Ministre de la Sécurité publique,
des Institutions démocratiques
et des Affaires intergouvernementales

Minister of Public Safety,
Democratic Institutions
and Intergovernmental Affairs

Ottawa, Canada K1A 0P8

L'honorable John MacKay, député
Président du Comité permanent de la défense nationale
Chambre des communes
Ottawa (Ontario)
K1A 0A4

Monsieur le Président,

À titre de ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales et au nom du gouvernement du Canada, je suis heureux de répondre au cinquième rapport du Comité permanent de la défense nationale intitulé La cyberdéfense du Canada. J'aimerais féliciter le Comité pour son travail visant à examiner cet important sujet.

Recommandation 1 : ***Que le gouvernement du Canada mette en place une plateforme multilatérale permanente pour susciter la collaboration et l'engagement des divers intervenants en matière de cybersécurité. La plateforme devrait avoir des objectifs fondés sur ceux du programme Industry 100 du Royaume-Uni. Elle devrait aussi former un espace collaboratif dans lequel les responsables de l'industrie et de la cybersécurité pourront se réunir pour échanger des informations et des pratiques exemplaires et établir des moyens de signaler les cyberattaques commises contre le secteur privé en vue d'améliorer le partage d'informations et de prévenir d'autres attaques.***

Le gouvernement appuie cette recommandation.

L'examen de mi-parcours de la Stratégie nationale de cybersécurité montre qu'un contexte numérique solide et sécuritaire dépendra d'une collaboration accrue avec des organisations fédérales et un large éventail d'intervenants nationaux et internationaux. Le rapport de l'examen recommande que les principaux intervenants nationaux renforcent leur collaboration pour veiller à ce que les systèmes canadiens soient protégés contre les menaces existantes et nouvelles.

Le gouvernement du Canada reconnaît que la protection de la cybersécurité du Canada nécessite une collaboration entre tous les ordres de gouvernement et avec l'industrie. Il faut créer et tirer parti de nouvelles relations significatives avec l'industrie pour trouver des solutions aux défis du Canada en matière de cybersécurité.

Dans le cadre de la Stratégie nationale de cybersécurité de 2018, le gouvernement du Canada a créé le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) du Centre de la sécurité des télécommunications (CST), qui est la source unique et unifiée en matière de conseils d'experts techniques, d'orientations et de services pour le Canada. Pour remplir ce mandat, le Centre pour la cybersécurité a tissé des liens étroits avec des intervenants de tout le Canada dans le secteur privé, le milieu universitaire et d'autres niveaux de gouvernement, et organise de nombreuses plateformes multipartites aux fins de collaboration. Par exemple, le Centre pour la cybersécurité organise toutes les deux semaines une séance d'information conjointe sur les menaces avec des représentants de divers secteurs (p. ex. la santé, le milieu universitaire, les transports, l'énergie, les fournisseurs de services Internet, la base industrielle de la Défense et les sociétés d'État) et des provinces et des territoires. Par ailleurs, certains secteurs font l'objet d'appels qui sont propres à leur domaine.

Le Centre pour la cybersécurité a également commencé à organiser des ateliers sectoriels sur place pour rencontrer les professionnels et les cadres supérieurs de la sécurité des TI pour cerner les domaines préoccupants sur le plan de la cybersécurité et trouver des solutions pour atténuer ces préoccupations. À titre d'exemples récents, notons des séances d'information sectorielles ainsi que la Table ronde fédérale, provinciale et territoriale et l'atelier de l'Association canadienne du gaz et de la Société indépendante d'exploitation du réseau électrique, tous les deux organisés au Centre pour la cybersécurité.

L'équipe des Partenariats du Centre pour la cybersécurité a élaboré une stratégie d'échange des analystes, semblable au programme Industry 100 du Royaume-Uni, et elle est prête à réaliser le premier projet pilote avec un partenaire du secteur financier.

Le Service canadien du renseignement de sécurité (SCRS) contribue à divers efforts de collaboration au sein du milieu de la cybersécurité pour remplir son mandat consistant à réduire les menaces contre la sécurité nationale du Canada et à enquêter sur celles-ci. Le SCRS procède aux notifications à la victime dans les cas de cyberincidents liés à la sécurité nationale, mène les discussions rétrospectives avec les victimes avec les entités visées par des cyberattaques ou des ingérences et collabore dans le cadre d'efforts visant à échanger des renseignements avec des pays alliés et des ministères fédéraux au Canada.

Recommandation 2 : ***Que le gouvernement du Canada investisse dans la cybersécurité de sa propre infrastructure réseau et évalue de façon exhaustive les mesures supplémentaires nécessaires pour renforcer les systèmes du gouvernement et l'infrastructure réseau des tierces parties qui hébergent ses données, afin d'assurer la sécurité de ses données critiques*.**

Le gouvernement appuie cette recommandation.

Le gouvernement travaille continuellement pour renforcer la cybersécurité de ses services en prévenant les attaques par la mise en œuvre de mesures de sécurité et de protection, l'identification des cybermenaces et des vulnérabilités, ainsi que par la préparation à tous les types de cyberincidents et la réponse à ceux-ci en vue de mieux protéger le Canada et les Canadiens. Au fur et à mesure de l'évolution du contexte des cybermenaces, le gouvernement évalue sa posture en matière de cybersécurité et détermine les investissements nécessaires pour suivre le rythme.

La Norme sur les configurations courantes des services de la technologie de l'information intégrée, établi en vertu de la Politique sur les services et le numérique et la Directive sur les services et le numérique, donne une orientation aux ministères sur la gestion des éléments de TI essentiels aux services de TI d'entreprise.

De plus, le gouvernement du Canada a un processus d'intégrité de la chaîne d'approvisionnement qui garantit qu'aucun équipement, logiciel ou service non fiable n'est acheté par Services partagés Canada (SPC) et utilisé dans la prestation et le soutien des services du gouvernement du Canada.

Enfin, conformément à la Politique sur la sécurité du gouvernement, les ministères et les organismes doivent s'assurer que les exigences de sécurité liées aux contrats et autres ententes, qui comprennent le recours à des services tiers pour héberger les données du gouvernement du Canada, sont déterminés et documentés, et que les mesures de sécurité connexes sont mises en œuvre et surveillées à chaque étape du processus d'octroi de contrats ou d'établissement d'ententes, afin de fournir une assurance raisonnable que l'information, les particuliers, les actifs et les services liés au contrat ou à l'entente sont protégés de façon adéquate.

Le Centre pour la cybersécurité du CST a élaboré et déployé des services de cybersécurité qui ont joué un rôle déterminant dans la défense des réseaux des institutions fédérales depuis plus d'une décennie. L'ensemble de services comprend des solutions de détection et de réponse dans le réseau, aux points terminaux et dans le nuage, intégrées dans une plateforme analytique. Environ 95 ministères et organismes sont protégés par le service de détection et de réponse dans le réseau déployé dans les passerelles Internet et infonuagiques de SPC. Le Centre pour la cybersécurité a

également effectué 90 déploiements de son service de détection et de réponse dans le nuage.

Le Centre pour la cybersécurité poursuit le déploiement de ses services de sécurité dans d'autres institutions fédérales. Par exemple, dans le cadre d'une initiative dirigée par SPC et le CST pour intégrer de petits ministères et organismes à des services de sécurité d'entreprise, 43 petits ministères et organismes feront une transition vers les passerelles Internet d'entreprise du gouvernement du Canada et par la même occasion bénéficieront de la solution de détection et de réponse dans le réseau du Centre pour la cybersécurité.

Recommandation 3 : ***Que le gouvernement du Canada collabore avec ses partenaires du Groupe des cinq pour adopter une norme CMMC (Cybersecurity Maturity Model Certification) compatible avec celles de ses partenaires et reconnue par ces derniers afin d'éviter que l'utilisation d'une norme distincte au Canada ne défavorise les entreprises de l'industrie de la défense canadienne par rapport à celles des autres pays membres du Groupe des cinq.***

Le gouvernement appuie cette recommandation.

Pour renforcer la protection des renseignements non classifiés détenus par les fournisseurs du secteur de la défense du Canada, le gouvernement du Canada met en place le Programme canadien de certification en cybersécurité, qui instaurera des exigences obligatoires en matière de certification en cybersécurité dans certains contrats de défense.

L'amélioration de la résilience en matière de cybersécurité de la base industrielle de la défense du gouvernement du Canada renforcera les objectifs du Plan d'action national en matière de cybersécurité et de la Stratégie nationale de cybersécurité du Canada.

Le nouveau programme reflétera étroitement le programme de CMMC des États-Unis, pour faire en sorte que les entrepreneurs du secteur de la défense faisant affaire avec le Canada et les États Unis n'auront qu'à être certifiés qu'en vertu d'un seul régime.

De plus, à plus long terme, le gouvernement du Canada se penchera sur l'harmonisation possible avec d'autres partenaires du Groupe des cinq et des proches partenaires, afin d'améliorer l'accès des entreprises canadiennes aux possibilités de marchés internationaux pour lesquels une certification en cybersécurité est exigée.

Recommandation 4 : ***Que le gouvernement du Canada offre des incitations (p. ex. des crédits d'impôt) aux entreprises pour les encourager à adopter des mesures de cybersécurité, comme le programme de certification « Cybersécurité Canada » créé par ISDE et le CST pour les petites et moyennes entreprises.***

Le gouvernement prend note de cette recommandation.

Innovation, Sciences et Développement économique Canada (ISDE) aide les petites et moyennes entreprises (PME) à adopter des mesures de cybersécurité dans le cadre du programme CyberSécuritaire Canada, qui donne aux PME des moyens peu coûteux de démontrer leur conformité aux contrôles de cybersécurité de base, augmentant ainsi le niveau de confiance de leurs clients et de leurs partenaires.

Le programme vise à :

- hausser le niveau de base en matière de cybersécurité des PME au Canada;
- accroître la confiance des consommateurs dans l'économie numérique;
- promouvoir la normalisation internationale;
- mieux positionner les PME face à la concurrence mondiale.

En ce qui a trait aux mesures fiscales, les PME qui font des investissements en capital, y compris ceux liés à la cybersécurité, peuvent déjà bénéficier de diverses mesures de déduction pour amortissement accéléré et d'autres mesures fiscales mises en place par le gouvernement. Il est notamment question de l'incitatif à l'investissement accéléré mis en place en 2018, qui accorde une déduction fiscale bonifiée pour la première année pour atteindre jusqu'à trois fois le taux normal, ainsi que de la mesure temporaire introduite dans le budget de 2021 qui permet aux petites entreprises d'amortir immédiatement jusqu'à 1,5 million de dollars en nouveaux investissements admissibles. Il est également noté que les logiciels qui ne sont pas considérés des logiciels d'exploitation sont en général admissibles à une déduction pour amortissement de 100 pour cent. De plus, le budget de 2022 comprend une élimination plus progressive de la déduction accordée aux petites entreprises, où l'accès est complètement éliminé lorsque le capital imposable atteint 50 millions de dollars, plutôt que 15 millions de dollars (dans le cadre de l'ancien régime). Cette mesure permet à un plus grand nombre de moyennes entreprises de bénéficier du taux réduit et augmente le montant des revenus admissible au taux réduit, ce qui mène à d'autres économies d'impôts pouvant être réinvesties dans l'entreprise.

Recommandation 5 : ***Que le gouvernement du Canada accélère le renouvellement de la stratégie nationale de cybersécurité du pays et qu'il soumette cette stratégie à un examen périodique pour pouvoir la mettre à jour au rythme de l'évolution des cybermenaces.***

Le gouvernement prend note de cette recommandation.

Dans sa lettre de mandat de 2021, le premier ministre a chargé le ministre de la Sécurité publique de collaborer avec les ministres de la Défense nationale, des Affaires étrangères, de l'Innovation, des Sciences et de l'Industrie, ainsi que d'autres ministres, afin d'élaborer et de mettre en œuvre une nouvelle Stratégie nationale de cybersécurité, qui exprimerait la stratégie à long terme du Canada pour protéger sa sécurité nationale et son économie, dissuader les auteurs de cybermenaces et promouvoir l'adoption, sur la scène internationale, d'un comportement fondé sur les normes dans le cyberespace. À la suite de la publication de l'évaluation de mi-parcours en 2022, Sécurité publique Canada travaille en collaboration avec ses partenaires pour respecter cet engagement.

Recommandation 6 : ***Que le gouvernement du Canada maintienne son dialogue avec les propriétaires et les exploitants d'infrastructures essentielles tels que les municipalités; les gouvernementaux provinciaux, territoriaux et autochtones; et les exploitants du secteur privé comme les sociétés de services publics, et que ces efforts soient officialisés afin qu'il y ait un dialogue constant sur les menaces éventuelles et sur les bonnes pratiques.***

Le gouvernement appuie cette recommandation.

Sous les auspices de la Stratégie nationale sur les infrastructures essentielles et des plans d'action connexes, le gouvernement continue de dialoguer avec la communauté élargie des propriétaires et des exploitants d'infrastructures essentielles au sujet des menaces potentielles et des pratiques exemplaires.

Ce dialogue se tient dans de nombreux formats, y compris dans des organes permanents d'intervenants publics et privés comme le Forum national intersectoriel et les réseaux sectoriels, les réunions directes avec les intervenants des secteurs public et privé, des consultations en ligne ciblées et des mémoires envoyés par courriel. Les perspectives obtenues dans ces discussions servent à orienter l'élaboration d'une vision tournée vers l'avenir pour la résilience des infrastructures essentielles.

Recommandation 7 : ***Que le gouvernement du Canada examine la Loi sur le Service canadien du renseignement de sécurité pour s'assurer que le Service dispose des outils juridiques dont il a besoin pour s'adapter aux réalités modernes de l'ère numérique et pour suivre le rythme des progrès technologiques et de la perpétuelle évolution des menaces qui planent sur la cybersécurité au Canada.***

Le gouvernement appuie cette recommandation.

Le rythme et la vitesse des progrès technologiques ont engendré un environnement opérationnel et technologique complexe. Les acteurs étatiques se servent de plus en plus des technologies numériques pour faire progresser leurs objectifs stratégiques, politiques, économiques et militaires, et ce, souvent au détriment de la sécurité nationale du Canada. Les cyberacteurs étatiques et non étatiques continuent également à représenter une menace pour la sécurité nationale, les infrastructures essentielles et les institutions fondamentales du Canada.

Pour faire face à cette évolution, le gouvernement évalue continuellement le cadre législatif de la sécurité nationale du Canada, y compris la Loi sur le Service canadien du renseignement de sécurité (SCRS). Ainsi, le gouvernement veille à ce que ce cadre donne au SCRS, ainsi qu'à d'autres ministères et organismes, les outils dont ils ont besoin afin d'enquêter et contrer efficacement les cybermenaces pour la sécurité du Canada.

Recommandation 8 : ***Que le gouvernement du Canada collabore avec les provinces et l'industrie pour créer des exigences obligeant les exploitants d'infrastructures essentielles critiques du secteur privé à signaler les attaques par rançongiciel et les atteintes à la cybersécurité au Centre canadien pour la cybersécurité dans un délai donné; qu'il mette en place des mécanismes appropriés pour protéger les victimes de cyberattaques et, ainsi, atténuer ou éliminer les facteurs qui les dissuadent de signaler ces attaques; et que le gouvernement incite les propriétaires et exploitants d'infrastructures critiques à coopérer avec les autorités compétentes pour déceler, signaler et éliminer les vulnérabilités.***

Le gouvernement appuie cette recommandation.

Le 14 juin 2022, le ministre de la Sécurité publique a déposé le projet de loi C-26, Loi concernant la cybersécurité, à la Chambre des communes. La partie 2 du projet de loi prévoit l'adoption de la Loi sur la protection des cybersystèmes essentiels (LPCE), qui établirait un cadre réglementaire visant à renforcer la cybersécurité de base pour les services et les systèmes essentiels à la sécurité nationale et à la sécurité publique. Ce projet de loi vise également à accroître l'échange de renseignements sur les cybermenaces.

La LPCE prévoit l'obligation pour les exploitants désignés de quatre secteurs des infrastructures essentielles de compétence fédérale – finances, télécommunications, énergie et transports – de signaler au CST les cyberincidents qui touchent leurs cybersystèmes critiques. Le signalement obligatoire des incidents donnerait au Centre pour la cybersécurité du CST une vue d'ensemble des menaces et des vecteurs au Canada, et permettrait au Centre de diffuser des renseignements essentiels sur les menaces à tous les exploitants de cyberinfrastructures au Canada, notamment des conseils techniques et des suggestions de mesures à prendre afin de contenir la

compromission, de se remettre de l'incident ou de prévenir d'autres incidents. Ainsi, la LPCE vise à améliorer la posture de cybersécurité globale du Canada.

Cette mesure législative peut servir de modèle pour les provinces, les territoires et les municipalités en vue de contribuer à sécuriser les infrastructures essentielles qui ne relèvent pas de la compétence fédérale. Dans les secteurs où les mêmes normes sont utilisées dans l'ensemble des administrations, il est possible que la LPCE contribue à renforcer les capacités et l'expertise à l'appui de systèmes plus résilients dans l'ensemble des secteurs et du pays.

Reconnaissant que de nombreux services et systèmes désignés conformément à la LPCE dépendent d'autres cybersystèmes qui ne relèvent pas de la compétence fédérale ou sont interconnectés avec eux, le gouvernement du Canada continuera à discuter avec les provinces et les territoires de manière à mieux protéger les cybersystèmes du Canada au moyen d'un cadre exhaustif et collaboratif de protection de la cybersécurité au Canada.

Bien que le projet de loi C-26 vise à rendre obligatoire le signalement des cyberincidents de sécurité, le Centre pour la cybersécurité continue d'encourager leur signalement volontaire. Les responsables des opérations d'infrastructures essentielles, d'entreprises et d'organismes gouvernementaux, ainsi que les professionnels de l'informatique peuvent signaler les cyberincidents directement au Centre pour la cybersécurité en consultant le site Web cyber.gc.ca, en écrivant à l'adresse contact@cyber.gc.ca ou en téléphonant au 1-833-CYBER-88. Les renseignements fournis au Centre pour la cybersécurité, y compris les données personnelles, sont conservés en toute sécurité, et leur accès est strictement limité. Le signalement contribue à la sécurité en ligne du Canada et de la population canadienne en permettant au Centre pour la cybersécurité de fournir des conseils, des orientations et des services en matière de cybersécurité.

Le Centre pour la cybersécurité du CST continue de travailler en collaboration avec les partenaires de l'industrie, y compris les partenaires gouvernementaux et non gouvernementaux, pour échanger de l'information afin de veiller à ce qu'ils aient accès aux experts et aux ressources en cybersécurité dont ils ont besoin pour se défendre contre les cyberactivités malveillantes et se remettre de celles-ci, et que les normes de cybersécurité soient respectées et fassent l'objet de rapports.

En outre, au cours de ses appels d'information sur les menaces qui ont lieu aux deux semaines, le Centre pour la cybersécurité discute directement avec les intervenants des avantages du signalement, présente les statistiques sur le signalement par secteur et encourage tous les partenaires à signaler les incidents, peu importe leur ampleur ou le besoin du soutien du Centre pour la cybersécurité.

Le gouvernement du Canada continue d'examiner la question du signalement des cyberincidents pour comprendre les obstacles et les facteurs dissuasifs au signalement. Par exemple, l'Enquête canadienne sur la cybersécurité et le cybercrime réalisée par Sécurité publique Canada interroge les entreprises pour comprendre les répercussions des cybercrimes sur la fonction publique et les sociétés d'État du Canada, notamment les aspects comme l'investissement dans les mesures de cybersécurité, la formation en matière de cybersécurité, le nombre de cyberincidents de sécurité et les coûts associés aux interventions en cas d'incident. La version actuelle de l'enquête comporte des questions sur le signalement des cyberincidents au gouvernement du Canada pour mieux comprendre les facteurs qui motivent ou incitent les signalements.

Recommandation 9 : ***Que le gouvernement du Canada collabore avec ses partenaires de l'industrie pour améliorer la cybersécurité au stade de la conception du matériel informatique et des logiciels afin de délester les utilisateurs d'une partie du fardeau d'assurer la cybersécurité.***

Le gouvernement appuie cette recommandation.

Le Canada effectue d'importants échanges commerciaux dans le domaine du matériel informatique et des logiciels. Les partenaires de l'industrie, tant au pays qu'à l'étranger, devront faire partie de la solution. Le gouvernement du Canada travaille en collaboration avec les pays alliés pour améliorer le matériel informatique et les logiciels servant à la cybersécurité afin de faire passer le fardeau de la sécurisation des réseaux aux utilisateurs individuels de ces produits aux fabricants de matériel informatique et aux développeurs de logiciels servant à la cybersécurité.

À cet égard, le Centre pour la cybersécurité s'est joint à la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis, au FBI et à d'autres partenaires internationaux aux vues similaires pour publier conjointement les lignes directrices Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-By-Design and Default qui exhortent les fabricants à prendre de façon urgente les mesures nécessaires pour livrer des logiciels et du matériel informatique qui enlèvent le fardeau des risques de cybersécurité aux consommateurs, qu'il s'agisse de particuliers ou d'organisations et encouragent plutôt les fabricants de produits technologiques à concevoir des produits sécuritaires dès leur conception et par défaut.

Ces lignes directrices premières de leur genre devraient, espère-t-on, encourager les investissements et le changement de culture nécessaires au renforcement de la cybersécurité dans le futur. Un futur où la sécurité sera intégrée dès le début, de l'étape de conception jusqu'au développement du produit et non pas seulement après coup (sécuritaire dès la conception), et où les produits peuvent être utilisés en toute sécurité dès leur sortie de l'emballage et ne nécessitent que peu ou pas de changements de configuration et disponibles sans coûts supplémentaires (sécuritaire par défaut). Les produits sécuritaires dès leur conception font de la sécurité des consommateurs une exigence fondamentale de l'entreprise, et non seulement une caractéristique technique. Cela fera en sorte que la prévention des cyberintrusions causées par des défauts de conception n'incombe pas aux Canadiens.

De plus, les lignes directrices encouragent les fabricants à fabriquer leurs produits de façon à ce que les consommateurs n'aient pas constamment à assurer la surveillance, à effectuer des mises à jour de routine ou à limiter les dégâts à leurs systèmes pour atténuer les cyberintrusions.

Les lignes directrices décrivent également les trois principes fondamentaux pour orienter ce travail : 1) s'approprier les résultats en matière de sécurité; 2) adopter la transparence et la responsabilité; et 3) créer une structure organisationnelle appropriée pour permettre aux fabricants de logiciels de prendre l'engagement, au niveau de la direction, d'accorder la priorité à la sécurité en tant qu'élément clé du développement de produits.

En plus de ce travail, le gouvernement du Canada continue également à surveiller les lignes directrices sur l'étiquetage des appareils et la cybersécurité de l'Internet des objets (IdO) qui sont en cours d'examen dans d'autres administrations partenaires, notamment les États-Unis (Cyber Trust Mark) et l'Union européenne (Loi sur la cyberrésilience), ainsi que de leurs répercussions sur les producteurs et des consommateurs canadiens.

Recommandation 10 : ***Que le gouvernement prenne des mesures pour maintenir au pays la propriété intellectuelle des technologies de l'information conçues au Canada, y compris des mesures de commercialisation pour préserver la propriété canadienne des cybertechnologies.***

Le gouvernement du Canada est en accord avec cette recommandation.

Placer les innovateurs canadiens dans une position qui leur permet de protéger la propriété intellectuelle (PI) relative aux technologies de l'information et d'en tirer parti de façon efficace s'avère de plus en plus important à mesure que la dépendance aux réseaux et appareils numériques dans les activités des entreprises et des individus gagne en importance. Par conséquent, le gouvernement appuie les innovateurs qui cherchent à accroître leur savoir-faire en matière de PI en protégeant leur PI et en

prenant des décisions stratégiques en la matière en fonction des besoins de leur entreprise. Par exemple, la Stratégie en matière de propriété intellectuelle (Stratégie en matière de PI) a été lancée en 2018 pour aider les entreprises, les créateurs, les sous-traitants et les innovateurs canadiens à mieux comprendre et protéger la PI grâce à trois piliers : sensibilisation à la PI, éducation et conseils; outils stratégiques en PI pour la croissance; législation en matière de PI. Ces initiatives s'accompagnent de programmes subséquents comme ÉleverlaPI et Aide à la PI, qui offrent du soutien pour la prise de décisions stratégiques relatives à la PI. De plus, le programme CanExport pour les PME aide les petites et moyennes entreprises à élaborer des occasions d'exportation pour les produits et services, notamment en finançant le processus de soumission pour les protections de la PI dans les marchés internationaux.

Le gouvernement a également investi dans des occasions de commercialisation, notamment dans la formation du Réseau d'innovation pour la cybersécurité (RIC). Le RIC, dirigé par le Consortium national pour la cybersécurité (CNS), contribuera à favoriser un écosystème national de cybersécurité solide en augmentant la collaboration entre le secteur académique et le secteur privé. Le RIC contribuera à appuyer la recherche et le développement dans le domaine de la cybersécurité, à accélérer la commercialisation des produits, des services et des processus liés à la cybersécurité ainsi qu'à appuyer le perfectionnement de talents hautement qualifiés au Canada. Pour être en position de prendre les mesures appropriées pour protéger la PI qui découle des activités du RIC, le CNS mettra en œuvre une stratégie de PI dans le but de définir des politiques claires sur la création, l'utilisation, les droits, la commercialisation et l'application de toute PI liée aux activités du réseau et l'accès à cette PI pour maximiser les avantages économiques et l'innovation pour le Canada. Les objectifs principaux de la Stratégie de PI sont les suivants :

- la création de la PI dans le cadre de l'intensification de la recherche et du développement dans l'écosystème de cybersécurité du Canada;
- la propriété des droits de PI pour permettre aux innovateurs en cybersécurité de commercialiser leurs connaissances et leurs produits;
- le partage de connaissances sur la PI au sein du réseau pour appuyer la gestion de la PI et, au besoin, partager de la PI entre les membres du CNS;
- la protection de la PI par la promotion de l'utilisation des outils et services juridiques grâce auxquels il sera possible de défendre les droits de PI de façon juste et sécuritaire.

De plus, le CNS mettra en œuvre un plan organisationnel de cybersécurité pour assurer la cyberrésilience et protéger les réseaux de données et la PI d'éventuels incidents de cybersécurité.

Recommandation 11 : ***Que le gouvernement du Canada, en collaboration avec la société civile, l'industrie et les pays alliés, développe davantage de ressources pour faire face aux opérations étrangères de guerre cognitive – dont la mésinformation, la désinformation et la malinformation – afin de mieux protéger les Canadiens et de veiller à ce que le public ait accès à de l'information exacte.***

Le gouvernement du Canada appuie cette recommandation.

Le gouvernement du Canada s'implique déjà dans la conception de ressources en collaboration avec la société civile et l'industrie par l'entremise de l'Initiative de citoyenneté numérique. Environ 100 projets ont été financés depuis la création du programme en 2019 pour appuyer des campagnes visant à améliorer les connaissances sur les médias numériques, et ce, pour que le public ait accès à de l'information exacte.

Compte tenu du fait que la mésinformation et la désinformation, entre autres vecteurs d'ingérence étrangère, menacent la démocratie et compromettent la sécurité nationale, les dirigeants du G7 se sont engagés à mettre sur pied le mécanisme de réponse rapide du G7 (MRR du G7) à l'occasion du Sommet du G7 à Charlevoix en 2018. Dirigé de façon continue par le Canada, le MRR du G7 a le mandat de repérer les menaces étrangères pour la démocratie et de les contrer. Depuis sa création, le MRR du G7 a avant tout été axé sur la lutte à la manipulation de l'information et l'ingérence étrangère; un ensemble d'activités malveillantes en ligne, y compris la désinformation. En plus de coordonner le MRR du G7, AMC surveille également les signes éventuels d'ingérence étrangère sur les priorités clés du gouvernement dans l'environnement de l'information numérique. Cette surveillance est notamment exercée lors des élections par l'entremise du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Parmi ces efforts, on compte la création d'une équipe autonome axée sur la lutte contre la désinformation russe, laquelle a été annoncée par le premier ministre l'été dernier (2022).

Le CST et son Centre pour la cybersécurité ont publié des conseils et des lignes directrices qui expliquent comment repérer la mésinformation et la désinformation. Ils ont également publié des renseignements sur les médias sociaux dans le cadre des efforts du gouvernement du Canada pour informer la population canadienne des façons d'éviter la propagation de désinformation et de se protéger de la désinformation. Le CST continue de fournir au gouvernement du Canada l'information la plus complète possible sur les priorités du Canada en matière de renseignement, ce qui contribue à maintenir la sûreté, la sécurité et la prospérité du Canada.

Certains États étrangers utilisent l'ingérence contre une panoplie d'intérêts canadiens et tirent parti d'outils cybernétiques et de plateformes en ligne sophistiqués pour diffuser leur mésinformation ou leur désinformation. Le SCRS conseille le gouvernement du Canada sur la menace d'ingérence étrangère et déploie des efforts considérables pour informer et sensibiliser la population canadienne à cet égard. Le SCRS a présenté l'état de l'ingérence étrangère dans tous ses rapports annuels publics au cours des 30 dernières années, et a publié des rapports non classifiés, comme le rapport intitulé « Ingérence étrangère et vous ». Ces rapports et d'autres ressources accessibles au public sur l'ingérence étrangère sont publiés dans plusieurs langues étrangères afin de s'assurer que les membres des collectivités vulnérables ont accès aux informations sur les menaces dans la langue de leur choix. Étant un membre actif du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, le SCRS collabore avec ses partenaires fédéraux pour lutter contre l'ingérence étrangère ciblant les élections canadiennes. Le SCRS s'associe également avec nos alliés pour élaborer conjointement des produits destinés à conseiller le gouvernement sur les menaces à la sécurité nationale (notamment la cybersécurité) et à déterminer l'attribution, les motivations et les capacités des auteurs de menaces. Dans l'avenir, il est fondamental que le SCRS renforce sa collaboration avec la société civile, l'industrie et ses alliés afin de recueillir des renseignements utilisables, de lutter contre des menaces à la sécurité en constante évolution (qui touchent les collectivités et la population canadienne) et d'éclairer les avis donnés par le SCRS au gouvernement du Canada.

Recommandation 12 : ***Que le gouvernement du Canada veille à ce que les ministères et les contrats fédéraux fassent l'objet d'une vérification afin de confirmer que les normes de sécurité de l'information sont bien respectées par le gouvernement et les sous-traitants.***

Le gouvernement prend note de cette recommandation.

L'ensemble de politiques liées à la sécurité de l'information pour les ministères et les organismes et les politiques liées à l'attribution de contrats et à d'autres types d'ententes renferment des instructions détaillées sur la gestion de la sécurité de l'information. Ces politiques établissent clairement des responsabilités en ce qui a trait à la mise en œuvre des directives et à la vérification de la conformité.

Par exemple, la Politique sur la sécurité du gouvernement (PSG) du Conseil du Trésor établit des responsabilités claires pour les ministères responsables, les organismes chargés de la sécurité et les organisations des services d'entreprise internes. Les dirigeants principaux de la sécurité des ministères ont un rôle unique selon la PSG qui leur permet d'effectuer des activités de sécurité et de présenter des rapports indépendants à leurs administrateurs généraux, notamment en ce qui concerne la conformité à la politique et aux

directives. De plus, la sécurité ministérielle compte parmi les secteurs de gestion évalués par le Cadre de responsabilisation de gestion.

En plus des vérifications de gestion du Bureau du vérificateur général du Canada, qui relève du Parlement, tous les grands ministères possèdent des fonctions de vérification internes. Ces fonctions sont indépendantes des ministères responsables et ont pour mandat d'évaluer les secteurs du risque, du contrôle et de la gouvernance, notamment les risques liés à la sécurité de la TI en fonction de leur évaluation des risques et des priorités. De même, la division des opérations de vérification du Bureau du contrôleur général effectue des vérifications horizontales périodiques sur une gamme de secteurs de risque au fil du temps. Plusieurs mobilisations horizontales liées à la sécurité de la technologie de l'information ont été effectuées au cours des dernières années.

Les risques pour la sécurité continueront d'être pris en compte avec d'autres risques et priorités du gouvernement dans le cadre d'une planification pluriannuelle de l'audit interne axée sur les risques ainsi que de mises à jour annuelles des plans de sécurité ministériels.

Recommandation 13 : ***Que le gouvernement du Canada collabore avec les provinces en vue d'établir des normes de cybersécurité de base pour les petites et moyennes entreprises, et qu'il offre des incitations aux entreprises pour les encourager à adopter les mesures de sécurité les plus récentes qui les protégeront contre les attaques à risque élevé, mais peu probables, ainsi que contre les attaques à faible risque, mais fréquentes.***

Le gouvernement du Canada prend note de cette recommandation.

La cybersécurité est une responsabilité partagée : la population canadienne, le gouvernement, le secteur privé et nos partenaires étrangers ont tous un rôle important à jouer en la matière. Le gouvernement du Canada continue à travailler pour améliorera coordination et la collaboration entre les systèmes fédéral, provinciaux et territoriaux, y compris en ce qui concerne la cybersécurité. Avec des engagements aux niveaux ministériel et des fonctionnaires, les homologues fédéraux, provinciaux et territoriaux partagent des observations sur le contexte actuel des menaces à la cybersécurité et d'autres approches en matière de politique en vue d'améliorer la cyber sécurité des canadiens et des entreprises canadiennes.

Pour que les petites et moyennes entreprises aient accès à des ressources pour bonifier leur cybersécurité et leur résilience générale, le CST et son Centre pour la cybersécurité ont contribué à élaborer et à offrir des conseils et des directives personnalisées, des programmes d'apprentissage (dont le programme Pensez cybersécurité, une campagne nationale de sensibilisation pour sensibiliser les Canadiens à la cybersécurité) et des partenariats élargis au sein du gouvernement du Canada.

De plus, le Centre pour la cybersécurité de CST conçoit et met régulièrement à jour les conseils et les directives adaptés aux petites et moyennes entreprises. Parmi les ressources, on compte entre autres les contrôles de sécurité de base pour les petites et moyennes entreprises, les meilleures mesures de cybersécurité pour accroître la sécurité de ces entreprises, le Guide sur les rançonlogiciels (un document qui définit ce qu'est un rançonlogiciel et présente les motivations et avantages pour les auteurs de menace ainsi que les mesures de prévention des cyberattaques), une explication des menaces pour la chaîne d'approvisionnement et une sensibilisation à l'espionnage industriel.

Le CST continuera de travailler avec les petites et moyennes entreprises et de leur fournir des conseils et des orientations à jour pour qu'elles soient en mesure de mettre en place les mesures de sécurité cruciales et nécessaires pour assurer la sécurité de leur organisation.

Recommandation 14 : ***Qu'il y ait une plus grande collaboration entre le gouvernement du Canada et l'industrie canadienne de la défense et de la sécurité pour renforcer l'infrastructure offensive des cyberopérations offensives et défensives à un moment où des États malveillants manifestent une audace croissante.***

Le gouvernement du Canada soutient cette recommandation.

En vertu de la Loi sur le Centre de la sécurité des télécommunications, le CST peut réaliser des cyberopérations défensives ou actives à l'étranger pour aider à protéger le Canada et les Canadiens. Les cyberopérations défensives permettent de défendre le Canada contre des cybermenaces de l'étranger en intervenant en ligne. Ce pouvoir peut aussi servir à défendre des systèmes que le ministre de la Défense nationale a désignés comme étant importants pour le gouvernement du Canada, notamment : réseaux énergétiques, réseaux de télécommunications, bases de données des soins de santé, systèmes bancaires et infrastructure électorale. Les cyberopérations actives permettent au CST d'intervenir en ligne pour perturber les capacités des menaces étrangères pour le Canada, comme les groupes terroristes étrangers, les cybercriminels étrangers, les services de renseignement ennemis et les pirates parrainés par l'État. Les menaces que perturbe le CST doivent viser les affaires internationales, la défense ou la sécurité.

Le CST et son Centre pour la cybersécurité travaillent aussi à contrer les cyberactivités malveillantes des acteurs d'États hostiles en partageant de l'information sur les cybermenaces et des conseils en matière d'atténuation aux responsables de ces réseaux critiques. Ils peuvent aussi déployer, sur demande, des outils de cybersécurité pour contribuer à défendre ces réseaux.

Plus tôt cette année, le Centre pour la cybersécurité du CST s'est mis à communiquer avec l'Infrastructure industrielle de défense (IID) et à la consulter. Ensemble, ils intègrent des partenaires de ce secteur aux services du Centre pour la cybersécurité et participeront à des ateliers sur la cybersécurité avec certaines entités petites et moyennes de l'IID. Le Centre pour la cybersécurité a participé à CANSEC (une conférence organisée par l'Association des industries canadiennes de défense et de la sécurité) pour la première fois cette année. L'équipe travaille également avec d'autres ministères du gouvernement du Canada à l'élaboration et à la mise en œuvre de la certification du modèle de maturité de la cybersécurité pour les organisations de l'IID canadienne.

De plus, la Loi sur le Service canadien du renseignement de sécurité (SCRS) permet au SCRS de réaliser des cyberopérations actives et défensives. Le SCRS utilise un ensemble de mesures de réduction des menaces, énoncées dans la Loi sur le SCRS, pour lutter contre les cyberincidents qui menacent la sécurité nationale du Canada, et ce, au pays et à l'étranger. Ainsi, le Service collabore avec divers ministères pour favoriser la cybersécurité du Canada et tenter de lutter contre l'ingérence étrangère dans le cyberespace.

Recommandation 15 : ***Que le Gouvernement du Canada entreprenne une analyse exhaustive de la cybersécurité afin de déterminer les vulnérabilités cybernétiques existantes au Canada, y compris, mais sans s'y limiter, celles des infrastructures essentielles, et qu'il accorde la priorité à l'élimination des vulnérabilités et des intrusions actuelles des acteurs hostiles.***

Le gouvernement du Canada appuie cette recommandation.

Le gouvernement du Canada entreprend de manière continue ce genre d'activité afin de mieux protéger les canadiens, leurs données, et les services essentiels dont ils dépendent.

Sécurité publique Canada offre une série de programmes ciblés de sensibilisation, d'exercices et d'évaluation pour aider les propriétaires et les exploitants d'infrastructures essentielles à cerner les vulnérabilités et à y remédier. La majorité des participants ont indiqué que ces programmes ont accru leur niveau de sensibilisation aux risques divers et changeants pour les infrastructures essentielles, ainsi qu'une meilleure réponse aux incidents de menaces qui ciblent leurs organisations.

Le CST et son Centre pour la cybersécurité continuent de travailler à l'amélioration des solutions d'authentification, par la collaboration avec les principaux organismes de sécurité du gouvernement du Canada et l'industrie pour trouver des solutions d'authentification multifactorielles pour les services internes et externes. Le CST et le Centre pour la cybersécurité publieront également des lignes directrices sur la cyber sécurité concernant la gestion sécurisée des identités numériques. Celles-ci ont été élaborées en

partenariat avec l'industrie (Microsoft) et ont été basées sur les vulnérabilités récemment observées. Elles se concentrent sur l'administration des services d'annuaire et la gestion efficace des environnements sécurisés grâce à des solutions d'authentification améliorées et des postes de travail dédiés.

Pour remédier aux vulnérabilités de jour zéro, le CST et son Centre pour la cybersécurité rappellent l'importance de la gestion des correctifs, alors que nous continuons de travailler avec les fournisseurs de services infonuagiques (FSI) pour améliorer les services de sécurité et la résilience cybernétique.

Pour remédier aux vulnérabilités persistantes qui peuvent être atténuées par une gestion adéquate, le CST et le Centre pour la cybersécurité publient régulièrement des documents d'orientation sur les pratiques exemplaires en matière de cybersécurité qui portent sur plusieurs sujets, notamment la gestion des mots de passe, les correctifs et l'importance de surveiller et de consigner les incidents qui touchent à la sécurité. De plus, le projet de loi C-26, Loi concernant la cybersécurité, aiderait les exploitants d'infrastructures essentielles désignés dans le secteur du transport, de l'énergie, des finances et des télécommunications à remédier aux vulnérabilités actuelles et à réduire leurs cyberrisques.

Pour aider le gouvernement et les secteurs des infrastructures essentielles à comprendre leur environnement et à élaborer des solutions cybernétiques plus robustes, le CST et son Centre pour la cybersécurité ont mis au point un outil d'analyse des menaces et des risques appelé ASTRA, pour aider au développement d'environnements sécurisés. Le CST et son Centre pour la cybersécurité offrent également un cours sur la façon d'utiliser l'outil par l'intermédiaire de leur centre d'apprentissage.

Recommandation 16 : ***Que le Gouvernement du Canada inclue les plateformes spatiales comme infrastructure essentielle et veille à ce qu'elles soient protégées et sécurisées.***

Le Gouvernement du Canada convient d'examiner cette recommandation plus en profondeur.

Depuis l'automne 2021, le Gouvernement collabore avec l'ensemble de la collectivité des infrastructures essentielles dans le cadre du renouvellement de la Stratégie nationale sur les infrastructures essentielles. Les intervenants ont indiqué qu'ils appuyaient l'option d'ajouter un secteur spatial en raison du rôle essentiel que jouent les plateformes spatiales dans le soutien de toutes les autres formes d'infrastructure essentielle et de surveillance environnementale. À mesure que le renouvellement de la Stratégie progressera, le gouvernement continuera d'explorer la possibilité de désigner les plateformes spatiales comme infrastructure essentielle.

Recommandation 17 : ***Que le Gouvernement du Canada définisse clairement les rôles et les responsabilités de chaque ministère responsable de la surveillance, de l'intervention et de l'utilisation des cybercapacités au Canada.***

Le Gouvernement du Canada appuie cette recommandation.

La cybersécurité est une responsabilité partagée au sein du gouvernement du Canada, les rôles et les responsabilités sont définis dans les mandats ministériels et les instruments de politique du Conseil du Trésor, comme la Politique sur la sécurité du gouvernement et la Politique sur les services et le numérique.

Recommandation 18 : ***Que le Gouvernement du Canada examine toutes les infrastructures liées à la cybersécurité, utilisées pour les fonctions opérationnelles du ministère de la Défense nationale (MDN) et des Forces armées canadiennes (FAC), afin de s'assurer qu'elles sont exemptes de technologie sensible conçue, assemblée et exploitée directement ou indirectement, par des États étrangers malveillants, qui pourraient poser un risque de cybersécurité ou compromettre autrement les renseignements protégés.***

Le Gouvernement du Canada appuie cette recommandation.

Le Gouvernement du Canada veille activement à ce que l'équipement, les logiciels ou les services non fiables ne soient pas utilisés dans la prestation et le soutien des services gouvernementaux.

Le Programme de sécurité du MDN et des FAC et le Programme d'assurance de la cybermission veillent à ce que les risques pour l'infrastructure militaire, y compris la technologie de l'information, la technologie des plateformes et la technologie opérationnelle, soient cernés et atténués avant l'approvisionnement et l'utilisation opérationnelle.

De plus, le Programme d'intégrité de la chaîne d'approvisionnement du Centre de la sécurité des télécommunications collabore avec Services partagés Canada pour évaluer les risques liés à l'acquisition d'équipement de technologie de l'information et des communications pour les systèmes et les réseaux du gouvernement du Canada. Ce programme évolue pour répondre à la demande croissante et à la complexité des risques liés à la chaîne d'approvisionnement cybernétique, notamment par la collaboration avec un plus grand nombre de partenaires du gouvernement et de l'industrie.

Recommandation 19 : ***Que le Gouvernement du Canada demande à tous les ministères fédéraux et aux gouvernements provinciaux, territoriaux et autochtones de fournir une liste détaillée des infrastructures essentielles au Conseil du Trésor et au Centre de la sécurité de télécommunications et de la mettre à jour chaque année.***

Le Gouvernement du Canada accepte d'examiner plus à fond cette recommandation.

Le Gouvernement reconnaît la nature intergouvernementale de la propriété, de la réglementation et de la protection des infrastructures essentielles. Par conséquent, nous continuerons de communiquer avec les intervenants appropriés pour régler les problèmes liés à la sécurité nationale, dont les questions liées aux listes d'infrastructures essentielles.

Recommandation 20 : ***Que le Gouvernement du Canada augmente le financement du Centre canadien pour la cybersécurité afin d'améliorer la coordination entre les systèmes de cybersécurité fédéraux et provinciaux afin de mieux traiter les incidents.***

Le Gouvernement du Canada appuie cette recommandation.

Le CST et son Centre pour la cybersécurité continuent de travailler à renforcer la coordination entre les systèmes fédéraux et provinciaux lorsqu'il s'agit de traiter les incidents, notamment la possibilité d'établir une ligne réservée au signalement des incidents et au soutien direct aux provinces et aux territoires

Recommandation 21 : ***Que le Parlement du Canada crée un comité mixte spécial sur la cybersécurité, la guerre de l'information et l'intelligence artificielle.***

Le Gouvernement du Canada prend note de cette recommandation.

Des comités mixtes spéciaux sont créés par ordre de renvoi des deux Chambres pour traiter de questions d'une grande importance publique. Les comités spéciaux sont indépendants du gouvernement, et la décision d'en créer relève du Parlement.

Recommandation 22 : ***Que le Gouvernement du Canada entreprenne immédiatement un examen approfondi et une réforme rapide du processus d'acquisition d'équipement militaire, y compris l'équipement de guerre cybernétique – ce qui comprendrait les lignes directrices du Conseil du Trésor sur la concurrence et l'attribution de contrats à fournisseur unique – avec l'intention de faire passer la durée des projets de plusieurs années à plusieurs mois ou semaines.***

Le gouvernement du Canada est d'accord avec cette recommandation en principe.

L'approvisionnement rationaliste et souple est nécessaire pour assurer la prestation réussie et rapide des capacités modernes nécessaires pour que les FAC soient prêtes et équipées pour mener des opérations. L'approvisionnement en matière de défense est un effort pangouvernemental, et la gestion de projets complexes d'approvisionnement en matière de défense, comme les avions de chasse et la modernisation du NORAD, exige des compétences acquises au fil des ans.

Le MDN et les FAC collaborent avec des partenaires clés de Services publics et Approvisionnement Canada, d'Innovation, Sciences et Développement économique Canada, de Construction de Défense Canada, de Services partagés Canada et du Secrétariat du Conseil du Trésor pour accélérer leur prestation des capacités et envisager des approches d'approvisionnement plus novatrices. Les processus d'approvisionnement ont pour but de répondre aux exigences opérationnelles actuelles et futures tout en veillant à ce que le Canada réalise les avantages industriels, technologiques et sociétaux qui découlent de ces investissements substantiels et préserve les principes d'ouverture, de transparence et d'équité.

Il existe des mécanismes et des procédures qui permettent au gouvernement de répondre rapidement aux besoins opérationnels urgents. Par exemple, L'approche axée sur les risques de SPAC pour L'approbation des marchés pour les projets de défense à faible risque a accéléré le processus d'approbation, ce qui améliore la rapidité d'exécution des projets et des capacités. En outre, le MDN et les FAC collaborent avec des partenaires de l'industrie pour assurer l'harmonisation, trouver des solutions réalistes et respecter l'échéancier.

Recommandation 23 : ***Que le Gouvernement du Canada adapte et élabore un plan complet pour le recrutement et le maintien en poste des cyberopérateurs qui fait concurrence au secteur privé afin de s'assurer que les postes sont comblés et que l'écart de compétences en matière de cybersécurité est comblé dans les FAC et au Centre de la sécurité des télécommunications.***

Le Gouvernement du Canada appuie cette recommandation.

Les FAC reconnaissent l'importance de recruter et de maintenir en poste des cyberopérateurs qualifiés. Protection, Sécurité, Engagement (PSE) a ordonné aux FAC d'établir un groupe professionnel d'opérateurs cybernétiques pour mener des cyberopérations défensives et offensives à l'appui des missions militaires. La première classe de cyberopérateurs a obtenu son diplôme de l'École d'électronique et des communications des Forces canadiennes et septembre 2021.

Les FAC ont mis en place un certain nombre d'initiatives de recrutement pour recruter de nouveaux membres. Le site Web des FAC présente le métier de cyberopérateur comme un choix de carrière potentiel et donne un aperçu du métier, des rôles et des responsabilités, de la formation requise, des programmes d'enrôlement, des options d'enrôlement direct et de l'information sur la rémunération et les avantages sociaux des FAC.

Le calcul des salaires des cyberopérateurs du MDN et des FAC tient compte des compétences spécialisées de ces derniers comparativement aux autres membres des FAC.

Recommandation 24 : ***Que le gouvernement du Canada, en collaboration avec les Forces armées canadiennes, se dote d'une capacité de mobilisation continue et qu'il en fasse usage.***

Le gouvernement du Canada appuie cette recommandation.

La politique Protection, Sécurité, Engagement appelait les Forces armées canadiennes (FAC) à adopter une posture plus assurée dans le cyberespace pour renforcer leurs défenses et mener des cyberopérations offensives à l'appui des missions militaires autorisées par le gouvernement. Les FAC reconnaissent l'importance des capacités tant offensives que défensives pour assurer la sécurité de leurs propres réseaux et systèmes et projeter leur puissance dans le cyberespace.

Pour défendre et protéger leurs réseaux et systèmes internes, les FAC misent sur l'intervention proactive et l'adaptation aux cybermenaces émergentes et en évolution. Elles reconnaissent par ailleurs l'importance de la défense collective et travaillent en étroite collaboration avec leurs alliés et partenaires pour prévenir les cyberactivités malveillantes en tout genre, de même que s'en défendre et y faire face. Par exemple, pour aider l'Ukraine à renforcer

ses capacités de défense, les FAC ont mis sur pied une cyberforce opérationnelle qui offre au pays de l'expertise en cybersécurité, du renseignement sur les cybermenaces, ainsi que des outils et des solutions techniques lui permettant de mieux défendre ses réseaux contre les cyberactivités malveillantes. Les FAC ont également déployé une force opérationnelle canadienne permanente en Lettonie pour mener des cyberopérations défensives conjointes visant les infrastructures essentielles lettonnes.

Recommandation 25 : ***Que le gouvernement du Canada mette sur pied un système permettant aux anciens combattants qui réintègrent la vie civile de conserver une autorisation de sécurité équivalente à celle qu'ils possédaient dans les Forces armées canadiennes, afin que leur habilitation de sécurité soit maintenue et que leur embauche au sein du ministère de la Défense nationale soit facilitée. Le gouvernement devrait également envisager un système permettant d'accélérer la délivrance d'habilitations de sécurité aux anciens combattants qui recherchent un emploi dans d'autres ministères fédéraux.***

Le gouvernement du Canada appuie cette recommandation.

La Norme sur le filtrage de sécurité fait la distinction entre une cote de sécurité et une autorisation de sécurité. Une cote de sécurité, également appelée cote de fiabilité, est la norme minimale de filtrage de sécurité pour les postes dont les titulaires doivent avoir un accès non supervisé à des biens, à des installations ou à des systèmes de technologie de l'information du gouvernement du Canada. Une autorisation de sécurité donne accès à des renseignements, à des biens, à des installations ou à des systèmes de technologie de l'information classifiés du gouvernement du Canada (niveau secret ou supérieur). Aux fins de cette recommandation, le gouvernement du Canada juge que l'expression « autorisation de sécurité » englobe la cote de sécurité et l'autorisation de sécurité.

On procède couramment au transfert des autorisations de sécurité des Forces armées canadiennes (FAC) au ministère de la Défense nationale (MDN). Le MDN et les FAC surveillent continuellement le processus afin de trouver des façons de réduire les temps d'attente et d'accélérer les transferts.

Les autorisations peuvent aussi être transférées pour les membres des FAC qui se joignent à d'autres ministères. Bien que l'échéancier du transfert puisse varier, le transfert de l'information sur les autorisations de sécurité du MDN vers un autre ministère fédéral ne prend généralement pas plus de deux semaines, et ce, dès la réception de la demande de transfert. Les délais de traitement varient selon le nombre de demandes de transfert qu'a reçu le MDN à ce moment.

Ainsi, l'autorisation de sécurité valide d'un membre des FAC en service peut être transférée à tout autre ministère lorsqu'il est transféré à un poste civil au sein de la fonction publique fédérale. Cependant, lorsqu'un membre quitte les FAC, il doit retourner à un poste au sein de la fonction publique fédérale avant que son autorisation arrive à échéance (dans les 12 mois pour les autorisations de niveau Secret ou supérieur et dans les 2 ans pour les cotes de fiabilité).

Bien que les ministères respectent la Politique sur la sécurité du gouvernement du Conseil du Trésor, y compris sa Norme sur le filtrage de sécurité, il incombe à chaque ministère, après avoir reçu le dossier du MDN, de voir à la réalisation de son propre filtrage de sécurité.

Les membres des Forces armées canadiennes libérés pour des raisons médicales attribuables au service ont un droit de priorité statutaire. Ils sont les premiers dans l'ordre de priorité établi par la Loi sur l'emploi dans la fonction publique, pourvu qu'ils possèdent les qualifications essentielles exigées pour le poste. Ce droit de priorité commence lorsque l'ancien combattant est jugé apte à retourner au travail par un médecin, et il est valide durant 5 ans.

Le gouvernement du Canada continuera à chercher d'autres moyens de faciliter la transition des anciens combattants au sein de la fonction publique.

Recommandation 26 : ***Que le gouvernement du Canada prenne des mesures pour bien définir les rôles et les responsabilités des Forces armées canadiennes et du Centre de la sécurité des télécommunications en matière de cybersécurité au Canada et à l'étranger.***

Le gouvernement du Canada appuie cette recommandation.

Les fonctions et responsabilités des FAC et du CST sont clairement définies. Le CST est la principale autorité technique fédérale en matière de cybersécurité, tandis que les FAC ont le mandat de défendre et de protéger les réseaux internes du MDN et des FAC, en plus de mener des cyberopérations à l'appui de missions militaires autorisées par le gouvernement.

Dans le cadre de ses responsabilités, le CST fournit du renseignement étranger précieux pour éclairer le processus décisionnel du gouvernement du Canada et protéger la sécurité nationale. Grâce à son expertise dans les domaines techniques et du cyberespace, le CST cerne et surveille les potentielles menaces qui pèsent sur les systèmes et les réseaux du Canada et aide à prendre des mesures actives pour les contrer.

Les FAC et le CST travaillent depuis longtemps en partenariat pour élaborer des capacités hautement techniques et spécialisées à l'appui des opérations des FAC, et ce partenariat continue d'évoluer en même temps que les cybermenaces et les capacités. Par exemple, le CST travaille en étroite collaboration avec les FAC à intégrer les opérations du renseignement électromagnétique militaire à l'appui des besoins en matière de renseignement de défense, à en établir les priorités et à dénouer les conflits connexes. Cette collaboration a permis aux FAC d'améliorer leurs connaissances du domaine et de mieux protéger leurs forces dans le cadre de ses opérations mondiales.

Cette relation favorise l'atteinte des objectifs des missions, en veillant à faire appel aux bons outils et capacités, tout en réduisant le dédoublement inutile des efforts. À l'heure actuelle, plusieurs membres des CAF font également partie d'une équipe conjointe au CST chargée de réaliser des cyberopérations à l'étranger. Par ailleurs, au titre de l'article 20 de la Loi sur le Centre de la sécurité des télécommunications, les FAC peuvent aussi demander de l'assistance technique et opérationnelle au CST. Le CST et les FAC travaillent en partenariat sur les plans opérationnel et stratégique à tous les niveaux, en vue d'harmoniser leurs résultats stratégiques et de maximiser l'avantage stratégique du Canada au chapitre des affaires internationales, de la défense, de la sécurité et de la cybersécurité.

Recommandation 27 : ***Que le gouvernement du Canada prenne immédiatement des mesures pour remédier aux problèmes de soutien logistique au sein des Forces armées canadiennes et de leurs cyberforces.***

Le gouvernement du Canada est d'accord avec cette recommandation en principe.

Pour veiller à ce que les FAC disposent du soutien logistique dont elles ont besoin pour remplir leur mandat, il est essentiel, entre autres, d'assurer la sécurité du matériel de gestion de l'information et de technologie de l'information (GI-TI) contre les défaillances et les cyberattaques.

En collaboration avec leurs partenaires du gouvernement du Canada, le MDN et les CAF voient à ce que le matériel de GI-TI soit sécurisé, résilient et capable de se remettre rapidement d'une défaillance ou d'une cyberattaque pour ne pas nuire aux opérations du ministère ou des FAC, dont celles des cyberforces.

Par ailleurs, le programme de sécurité du MDN et des FAC, tout comme le programme d'assurance des cybermissions, vise à cerner et à atténuer les risques pour les infrastructures militaires (y compris les ressources du réseau, comme les logiciels et le matériel informatique) avant leur utilisation à des fins opérationnelles.

Recommandation 28 : ***Que le gouvernement du Canada assure la viabilité à long terme des cyberforces des FAC grâce à la création d'un programme de maintien en poste des cyberopérateurs et à la mise en place des cyberinfrastructures nécessaires.***

Le gouvernement du Canada appuie cette recommandation.

Les CAF peinent à maintenir en poste l'effectif de plusieurs groupes professionnels; la Stratégie de maintien de l'effectif des Forces armées canadiennes, dont l'objectif est de garder en poste les militaires faisant preuve de talent en créant un milieu de travail accueillant et sain, vise à régler le problème. Par ailleurs, l'offre d'instruction appropriée et d'infrastructures à l'appui constitue un autre problème reconnu, pour lequel on évalue actuellement des options.

Comme le prévoit la politique Protection, Sécurité, Engagement, les FAC soutiendront leurs membres en améliorant considérablement le recrutement, l'instruction et le maintien en poste du personnel. Les FAC prévoiront mieux les besoins des groupes militaires professionnels et réaliseront davantage d'activités de recrutement ciblées, notamment afin de tirer parti de la diversité de la population canadienne, ainsi que des compétences et des talents particuliers qu'elle détient.

Face à l'évolution rapide du paysage mondial et technologique, les FAC et le MDN se heurtent à de nombreux défis et questions complexes quant à l'élaboration, à la mise sur pied, au maintien et à la gestion des capacités militaires avec efficacité et efficience, tout en voyant à la transformation numérique. Depuis la diffusion de la politique Protection, Sécurité, Engagement en 2017, le MDN et les CAF poursuivent leur travail dans le cadre des principales cyberinitiatives. Ils s'emploient notamment à se munir de cybercapacités actives qui serviront contre d'éventuels adversaires dans le cadre de missions militaires autorisées par le gouvernement, à mettre sur pied un nouveau groupe professionnel de « cyberopérateurs » aux FAC en vue d'attirer les cybertalents les plus qualifiés et éminents au Canada, et à faire appel à des réservistes munis de compétences spécialisées pour combler des postes dans la cyberforce des FAC.

Recommandation 29 : ***Que le gouvernement du Canada maintienne à jour de façon continue le cadre juridique pour ce qui est de faire face aux cyberattaques, y compris les directives pour les attributions, les interventions et la responsabilité.***

Le gouvernement du Canada soutient cette recommandation.

Il y a un cadre politique pour l'attribution, lequel oriente également les décisions d'intervenir. AMC consulte actuellement plusieurs ministères pour passer en revue et mettre à jour le cadre d'attribution. Le gouvernement du Canada doit rester attentif à l'évolution des lois internationales et du cadre multilatéral pour un comportement stable de l'état dans le cyberespace.

Recommandation 30 : ***Que le gouvernement du Canada travaille avec nos alliés pour mettre à jour les lois internationales, comme le Statut de Rome et la Convention de Genève, en vue d'y inclure la cyberguerre soutenue par un état à titre de crime de guerre.***

Le gouvernement du Canada prend note de cette recommandation.

Le gouvernement du Canada soutient l'ordre international fondé sur des règles et affirme que les lois internationales existantes s'appliquent aux activités de tous les états dans le cyberespace.

Le gouvernement du Canada continuera d'encourager les états à publier leurs points de vue nationaux sur la façon dont les lois internationales s'appliquent au cyberespace.

Recommandation 31 : ***Que le gouvernement du Canada adopte immédiatement toutes les recommandations en suspens du Rapport 7 de la vérificatrice générale — La cybersécurité des renseignements personnels dans le nuage, déposé devant le Parlement le 15 novembre 2022.***

Le gouvernement du Canada soutient cette recommandation.

Le SCT travaille en collaboration avec SPC, SPAC et le CST pour mettre en œuvre les recommandations du Rapport 7 de la vérificatrice générale — La cybersécurité des renseignements personnels dans le nuage conformément à la réponse décrite dans la section « Recommandations et réponses » du rapport.

Recommandation 32 : ***Que le gouvernement du Canada utilise les régimes de sanctions existants contre les individus et les entités qui envoient aux Canadiens de la mésinformation, de la désinformation ou de la malinformation.***

Le gouvernement du Canada est d'accord pour examiner cette recommandation plus en profondeur.

Le Canada adopte une approche judicieuse lorsqu'il impose des sanctions, et il est engagé à les utiliser de façon efficace et coordonnée, au besoin. À cette fin, le Canada a mis en place un processus rigoureux de diligence raisonnable pour prendre en considération et évaluer les cas possibles de violation flagrante des droits de la personne et de corruption, ou les autres circonstances qui pourraient justifier l'imposition de sanctions. Puisque chaque situation est unique, les contextes nationaux et internationaux plus vastes sont également des points importants à prendre en considération pour ce qui est de déterminer si des sanctions ou d'autres outils de politique étrangère du Canada sont des mécanismes d'intervention appropriés.

Les lois sur les sanctions autonomes du Canada indiquent les seuils juridiques qui doivent être dépassés pour qu'il y ait des sanctions. De plus, la disponibilité d'information crédible de source ouverte est aussi un facteur important pour ce qui est d'envisager l'imposition de sanctions, puisque les justifications pour l'imposition de sanctions autonomes à des cibles précises doivent être soutenues par des sources ouvertes accessibles dans le domaine public.

Le Canada a auparavant imposé des sanctions à des individus et à des entités impliqués dans des activités de mésinformation, de désinformation ou de malinformation, surtout dans le cadre de sanctions plus vastes relatives à l'invasion russe en Ukraine.

Le Mécanisme de réponse rapide du G7 (MRR du G7), mené par le Canada sur une base continue, est une partie importante du Plan pour protéger la démocratie canadienne. En reconnaissance que la mésinformation et la désinformation, entre autres vecteurs d'interférence étrangère, menacent la démocratie et nuisent à la sécurité nationale, les dirigeants du G7 se sont engagés à mettre sur pied le MRR du G7 lors du Sommet de Charlevoix en 2018. Mené par le Canada sur une base continue, le MMR du G7 a le mandat de cerner les menaces étrangères à la démocratie et d'y répondre. Depuis sa conception, le MMR du G7 est axé sur la lutte contre la manipulation de l'information et l'ingérence étrangère, un ensemble d'activités en ligne malveillantes qui comprend la désinformation. Outre la coordination du MMR du G7, AMC surveille également l'environnement de l'information numérique pour y déceler des signes d'interférence étrangère sur les priorités clés du gouvernement du Canada, y compris durant les élections, dans le cadre du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections. Cela comprend une équipe autonome

axée sur la lutte contre la désinformation russe, annoncée par le premier ministre l'été dernier (2022).

Nous continuerons de surveiller les cas possibles de mésinformation, de désinformation et de malinformation, et nous continuerons à envisager les sanctions autonomes à titre de mécanisme d'intervention possible, au besoin.

Recommandation 33 : ***Que le gouvernement du Canada impose des sanctions efficaces aux pays qui cautionnent ou qui mettent en place des cybercriminels en vue par exemple de vols de fonds, de vols de propriété intellectuelle, de guerre de l'information et d'autres intentions malveillantes.***

Le gouvernement du Canada accepte d'examiner davantage cette recommandation.

Le Canada est engagé à lutter contre les cybercrimes et à les prévenir, et il travaille activement avec les partenaires internationaux pour promouvoir et protéger les intérêts des Canadiens qui sont de plus en plus visés par ces crimes. Pour donner suite à la réponse à la recommandation 32, et en reconnaissance des grandes lignes des seuils juridiques de la loi en matière de sanctions autonomes au Canada, si l'on conclut que les activités de cybercriminels constituent une violation flagrante des droits de la personne, des actes de corruption importants ou des infractions graves de la sécurité et de la paix internationales qui ont causé ou qui causeront probablement des crises internationales, on pourrait envisager des sanctions à titre de mécanisme possible d'intervention.

Nous continuerons de surveiller les actions possibles des pays qui cautionnent ou qui mettent en place des cybercriminels, et nous évaluerons si de telles actions répondent aux critères selon lesquels le Canada peut imposer des sanctions autonomes à titre de mécanisme d'intervention possible, au besoin.

Recommandation 34 : ***Que le gouvernement du Canada entreprenne un examen de la politique actuelle de cyberdéfense et tienne des conversations bilatérales avec les alliés, comme les États-Unis, pour garantir que des politiques cohérentes et uniformes sont utilisées.***

Le gouvernement du Canada soutient cette recommandation.

La politique de défense du Canada, intitulée Protection, Sécurité, Engagement, exige aux Forces armées canadiennes (FAC) d'adopter une position plus ferme dans le cyberespace, en plus d'élaborer et d'utiliser des cybercapacités pour soutenir les missions militaires.

Les FAC passent habituellement en revue ses politiques internes pour s'assurer d'avoir l'orientation, les ressources et les capacités prêtes pour l'avenir nécessaires pour répondre aux défis d'aujourd'hui et à venir. Le MDN et les FAC continuent de s'adapter à l'environnement changeant de la sécurité internationale et modifient leurs priorités en conséquence.

Le Canada participe à des conversations bilatérales avec des alliés pour garantir l'application uniforme de politiques pertinentes. Par exemple, en mars 2023, le premier ministre Trudeau et le président Biden ont publié une déclaration commune reconnaissant que les cybermenaces ont des répercussions à la fois sur les Canadiens et sur les Américains, surtout lorsqu'elles sont dirigées vers les systèmes transfrontaliers sur lesquels les deux nations reposent. Le Canada et les États-Unis demeurent engagés à une meilleure protection contre les menaces et à une amélioration de la coopération pour ce qui est de favoriser les améliorations à la cybersécurité et la résilience des infrastructures essentielles.

Recommandation 35 : ***Que le gouvernement partage avec la Finlande et la Suède une éducation sur la guerre cognitive pour les civils avec les provinces.***

Le gouvernement du Canada soutient cette recommandation.

Comme il l'a déclaré dans son rapport du 6 avril 2023 intitulé Contrer une menace en évolution : mise à jour sur les recommandations visant à prévenir l'ingérence étrangère dans les institutions démocratiques canadiennes, le gouvernement a travaillé et travaillera de concert avec des responsables provinciaux, territoriaux, municipaux et autochtones. Ces dernières années, la Gendarmerie royale du Canada, le Service canadien du renseignement de sécurité, le Centre canadien pour la cybersécurité et Sécurité publique Canada ont collaboré avec des collègues provinciaux, territoriaux et municipaux ainsi qu'avec des propriétaires et des exploitants d'infrastructure critique pour mieux faire connaître les menaces d'ingérence étrangère et renforcer la résilience.

Une mobilisation soutenue, régulière et coordonnée avec les partenaires est essentielle pour détecter les menaces, renforcer la résilience et contrer efficacement les activités d'ingérence étrangère. Le nouveau coordonnateur national de la lutte contre l'ingérence étrangère travaillera à élargir les mécanismes d'information avec des responsables provinciaux, territoriaux, municipaux et autochtones. L'Unité de protection de la démocratie du Bureau du Conseil privé, qui coordonne, élabore et met en œuvre des mesures pangouvernementales canadiennes visant à lutter contre la désinformation et à protéger nos institutions et nos processus démocratiques, élargira la portée de ses travaux avec les provinces et les territoires.

L'Initiative de citoyenneté numérique (ICN), établie dans le cadre du Plan pour protéger la démocratie canadienne, est liée à d'autres organismes gouvernementaux, chercheurs et sociétés civiles, et elle aide à la mise en commun de l'information et des ressources entre ces intervenants. En juin 2023, par l'entremise de l'ICN, le gouvernement a annoncé un investissement de 5,5 millions de dollars pour la création du Réseau canadien de recherche sur les médias numériques (RCRMN). Le RCRMN renforcera encore plus la résilience en matière d'information des Canadiens en menant des recherches pour déterminer l'incidence de la qualité de l'information, y compris des récits de désinformation, sur les attitudes et les comportements des Canadiens ainsi qu'en appuyant des stratégies pour la littératie numérique de ces derniers. Le RCRMN est administré de façon indépendante par l'Observatoire de l'écosystème médiatique de l'Université de Toronto et de l'Université McGill. Les résultats de recherche et les rapports du RCRMN seront rendus publics, et tous les Canadiens y auront donc accès, y compris les fonctionnaires des administrations provinciales, territoriales, municipales et autochtones.

Le Mécanisme de réponse rapide (MRR) du G7, dirigé de façon continue par le Canada, a le mandat de repérer les menaces étrangères pour la démocratie et de les contrer. Depuis sa création, le MRR du G7 a avant tout été axé sur la lutte à la manipulation de l'information et l'ingérence étrangère, un ensemble d'activités malveillantes en ligne qui incluent la désinformation. En 2021, dans le cadre du Mécanisme de réponse rapide du G7 (MRR), la Suède a été accueillie à titre d'observateur en vue de tirer profit de l'expertise et d'éviter les répétitions. Le gouvernement du Canada continuera également d'établir des liens avec l'agence suédoise de défense psychologique.

Le gouvernement du Canada continuera de travailler avec la Suède et d'explorer la possibilité de travail avec la Finlande pour tirer profit de ses efforts dans le domaine de l'éducation civile sur la guerre cognitive.

Recommandation 36 : ***Que le gouvernement du Canada établisse des démarcations claires entre les activités du Centre de la sécurité des télécommunications se rapportant au renseignement électromagnétique et celles se rapportant à la cybersécurité, y compris les processus d'autorisation ministérielle et les mécanismes de déclaration.***

Le gouvernement prend note de cette recommandation.

Le cadre juridique existant du Canada assure un niveau de séparation approprié et rigoureux entre les différents volets du mandat du Centre de la sécurité des télécommunications (CST), tout en permettant un certain échange d'information au sein du CST. Ces échanges se font strictement en conformité avec la Loi sur le Centre de la sécurité des télécommunications (LCST), la Loi sur la protection des renseignements personnels et la Charte

canadienne des droits et libertés. Ils sont essentiels à la capacité du CST de fournir en temps opportun des conseils, une orientation et des services en matière de cybersécurité de la plus haute qualité qui permettent d'assurer la protection des renseignements personnels et la sécurité des Canadiens. De plus, il est important de noter que, en vertu de la LCST, les activités du CST ne peuvent pas viser les Canadiens où qu'ils soient ni toute personne se trouvant au Canada.

En 2016, par l'entremise de Sécurité publique Canada, le gouvernement a consulté les Canadiens à l'échelle du pays pour leur demander vers où la gestion de la cybersécurité devrait s'orienter au Canada. Ces commentaires ont été pris en compte lors de la planification de la Stratégie nationale de cybersécurité de 2018. À titre d'initiative clé de cette Stratégie, les fonctions opérationnelles de cybersécurité de trois ministères ont été regroupées en vue de mettre sur pied le Centre canadien pour la cybersécurité (Centre pour la cybersécurité), qui fait partie du CST. Cette décision reconnaissait l'utilité et l'importance d'une gestion fédérale plus ciblée de la cybersécurité, laquelle profite du milieu novateur, de l'expertise technique et des perspectives stratégiques du CST. Cela mène à une capacité accrue de relever, de traiter et de communiquer des connaissances sur les menaces, les risques et les vulnérabilités systémiques. Ce modèle est aussi utilisé dans les cadres de cybersécurité des autres partenaires du Groupe des cinq.

En vertu de l'article 15 de la LCST, le mandat du CST comporte cinq volets, notamment le renseignement étranger et la cybersécurité, qui sont décrits respectivement aux articles 16 et 17 de la Loi. Comme l'exige la LCST, le CST conserve des autorisations ministérielles distinctes pour les volets du renseignement étranger et de la cybersécurité de son mandat, et chacune d'entre elles doit être approuvée par le commissaire au renseignement. Ce dernier agit à titre d'entité externe indépendante, et il lui incombe de s'assurer que les autorisations accordées par le ministre cadrent avec le volet précis du mandat du CST pour lequel elles sont accordées et qu'elles sont raisonnables, proportionnelles et nécessaires.

Les activités prévues sous chaque autorisation peuvent aussi faire l'objet d'un examen par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR).

De plus, dans les 90 jours suivant la date d'abrogation ou d'expiration de chaque autorisation, le CST doit fournir au ministre un rapport sur le résultat des activités menées au titre de l'autorisation, puis le ministre en fournit une copie au commissaire au renseignement et à l'OSSNR. Conformément aux autorisations elles mêmes, les autorisations de renseignement de sécurité et les autorisations de cybersécurité font l'objet de rapports distincts.

Recommandation 37 : ***Que le gouvernement du Canada se dote d'un ambassadeur en matière de cybersécurité.***

Le gouvernement du Canada accepte d'examiner davantage cette recommandation.

Le gouvernement du Canada étudie activement cette option. La nomination d'un haut fonctionnaire aiderait à accentuer la mobilisation mondiale et à faire avancer nos priorités internationales en matière de sécurité en collaboration avec les cyberdiplomates du Canada. En cette ère de transformation numérique profonde, il pourrait être justifié d'envisager un portefeuille plus vaste plutôt que de se limiter à la cybersécurité.

Conclusion

Le gouvernement remercie le Comité pour ses commentaires et ses recommandations. Ce rapport lui sera une ressource utile dans le cadre des mesures prises pour renforcer la protection du Canada contre les cyberactivités malveillantes.

Veuillez recevoir, Monsieur le Président, l'assurance de ma haute considération.

L'honorable Dominic LeBlanc, C.P., c.r., député
Ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales

c.c. L'honorable Bill Blair, C.P., député
Ministre de la Défense

L'honorable Mélanie Joly, C.P., députée
Ministre des Affaires étrangères

L'honorable François-Philippe Champagne, C.P., député
Ministre de l'Innovation, des Sciences et de l'Industrie

L'honorable Chrystia Freeland, C.P., députée
Ministre des Finances et vice-première ministre du Canada