques. (Paragraphes 95 à 125)
- Les sociétés d'État, et possiblement certains secteurs d'intérêt du gouvernement, constituent des cibles connues des acteurs étatiques, mais ne sont pas assujettis aux directives ou aux politiques liées au cyberenvironnement du Conseil du Trésor, et ne sont pas tenus de se procurer les services de cyberdéfense du gouvernement. Cette situation expose l'intégrité de leurs données et de leurs systèmes à un risque, et expose possiblement ceux du gouvernement à un risque important. (Paragraphes 251 à 254)
- Les services de cyberdéfense sont offerts de manière non uniforme. Même si Services partagés Canada offre certains services à 160 des 169 organisations fédérales, seuls 43 d'entre elles reçoivent l'ensemble complet de ses services. Le Centre de la sécurité des télécommunications fournit des services à l'appui de ceux de Services partagés Canada et dans le cadre d'ententes avec certaines organisations. Ce manque d'uniformité fait en sorte que ces organisations de même que le reste du gouvernement courent des risques, et limite l'efficacité globale du programme de cyberdéfense du CST. (Paragraphes 126 à 153)

Recommandations

260. Le Comité formule les recommandations suivantes :

R1. Le gouvernement doit continuer de renforcer son cadre visant à défendre ses réseaux contre les cyberattaques en s'assurant que ses pouvoirs et ses programmes de cyberdéfense sont modernisés à mesure qu'évoluent la technologie et d'autres facteurs pertinents, y compris de les harmoniser au cadre horizontal de la cyberdéfense qui est apparu au cours de la dernière décennie.

R2. Dans la mesure du possible, le gouvernement doit :

- appliquer les politiques du Conseil du Trésor relatives à la cyberdéfense de manière uniforme dans les ministères et organismes;
- étendre les politiques du Conseil du Trésor relatives à la cyberdéfense à toutes les organisations fédérales, y compris les petits organismes, les sociétés d'État et les autres organisations fédérales qui ne sont pas actuellement assujettis aux politiques et aux directives du Conseil du Trésor liées à la cyberdéfense;
- étendre les services avancés de cyberdéfense, notamment le Service Internet d'entreprise de Services partagés Canada et les capteurs de cyberdéfense du Centre de la sécurité des télécommunications, à toutes les organisations fédérales.

Réponses du gouvernement aux recommandations

Recommandation (R1) Le gouvernement doit continuer de renforcer son cadre visant à défendre ses réseaux contre les cyberattaques en s'assurant que ses pouvoirs et ses programmes de cyberdéfense sont modernisés à mesure qu'évoluent la technologie et d'autres facteurs pertinents, y compris de les harmoniser au cadre horizontal de la cyberdéfense qui est apparu au cours de la dernière décennie.
Réponse Approuvé. Sécurité publique Canada, le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada conviennent que le gouvernement doit continuer de renforcer son cadre servant à défendre ses réseaux des cyberattaques, en veillant à ce que les pouvoirs et les programmes connexes soient modernisés à mesure qu'évoluent les technologies et les autres facteurs pertinents. Sécurité publique Canada, le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada continueront de travailler en collaboration en vue d'harmoniser le cadre horizontal de cybersécurité, dans le but de veiller à ce qu'une structure de gouvernance appropriée soit en place pour faire progresser la politique de cybersécurité. Responsables : Sécurité publique Canada, en consultation avec le Centre de la sécurité des télécommunications et le Secrétariat du Conseil du Trésor du Canada.
Recommandation (R2.1) Dans la mesure du possible, le gouvernement doit : appliquer les politiques du Conseil du Trésor relatives à la cyberdéfense de façon uniforme dans les ministères et les organismes.
Réponse Approuvé. Le Secrétariat du Conseil du Trésor du Canada examinera le cadre stratégique du Conseil du Trésor afin de s'assurer que les politiques de cyberdéfense soient appliquées aussi uniformément que possible aux ministères et organismes. Cela comprend l'harmonisation de la portée de la *Politique sur la sécurité du gouvernement* avec la *Politique sur les services et le numérique*. Responsables : Secrétariat du Conseil du Trésor du Canada.
Recommandation (R2.2) Dans la mesure du possible, le gouvernement doit : étendre les politiques du Conseil du Trésor relatives à la cyberdéfense à toutes les organisations fédérales, y compris les petits organismes, les sociétés d'État et les autres organisations fédérales qui ne sont pas actuellement assujettis aux politiques et aux directives du Conseil du Trésor liées à la cyberdéfense.

Réponse

Approuvé. Le Secrétariat du Conseil du Trésor du Canada entreprendra un examen du cadre stratégique du Conseil du Trésor afin d'étudier et de cerner les options éventuelles permettant d'étendre les politiques du Conseil du Trésor relevant de la cyberdéfense à toutes les organisations fédérales, y compris les petits organismes, les sociétés d'État et les autres organisations fédérales qui ne sont pas actuellement assujettis aux politiques et aux directives du Conseil du Trésor en lien avec la cyberdéfense. Cet examen tiendra compte de la *Loi sur la gestion des finances publiques* et des pouvoirs attribués en vertu de celle-ci, ainsi que toute considération juridique.

Responsables : Secrétariat du Conseil du Trésor du Canada.

Recommandation (R2.3)

Dans la mesure du possible, le gouvernement doit :

étendre les services avancés de cyberdéfense, notamment le Service Internet d'entreprise de Services partagés Canada et les capteurs de cyberdéfense du Centre de la sécurité des télécommunications, à toutes les organisations fédérales.

Réponse

Approuvé. Le Secrétariat du Conseil du Trésor du Canada, en consultation avec Services partagés Canada et le Centre de la sécurité des télécommunications, convient que le gouvernement devrait étendre à l'ensemble des organisations fédérales ses services de cyberdéfense avancés, notamment le service Internet d'entreprise de Services partagés Canada et les capteurs de cyberdéfense du Centre de la sécurité des télécommunications, dans la mesure du possible.

Le Secrétariat du Conseil du Trésor du Canada continuera de renforcer ses mesures de cyberdéfense dans le cadre de ses modifications apportées à la *Politique sur les services et le numérique*, en s'appuyant notamment sur les procédures obligatoires décrites à l'annexe G : Norme relative aux configurations communes des services informatiques intégrés de la *Directive sur les services et le numérique*, qui sera publiée au début de 2022.

Services partagés Canada, en consultation avec le Secrétariat du Conseil du Trésor du Canada et le Centre de la sécurité des télécommunications, évalue, dans le cadre d'une étude financée, la situation actuelle des petits ministères et organismes (MPO) qui n'ont pas adopté le service Internet d'entreprise de Services partagés Canada. L'évaluation a pour but de produire une analyse de rentabilisation chiffrée décrivant le financement nécessaire pour migrer les MPO au service Internet d'entreprise de Services partagés Canada, d'éliminer le recours à des services Internet qui ne sont pas gérés par Services partagés Canada, et de fournir d'autres services intégrés (y compris les capteurs de cyberdéfense du Centre de la sécurité des télécommunications), ce qui permettra d'améliorer la sécurité des MPO et de réduire l'exposition aux menaces des réseaux intégrés du gouvernement.

Le Centre de la sécurité des télécommunications, en consultation avec le Secrétariat du Conseil du Trésor du Canada, étudiera les options permettant de fournir les capteurs de cyberdéfense du Centre de la sécurité des télécommunications à l'ensemble des organisations fédérales.

Responsables : Secrétariat du Conseil du Trésor du Canada, en consultation avec Services partagés Canada et le Centre de la sécurité des télécommunications.

Annexe A – Liste des témoins

Le Centre de la sécurité des télécommunications

- Dirigeant principal, Centre canadien pour la cybersécurité
- Dirigeant associé, Centre canadien pour la cybersécurité
- Directeur général, Capacités de cyberdéfense, Centre canadien pour la cybersécurité
- Directeur général, Gestion des incidents et atténuation des menaces, Centre canadien pour la cybersécurité
- Directeur général, Divulgation, politiques et examen
- Directeur général, Évolution du programme, Centre canadien pour la cybersécurité
- Directeur, Gestion des incidents et coordination opérationnelle, Centre canadien pour la cybersécurité
- Directrice, Politiques et examen

Le Secrétariat du Conseil du Trésor du Canada

- Dirigeant principal de l'information du Canada par intérim
- Directrice générale de la cybersécurité par intérim