Ron McKinnon, député
Président du Comité permanent de la sécurité publique et nationale
Chambre des communes
Ottawa (Ontario)
K1A 0A4

Cher collègue,

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 septième rapport du Comité permanent de la sécurité publique et nationale intitulé *Prêt à relever le défi : renforcer la posture de sécurité du Canada par rapport à la Russie*.

J'aimerais féliciter le Comité pour son travail visant à examiner la posture de sécurité du Canada par rapport à la Russie.

Le gouvernement est d'accord en principe avec la teneur générale et la plupart des recommandations du Comité. Sans être en désaccord avec ces recommandations, le gouvernement juge toutefois qu'une étude ou un examen plus approfondi est nécessaire dans certains cas.

Recommandation 1 : ***Que le gouvernement du Canada continue d'imposer à la Russie des coûts élevés pour son agression contre l'Ukraine; d'appuyer la souveraineté, l'indépendance et l'intégrité territoriale de l'Ukraine; de collaborer avec ses alliés et ses partenaires pour défendre l'ordre international fondé sur des règles; et d'accélérer les efforts de dissuasion et de défense pour combattre toute menace conventionnelle ou non conventionnelle à la sécurité nationale du Canada.***

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

La sécurité et la prospérité futures du Canada passent par un système international stable, prévisible et concerté qui repose sur le respect des principes de la Charte des Nations Unies, notamment la souveraineté, les droits de la personne et l'état de droit. L'appui du Canada à l'Ukraine se veut un investissement dans un monde plus stable, plus démocratique et plus responsable qui garantit que l'agression par la Russie n'est pas avantageuse ou imitée ailleurs.

Le Canada demeure déterminé à jouer un rôle d'exemplarité dans la protection et le renforcement d'un ordre international fondé sur des règles – les sanctions sont une composante essentielle de cette approche.

Pour appuyer la souveraineté, l'indépendance et l'intégrité territoriale de l'Ukraine, l'investissement de plus de 1 milliard de dollars du gouvernement du Canada dans l'aide militaire et les équipements donnés à l'Ukraine a inclus la défense aérienne, des chars de combat Leopard 2, le transport de troupes blindé, l'artillerie, des caméras sur drone, des munitions et du matériel de communication par satellite. De plus, dans le cadre de l'Opération UNIFIER, élargie et prolongée jusqu'en mars 2025, le Canada a entraîné plus de 35 000 soldats ukrainiens et continue de fournir l'instruction en Pologne et au Royaume-Uni et a déployé des formateurs et des sapeurs de combat dans la région.

Pour défendre l'ordre international fondé sur des règles, le Canada a tiré parti de son influence mondiale, de ses ressources et de ses réseaux diplomatiques pour optimiser le soutien à l'Ukraine et isoler le régime de Poutine. Le Canada a participé à diverses tribunes multinationales, notamment celles de l'Organisation du Traité de l'Atlantique Nord (OTAN), de l'Organisation pour la sécurité et la coopération en Europe (OSCE), du G7 (dont à sa plateforme de coordination des donateurs d'organisations multiples) et du G20. Le Canada a également été cofacilitateur et coauteur de résolutions de l'Assemblée générale des Nations Unies (AGNU) qui dénoncent l'agression russe, dont celles adoptées les 24 mars, 7 avril et 12 octobre 2022, ainsi que le 2 mars 2023.

Le Canada prend au sérieux les préoccupations des nouveaux partenaires et recherche activement un soutien international à l'Ukraine. Par exemple, le Canada et ses alliés ont mené une campagne dans le monde entier avant la résolution de l'Assemblée générale des Nations Unies du 22 octobre 2022 sur l'intégrité territoriale de l'Ukraine. Ils ont aidé à obtenir un nombre record de 143 votes « oui ». À d'autres tribunes, notamment la réunion des chefs de gouvernement du Commonwealth de juin 2022 à Kigali, au Rwanda, le Canada a aidé à remédier aux conséquences de la crise pour les pays les plus vulnérables en annonçant l'injection de 250 millions de dollars pour la sécurité alimentaire mondiale qui met l'accent sur l'Afrique subsaharienne.

Depuis l'occupation illégale et la tentative d'annexion de la Crimée par la Russie en 2014, le Canada a imposé des sanctions à quelque 2400 particuliers et entités en Russie, au Belarus et en Ukraine.

Le Canada maintiendra sa collaboration avec ses alliées et ses partenaires en vue de faire pression sur la Russie pour qu'elle mette fin à sa guerre. Le Canada est solidaire de l'Ukraine.

Le Centre de la sécurité des télécommunications (CST) fait le suivi de l'activité liée aux cybermenaces associées à la crise actuelle. Le CST communique de précieux renseignements sur des cybermenaces éventuelles avec ses principaux partenaires en Ukraine et maintient sa collaboration avec les Forces armées canadiennes en appui à l'Ukraine.

Le CST continue de tirer parti de sa multiplicité de pouvoirs liés à la cyberdéfense pour assurer la sécurité nationale du Canada. Il s'agit entre autres de pouvoirs et de capacités de cybersécurité, de renseignement étranger et cyberopérations étrangères pour imposer des coûts aux auteurs de menaces associés qui visent des systèmes d'importance canadiens.

Recommandation 2 : ***Que le gouvernement du Canada travaille avec ses partenaires provinciaux et territoriaux pour créer et promouvoir des programmes de formation postsecondaire agréés dans le domaine de la cyberdéfense.***

Le gouvernement du Canada accepte d'examiner cette recommandation plus en détail.

Le Centre canadien pour la cybersécurité, qui fait partie du CST, représente la seule source fédérale unifiée fournissant des avis, des conseils, des services et du soutien spécialisé en matière de cybersécurité pour les Canadiens. Le Centre est responsable de défendre les réseaux informatiques du gouvernement du Canada, de fournir des avis, des conseils et des services pour les systèmes d'importance du gouvernement du Canada, et d'offrir des astuces simples et efficaces à l'intention de tous les Canadiens pour assurer leur sécurité en ligne.

Le CST maintient sa collaboration avec des intervenants, y compris des partenaires gouvernementaux et non gouvernementaux, pour échanger des informations afin de s'assurer qu'ils disposent des spécialistes, de l'expertise et des ressources dont ils ont besoin en matière de cybersécurité pour faire face à une cyberattaque et s'en remettre. Par exemple, le Carrefour de l'apprentissage du Centre pour la cybersécurité offre de la formation visant l'amélioration de la cybersécurité au sein du gouvernement du Canada et des organisations des infrastructures essentielles. Le Centre pour la cybersécurité collabore également avec les établissements universitaires pour accroître le bassin de candidats talentueux en cybersécurité au Canada et a publié une liste des certifications offertes dans le domaine de la cybersécurité.

Recommandation 3 : ***Que le gouvernement du Canada, en consultation avec les parties concernées, mise sur la Stratégie nationale de cybersécurité afin de faire en sorte que les propriétaires et exploitants d'infrastructures essentielles de toute taille disposent des spécialistes, de l'expertise et des ressources dont ils ont besoin en matière de cybersécurité pour faire face à une cyberattaque et à s'en remettre; de s'assurer que les normes de cybersécurité sont respectées et font l'objet de rapports.***

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

Sécurité publique Canada rédige une nouvelle Stratégie nationale de cybersécurité en concertation avec les représentants fédéraux de la cybersécurité. Dans le cadre de ce processus, le Ministère continuera de concerter les parties concernées des provinces, des territoires et de l'industrie, notamment les représentants des infrastructures essentielles pour que le Canada puisse faire face, dans les meilleures conditions, aux défis de l'ère numérique.

La nouvelle stratégie prévoit la présentation de la vision du Canada pour protéger notre sécurité nationale et notre économie, dissuader les auteurs de cyberattaques et promouvoir un comportement fondé sur des normes dans le cyberespace.

Pour le CST, l'élaboration de la nouvelle Stratégie est une occasion de prendre du recul, de faire le point et de continuer sur la lancée des acquis du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) ces cinq dernières années puisque sa création était une initiative-phare en vertu de la Stratégie précédente de 2018.

Comme les biens et les systèmes essentiels sont de plus en plus interconnectés, intégrés et interdépendants, Sécurité publique Canada procède également à la modernisation de la Stratégie nationale sur les infrastructures essentielles et consulte la communauté des infrastructures essentielles pour ce faire. Les infrastructures essentielles du Canada sont plus susceptibles de subir des défaillances en cascade dans plusieurs secteurs de notre économie compte tenu de l'évolution du contexte des menaces et c'est pourquoi des efforts sont nécessaires pour renforcer la sécurité et la résilience des infrastructures essentielles du Canada.

Recommandation 4 : ***Que le gouvernement du Canada ordonne au Centre de la sécurité des télécommunications d'élargir l'éventail d'outils utilisés pour sensibiliser les petites et moyennes entreprises à la nécessité d'adopter des normes de cybersécurité.***

Le gouvernement est d'accord avec cette recommandation.

La cybersécurité est une responsabilité partagée; les Canadiens, le gouvernement, le secteur privé et nos partenaires internationaux ont tous de grands rôles à jouer. Pour s'assurer que les petites et moyennes entreprises (PME) aient accès aux ressources pour soutenir leur cybersécurité et leur résilience globales, le CST a participé à l'élaboration et à la diffusion d'avis et de conseils adaptés, ainsi que de programmes éducatifs par l'entremise de son Centre pour la cybersécurité (dont le programme Pensez cybersécurité, la campagne nationale de sensibilisation du public créée pour renseigner les Canadiens sur la cybersécurité) et de partenariats généraux du gouvernement du Canada. Sécurité publique Canada a également élaboré des applications et des exercices pour aider les propriétaires et les exploitants d'infrastructures essentielles du Canada à comprendre de quelle façon ils peuvent améliorer la cyberrésilience et la cybersécurité de leurs installations. Les systèmes de contrôle industriel jouent un rôle clé dans le bon fonctionnement de toutes les infrastructures et, si ces systèmes étaient touchés par des cyberincidents, ils pourraient compromettre la capacité des Canadiens à fonctionner au sein de notre économie de plus en plus numérique.

Le Centre pour la cybersécurité du SCT élabore et met à jour régulièrement des avis et des conseils adaptés aux PME. On y aborde des sujets comme les contrôles de cybersécurité de base pour les PME, les principales mesures pour améliorer la cybersécurité pour les PME, le Guide sur les rançongiciels ainsi que les menaces aux chaînes d'approvisionnement et l'espionnage commercial.

Le CST poursuivra sa collaboration avec les PME et à leur prodiguer des conseils à jour pour s'assurer qu'elles sont en mesure d'appliquer les contrôles de sécurité nécessaires et importants pour assurer la sécurité de leurs organisations.

Recommandation 5 : ***Que le gouvernement du Canada instaure des mesures incitatives – entre autres choses – une déduction pour amortissement accéléré ou d'autres mesures fiscales – destinées aux petites et moyennes entreprises pour les encourager à procéder aux investissements nécessaires pour appliquer les contrôles de cybersécurité de base établis par le Centre de la sécurité des télécommunications.***

Le gouvernement prend note de cette recommandation.

Les PME qui engagent des dépenses en capital, y compris celles liées à la cybersécurité, bénéficient déjà des mesures de déduction pour amortissement accéléré et d'autres mesures fiscales présentées par le gouvernement. Parmi ces mesures, il y a l'incitatif à l'investissement accéléré présenté en 2018. Il permet une déduction fiscale bonifiée pour la première année jusqu'à concurrence de trois fois le taux normal. Il y a aussi la mesure temporaire présentée dans le budget de 2021 qui permet aux petites entreprises de passer immédiatement les dépenses en charges jusqu'à 1,5 million de dollars sous forme d'investissements neufs. On remarque également que les logiciels qui ne sont pas considérés comme des logiciels de base donnent généralement droit à un taux de déduction pour amortissement de 100 %. En outre, le budget de 2022 a présenté une élimination plus graduelle de la déduction pour petite entreprise, l'accès étant complètement éliminé lorsque le capital imposable atteindra 50 millions de dollars, plutôt que 15 millions (selon les règles précédentes). Davantage de moyennes entreprises pourront ainsi bénéficier du taux réduit et de la majoration du montant de revenu qui peut être admissible. Cette amélioration se traduit par d'autres économies d'impôt qui peuvent être réinvesties dans l'entreprise.

Recommandation 6 : ***Que le gouvernement du Canada exige que les exploitants d'infrastructures essentielles de secteurs désignés se préparent à faire face à des cyberincidents, les préviennent et les signalent, qu'il mette en place des délais pour le signalement des incidents graves, des services d'assistance technique et des mesures de protection de l'information signalée au Centre de la sécurité des télécommunications, qui aurait pour mandat de partager les leçons apprises avec l'industrie, et qu'il soumette au Parlement des rapports annuels sur ces efforts.***

Le gouvernement est d'accord avec cette recommandation.

En juin 2022, le gouvernement a présenté le projet de loi C-26, Loi concernant la cybersécurité. En vertu de la partie deux de ce projet de loi, la *Loi sur la protection des cybersystèmes essentiels*, les exploitants désignés seraient tenus de déclarer au CST les incidents de cybersécurité qui remplissent un critère ou le dépassent. Dès qu'il a déclaré l'incident de cybersécurité, l'exploitant désigné serait tenu d'en informer l'organisme réglementaire compétent. Sur demande, le Centre pour la cybersécurité serait tenu de fournir un rapport d'incident à l'organisme réglementaire de l'industrie.

De plus, le Centre pour la cybersécurité a déjà noué des relations professionnelles étroites avec l'industrie et les exploitants d'infrastructures essentielles, dont bon nombre signalent volontairement les cybers incidents. La LPCE permettrait au Centre pour la cybersécurité de continuer l'action de ces relations d'une façon collaborative et plus concertée.

Recommandation 7 : ***Que le gouvernement du Canada veille à ce que les rôles, responsabilités et structures en matière de cybersécurité à l'échelle du gouvernement fédéral optimisent la cohérence, la coordination et la prise de mesures en temps opportun dans le domaine de la cybersécurité, et qu'il soumette au Parlement des rapports annuels sur ces efforts.***

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

Le projet de loi C-26 veillerait à ce que les rôles, responsabilités et structures qui existent à l'échelle du gouvernement fédéral optimisent la cohérence, la coordination et la prise de mesures en temps opportun dans le domaine de la cybersécurité. La *Loi sur la protection des cybersystèmes essentiels* (LPCE) garantira une approche intersectorielle uniforme en cybersécurité en réponse à l'interdépendance grandissante des cybersystèmes. Qui plus est, la LPCE autorisera les organismes réglementaires déjà chargés d'assurer les activités de conformité et d'application de la loi aux termes d'autres lois fédérales à exercer les pouvoirs en matière de conformité et d'application de la loi qui leur sont accordés par cette loi et le règlement propre au secteur.

Rôles prévus par la Loi :

Ministre de la Sécurité publique : Le ministre de la Sécurité publique, étant donné son rôle de ministre responsable de la coordination et des politiques de la sécurité et de la cybersécurité nationale, serait responsable de la mise en œuvre et de l'administration de la Loi.

Le ministre de la Sécurité publique soumettrait à l'examen du gouverneur en conseil, en consultation avec les ministres concernés, les directives en matière de cybersécurité qui obligerait tout exploitant désigné à prendre les mesures précises nécessaires pour faire face à une menace ou à une vulnérabilité connue et imminente.

Le ministre serait responsable de déposer un rapport annuel au Parlement sur l'administration de la LPCE.

Sécurité publique Canada : Sécurité publique dirigerait l'élaboration des règlements nécessaires pour mettre la Loi en œuvre, en consultation des principaux ministères fédéraux concernés, le CSTC, les organismes de réglementation et les Canadiens. Ces ministères et leurs ministres mobiliseraient probablement leurs organismes de réglementation respectifs, au besoin, pour mettre à profit leur expertise et contribuer aux discussions qui mèneront à l'élaboration des règlements.

Gouverneur en conseil : Le gouverneur en conseil serait habilité, par décret, à demander à tout exploitant désigné ou catégorie d'exploitants de respecter toute mesure établie dans une directive de cybersécurité (DCS) dans le but de protéger un cybersystème essentiel.

Les règlements seront élaborés par le gouverneur en conseil sur recommandation du ministre de la Sécurité publique.

Organismes de réglementation : Les organismes de réglementation aux termes de la Loi incluraient le ministre de l'Industrie, la Régie de l'énergie du Canada, la Commission canadienne de sûreté nucléaire, le ministre des Transports, le Bureau du surintendant des institutions financières et la Banque du Canada.

Exploitants désignés : La Loi exigerait des exploitants désignés, notamment, qu'ils établissent et mettent en œuvre des programmes de cybersécurité, qu'ils atténuent les risques de la chaîne d'approvisionnement et ceux liés aux tierces parties, qu'ils signalent les incidents de cybersécurité et qu'ils suivent les DCS.

Recommandation 8 : ***Que le gouvernement du Canada insiste sur l'importance et la modernisation de la cybersécurité dans les mandats de ses ministères.***

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

En 2019, la Politique sur les services et le numérique du Conseil du Trésor a été publiée. La Politique et les instruments de soutien constituent un ensemble intégré de règles qui énoncent comment les organisations du gouvernement du Canada gèrent la prestation des services, l'information et les données, la technologie de l'information et la cybersécurité à l'ère numérique. La Politique fait progresser la prestation des services et accroître l'efficacité des

opérations gouvernementales, y compris la modernisation des services numériques et la cybersécurité, en soutien de l'ambition numérique du gouvernement et la Stratégie du Gouvernement numérique du Canada.

Par ailleurs, la Directive sur les services et le numérique décrit l'orientation que doit suivre le représentant ministériel désigné pour la cybersécurité, en collaboration avec le dirigeant principal de l'information du ministère et le dirigeant principal de la sécurité, comme il se doit, pour s'assurer que les exigences en matière de cybersécurité et les mesures appropriées fondées sur les risques sont respectées de manière continue dans le cadre d'une approche visant à identifier, à protéger, à détecter, à répondre et à rétablir afin de protéger les services et les systèmes d'information.

Enfin, le Secrétariat du Conseil du Trésor, en collaboration avec Services partagés Canada, et en consultation du Centre de la sécurité des télécommunications et des autres ministères concernés, est à élaborer une vision et un plan pangouvernementaux globaux pour la cybersécurité des opérations gouvernementales.

Recommandation 9 : ***Que le gouvernement du Canada explore les options pour la création d'une structure canado-américaine de commandement de la cyberdéfense.***

Le gouvernement du Canada est d'accord sur l'importance de collaborer avec les États-Unis sur la cyberdéfense.

Les États-Unis sont le plus proche allié et partenaire du Canada, et la Défense nationale maintien des liens étroits en matière de défense et de sécurité avec les forces armées américaines. La Défense nationale, en partenariat avec le CST, continue de collaborer étroitement avec le Cybercommandement des États-Unis pour s'assurer de notre sécurité et de notre défense collective dans le cyberespace.

Le Commandement de la Défense aérospatiale de l'Amérique du Nord (NORAD) est le seul commandement binational entre le Canada et les États-Unis, et il est déjà en fonction pour ce qui est de la défense du continent, dont le cyberespace. La Défense nationale et le CST continueront de travailler en étroite collaboration avec le Cybercommandement des États-Unis afin de favoriser et d'améliorer la coordination et la collaboration en matière de cyberdéfense opérationnelle. Nous atteindrons nos buts communs grâce à une meilleure compréhension des responsabilités et des pouvoirs respectifs, une meilleure connaissance commune de la situation et en collaborant dans le cadre des opérations cybernétiques lorsqu'il convient de le faire.

Recommandation 10 ***: Que le gouvernement du Canada cherche à déterminer la pleine étendue des activités de désinformation russes – et des campagnes parrainées par d'autres États – qui ciblent le Canada, ainsi que les intervenants, les méthodes, les messages et les plateformes en jeu, de même que les répercussions de la désinformation sur la population canadienne et la sécurité nationale du pays, et qu'il rende compte chaque année de ses constatations au Parlement.***

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Dans le budget de 2022, le gouvernement du Canada s'est engagé à investir 13,4 millions de dollars sur cinq ans, à compter de 2022-2023, pour renouveler et élargir la portée du Mécanisme de réponse rapide du G7, un forum international qui lutte contre les menaces étrangères à la démocratie, par exemple la désinformation parrainée par les États. De plus, le gouvernement a annoncé en août la création d'une équipe spéciale qui aura pour tâche de surveiller et de détecter les opérations d'influence de la Russie, et qui permettra une meilleure coordination à l'échelle mondiale, notamment par l'entremise du Mécanisme de réponse rapide du G7.

La communauté canadienne de la sécurité et du renseignement continue de surveiller la menace d'ingérence russe contre la population et les intérêts du Canada en représailles à notre soutien à l'Ukraine.

Recommandation 11 : ***Que le gouvernement du Canada, en collaboration avec ses alliés et ses partenaires canadiens, continue à exposer et à contrecarrer les campagnes de désinformation russes et celles soutenues par des États étrangers ciblant les Canadiens.***

Le gouvernement est d'accord avec cette recommandation.

Le rôle de secrétariat du Mécanisme de réponse rapide du G7 qu'occupe le Canada facilite la surveillance et la détection de la désinformation parrainée par la Russie et approfondit les liens et la collaboration.

En Russie, des récits et de la désinformation sont employés pour justifier l'invasion de l'Ukraine, discréditer le gouvernement ukrainien et délégitimer la réponse de l'Occident. Le Canada continuera de condamner le recours à la désinformation, dissimulé ou non, non seulement par le gouvernement russe et les médias et mandataires qui lui sont affiliés, mais également par tout État étranger qui tente de déstabiliser la démocratie et de mettre en péril la sécurité des Canadiens.

Recommandation 12 : ***Que le gouvernement du Canada travaille avec des experts, des fournisseurs de services Internet, des plateformes de médias sociaux et des partenaires internationaux pour lutter contre les robots en ligne qui amplifient la désinformation parrainée par des États, et qu'il présente dans un rapport au Parlement ses observations et les mesures qui ont été prises.***

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Le Mécanisme de réponse rapide d'Affaires mondiales Canada : le Canada et ses équipes de communication collaborent avec partenaires internationaux des gouvernements, du milieu universitaire et de la société civile afin de contrer la désinformation parrainée par l'État, y compris la désinformation amplifiée par les réseaux de zombies dans les médias sociaux. Cela se fait au moyen de la promotion de l'information factuelle par les voies officielles et les efforts diplomatiques qui visent à rallier les partenaires d'autres pays pour qu'ils collaborent eux aussi avec les fournisseurs de services et les plateformes de médias sociaux à trouver et à déjouer les réseaux de comptes automatisés qui répandent de la désinformation parrainée par l'État. Le MRR du Canada soutient également les efforts des groupes de réflexion et des organisations de la société civile (OSC) qui effectuent des recherches dans des sources ouvertes pour repérer ces réseaux, attirer l'attention sur leurs tactiques discrètes et malveillantes, qui collaborent également avec les entreprises de médias sociaux pour déjouer ces réseaux.

Recommandation 13 : ***Que le gouvernement du Canada soutienne les journalistes et les universitaires russes indépendants et les aide à exposer la propagande et la désinformation diffusée par le régime.***

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Par l'entremise d'Affaires mondiales Canada, le Canada fournit du soutien pour améliorer la sécurité des journalistes, contrer les restrictions envers les espaces civiques libres et sécuritaires, promouvoir l'intégrité de l'information et contrer la mésinformation et la désinformation à l'échelle mondiale. Bien que cela ne comprenne pas le soutien direct aux journalistes russes, cela inclut le soutien aux journalistes indépendants de l'Europe l'Est, y compris ceux qui sont en exil, dont certains font des reportages en russe à des auditoires russes.

Recommandation 14 : ***Que le gouvernement du Canada travaille de toute urgence en collaboration avec ses partenaires internationaux et nationaux afin de lutter contre le contournement des sanctions, notamment en prenant les mesures qui s'imposent pour recenser et bloquer les biens qui se trouvent au Canada et appartiennent à des individus et des entités russes visées par des sanctions.***

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

Le Canada est conscient de l'importance de résoudre le contournement des sanctions, et d'améliorer l'effet de nos sanctions. À cet égard, le Canada souhaite travailler avec ses alliés internationaux et partenaires nationaux pour trouver des manières de surmonter les difficultés en matière d'application de la loi.

Le Canada coopère aussi régulièrement avec les membres du G7, l'Australie, et la Nouvelle-Zélande pour améliorer l'efficacité des sanctions lorsqu'elles sont imposées. Cela comprend la participation dans des forums multilatéraux sur la mise en œuvre et l'application des sanctions, avec une attention particulière sur la collaboration avec les alliés et les partenaires pour mettre au point des solutions permettant de confronter les tactiques de contournement et de remplacement. Par exemple, le 24 février 2023, les dirigeants du G7 ont annoncé l'établissement d'un mécanisme de coordination d'application visant à maintenir les mesures imposées, les mettre en œuvre dans leur entièreté et en élargir la portée, ce qui comprend la prévention du contournement des sanctions et la prise de mesures en cas de contournement.

Comme première étape, le Canada échange activement des données commerciales avec ses alliés pour déceler les anomalies relatives aux échanges commerciaux et cerner les comportements de contournement et de remplacement. Le gouvernement continuera également à se pencher sur la meilleure manière de traiter les biens non visés pouvant être redirigés vers des tiers. Cela aidera à comprendre et contrer les tactiques de contournement de la Russie pour que les sanctions puissent restreindre la Russie et limiter sa capacité d'agir sur le champ de bataille.

Peu après l'invasion de l'Ukraine par la Russie, l'Australie, le Canada, la France, l'Allemagne, l'Italie, le Japon, le Royaume-Uni, les États-Unis et la Commission européenne ont lancé conjointement le groupe de travail sur les élites, les mandataires et les oligarques russes (REPO), un effort multilatéral qui a utilisé l'échange de renseignements et la coordination pour isoler et exercer une pression sans précédent sur les personnes et entités russes sanctionnées. Les efforts collectifs du groupe de travail REPO ont entraîné le gel de milliards de dollars et, dans certains cas, la saisie de biens. Le groupe de travail s'attaque aux lacunes qui facilitent le contournement des sanctions. Plus particulièrement, le 9 mars 2023, le groupe de travail REPO et ses membres, dont le Canada, ont coordonné la publication d'un conseil mondial qui précise les tactiques utilisées par la Fédération de Russie, les oligarques et leurs mandataires pour contourner les sanctions afin d'accéder à des fonds et de soutenir leurs efforts de guerre. Le Canada continuera de jouer un rôle actif dans le groupe de travail REPO pour coordonner la mise en œuvre des sanctions et sévir contre le contournement des sanctions.

Les Canadiens et les personnes au Canada sont tenus de respecter ces sanctions et de signaler les cas de violations de sanctions. En vertu de la *Loi sur les mesures économiques spéciales* (LMES), toute personne au Canada et tout Canadien à l'extérieur du Canada doit divulguer à la Gendarmerie royale du Canada (GRC) l'existence de biens qu'elle détient ou contrôle dont la propriété ou le contrôle par une personne désignée est soupçonné. Les institutions financières canadiennes continuent de jouer un rôle essentiel et apprécié à cet égard.

L'application des sanctions est un effort pangouvernemental, et Affaires mondiales Canada travaille de près avec les organismes d'application de la loi nationaux pour s'assurer que les sanctions canadiennes sont respectées. La GRC et l'Agence des services frontaliers du

Canada (ASFC) disposent des pouvoirs pour prendre des mesures d'application de la loi en enquêtant sur les violations possibles et en sévissant contre les contraventions délibérées. Par exemple, l'ASFC arrête et retient régulièrement les expéditions interdites à la frontière, et fait preuve de vigilance, souvent en partenariat avec ses alliés internationaux, pour déterminer les cas de contournement possibles. La GRC jour un rôle critique dans la collecte de renseignements sur les biens appartenant à des personnes désignées ou qui sont contrôlés par ceux-ci (c.-à-d., personnes ou entités). Jusqu'à maintenant, la GRC indique que des biens d'une valeur d'environ 122 millions de dollars canadiens au Canada ont été effectivement gelés, et que des transactions financières d'une valeur totale de 292 millions de dollars canadiens ont été bloquées en raison d'interdictions dans le *Règlement sur les mesures économiques spéciales visant la Russie*.

Le budget de 2023 a annoncé d'autres mesures qui renforceront le respect et l'application des sanctions. Le projet de loi C-47 (*Loi d'exécution du budget de 2023*) propose des modifications ciblées de la LMES et de la *Loi sur la justice pour les victimes de dirigeants étrangers corrompus* (LJVDEC) pour appuyer l'efficacité du cadre de saisie, de confiscation ou de destruction adopté en 2022, ainsi que des modifications liées de la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes* pour exiger que le CANAFE communique des renseignements à la ministre des Affaires étrangères dans certaines circonstances.

Le gouvernement a en outre l'intention d'établir des obligations pour que le secteur financier communique les renseignements liés aux sanctions au CANAFE et examinera le mandat du CANAFE afin de déterminer s'il devrait faire l'objet d'une expansion pour contrer le contournement de sanctions. Une mise à jour sera fournie dans la mise à jour économique et financière de l'automne 2023.

Le gouvernement du Canada continuera de travailler avec ses alliés internationaux et partenaires nationaux pour combler les lacunes dans la mise en œuvre de nos sanctions, notamment pour s'attaquer au contournement des sanctions et au remplacement.

Recommandation 15 : *Que le gouvernement du Canada accélère la modernisation du Commandement de la défense aérospatiale de l'Amérique du Nord (NORAD).*

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

Depuis l'annonce faite par la ministre de la Défense nationale en juin 2022 pour un plan sur la modernisation du NORAD, la Défense nationale déploie des efforts afin de mettre en place des projets de modernisation du NORAD et de les intégrer dans le programme général de la défense, de donner suite aux principales priorités du plan de 20 ans et de jeter les bases d'un engagement plus profond des partenaires et des intervenants à l'égard de l'ensemble des initiatives au cours des mois et des années à venir.

La Défense nationale tient une page Web accessible au public indiquant les échéances à jour des projets pour la modernisation du NORAD.

La Défense nationale adopte une approche progressive de la modernisation du NORAD. De nombreux projets atteindront la capacité opérationnelle initiale (COI) vers la fin des années 2020, tandis que d'autres projets plus complexes devraient atteindre la COI vers le milieu des années 2030.

Pour mener à bien cette nouvelle série d'investissements rapidement, la Défense nationale travaille aussi rapidement que possible à l'établissement de nouveaux bureaux de programme et au renforcement de la capacité de nos services internes. Cette approche, qui est fondée sur les leçons tirées de la politique *Protection, Sécurité, Engagement*, favorisera une mise en œuvre rapide et efficace.

Premiers progrès sur les capacités :

- Collaboration accrue avec les États-Unis en matière de planification. Pendant la visite du président Biden au Canada en mars 2023, le premier ministre et le président ont publié un communiqué conjoint du premier ministre et du président des États-Unis pour reconfirmer leur engagement dans la collaboration continue pour moderniser le NORAD.
- Perfectionnement des concepts d'opérations et des options d'emplacement avec les États-Unis dans le cadre du projet de radar transhorizon (OTHR), afin d'optimiser la couverture radar des approches du continent. Pendant la réunion bilatérale avec le président en mars 2023, le premier ministre a confirmé l'intention du Canada d'aligner rapidement notre échéancier pour le radar transhorizon avec celui des États-Unis, et en ce sens il a annoncé la cible d'une date de COI pour un OTHR arctique en 2028.
- Avancement des travaux binationaux en cours sur le commandement et le contrôle en nuage informatique pour la modernisation du NORAD.
- Progrès concernant l'intégration de la capacité supplémentaire de ravitaillement en vol dans le projet Avion stratégique de transport et de ravitaillement en vol (ASTRV) [précédemment approuvé en décembre 2020] annoncé dans la politique *Protection, Sécurité, Engagement*.

Tout comme pour les nouvelles capacités, les investissements dans l'infrastructure seront mis en œuvre selon une approche progressive. Les délais dépendront des exigences opérationnelles et de la coordination continue avec les partenaires dans le Nord et autochtones. Il faudra également tenir compte des délais de construction plus longs et des autres défis associés aux infrastructures dans le Nord.

- La Défense nationale a commencé à travailler avec des partenaires territoriaux, municipaux et autochtones à l'élaboration de plans de développement de sites pour la mise à niveau des infrastructures du Nord à Inuvik, Yellowknife, Iqaluit et Goose Bay.

Le CST a également profité d'investissements pour améliorer ses capacités de défense et de promotion des intérêts nationaux et collectifs du Canada dans le Nord. Il collaborera avec le MDN et les FAC pour protéger les Canadiens contre les menaces aérospatiales nouvelles et émergentes envers le Canada et l'Amérique du Nord.

Recommandation 16 : *Que le gouvernement du Canada s'assure d'avoir la capacité et les fonds nécessaires pour atteindre ses objectifs en matière d'approvisionnement pour la défense du pays, qu'il prenne toutes les mesures qui s'imposent pour faciliter la reconstitution des Forces armées canadiennes et qu'il rende compte périodiquement au Parlement des efforts déployés en vue d'atteindre ces deux objectifs.*

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

La Défense nationale, en collaboration avec SPAC, ISDE et les organismes centraux, dirige de nombreuses initiatives et y participe pour s'assurer qu'elle dispose de la capacité et du financement nécessaire pour atteindre les objectifs en matière d'approvisionnement du Canada. La Défense nationale continuera d'examiner des mesures lui permettant de surmonter les défis liés à l'approvisionnement pour la défense. Cela comprend l'embauche continue des civils pour soutenir les activités d'approvisionnement.

En ce qui a trait à la reconstitution, en octobre 2022, les FAC ont publié la stratégie de maintien des effectifs des FAC, qui est conçue pour alimenter la prise de conscience, favoriser des approches fondées sur des principes pour appuyer les personnes, et aider à orienter les influenceurs stratégiques et les décideurs pour qu'ils soient plus efficaces lorsque vient le temps de prendre des décisions qui ont une incidence sur les membres des FAC. La Défense nationale reconnaît aussi l'accélération du changement de culture dans les FAC pourrait contribuer à une amélioration du recrutement et de la rétention. De plus, la Défense nationale entreprend une évaluation des initiatives de recrutement de la FAC pour faciliter la revitalisation du recrutement et de l'instruction qui devrait se produire au cours des cinq prochaines années.

La Défense nationale présente régulièrement des rapports au Parlement sur des questions liées à la défense, notamment grâce au processus budgétaire et les processus d'établissement de rapports annuels comme le Rapport sur les résultats ministériels. La Défense nationale continuera à informer le Parlement par l'entremise de ces mécanismes, et bien d'autres.

Recommandation 17 : *Que le gouvernement du Canada respecte ses engagements envers ses alliées de l'OTAN et atteigne la cible de 2 % des dépenses pour la défense de l'Alliance.*

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Le Canada maintient fermement son engagement envers l'OTAN et en faveur de la défense de la sécurité euro atlantique ainsi que d'un ordre international fondé sur des règles. Dans l'ensemble, les dépenses et l'approvisionnement pour la défense du Canada sont fondés sur des analyses des menaces et des évaluations de ses besoins plutôt que sur des cibles de dépenses arbitraires.

Le Canada demeure résolu à respecter les hausses du budget pour la défense qui ont été établies dans la politique de défense du Canada, *Protection, Sécurité, Engagement*. Ces hausses feront passer le budget de défense total du Canada de 18,9 milliards de dollars en 2016-2017 à 32,7 milliards de dollars d'ici 2026-2027, ce qui représente une augmentation de plus de 70 %. Par ailleurs, au cours des 20 prochaines années, le Canada investira 38,6 milliards de dollars selon la comptabilité d'exercice dans la modernisation du NORAD. Ces investissements assureront la sécurité de l'Amérique du Nord et lui permettront ainsi de projeter sa puissance à l'appui des alliées de l'OTAN sans être confronté sur le continent à des menaces émergentes et futures.

Le Canada maintient son engagement constant et fiable en faveur des missions, des opérations et des activités de l'OTAN. Cela comprend la direction et l'élargissement du groupement tactique de la présence avancée renforcée en Lettonie, le soutien des forces maritimes de l'OTAN en déployant jusqu'à trois navires de surface ainsi que la prestation d'une aide militaire létale et non létale à l'Ukraine. Le Canada soutient sans réserve le renouvellement de l'engagement en matière d'investissements de défense (EID) pendant le prochain Sommet des dirigeants, qui aura lieu en juillet.

Dans l'avenir, il faut favoriser la réussite de l'OTAN, notamment en établissant un équilibre entre l'ambition et les objectifs réalisables. Comme l'Alliance adapte sa posture de dissuasion et de défense pour relever les défis de l'avenir, un EID renouvelé doit rendre compte des contributions des alliés dans les trois domaines suivants : l'argent, les capacités et les contributions. Il doit également cadrer avec les engagements pris par les dirigeants dans le cadre du Concept stratégique 2022.

Recommandation 18 : *Que le gouvernement du Canada mette en place un registre des agents étrangers ou une mesure équivalente à la loi australienne sur le régime de transparence en matière d'influence étrangère.*

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Certains gouvernements étrangers ou leurs mandataires utilisent des personnes ou des entités pour tenter d'influencer, secrètement ou de manière non transparente, les politiques du gouvernement du Canada ou le discours public canadien. Ces activités peuvent porter un préjudice à l'intérêt national, à la sécurité nationale et à la confiance du public dans les processus et les institutions démocratiques. La menace posée par l'ingérence étrangère est maintenant plus sophistiquée et omniprésente et vise le Canada et les Canadiens. C'est pourquoi le gouvernement du Canada a lancé en mars 2022 des consultations auprès du public et des intervenants sur un registre visant la transparence en matière d'influence étrangère. Les consultations en ligne à ce sujet ont duré 60 jours et permis de recueillir près de 1000 réponses fournies par un vaste éventail de répondants d'un bout à l'autre du Canada en vue de guider la

création du registre. Des discussions bilatérales et en table ronde avec des intervenants (organismes communautaires, groupes autochtones, intervenants provinciaux et territoriaux, etc.) se sont poursuivies au-delà de cette date. Le gouvernement du Canada continue d'examiner les outils et les pouvoirs dont il dispose pour s'assurer que son approche suit le rythme de l'évolution du contexte de menace et est adaptée au contexte canadien.

Recommandation 19 : ***Que le gouvernement du Canada publie une stratégie globale et intégrée sur la sécurité nationale, qui prend en compte les résultats d'un examen interne des capacités du Canada en matière de sécurité nationale.***

Le gouvernement accepte d'examiner cette recommandation plus en détail.
Protéger une société ouverte : la politique canadienne de sécurité nationale a été publiée en 2004 et représentait la toute première prise de position de ce genre par le gouvernement du Canada. Cette politique établit un cadre stratégique et un plan d'action conçus pour s'assurer que le Canada est préparé à faire face aux menaces présentes et futures et peut les contrer. Le gouvernement du Canada est conscient que le contexte de la sécurité nationale a évolué depuis qu'il a publié cette politique et que les menaces d'aujourd'hui posent une multitude de problèmes et défis complexes et multidimensionnels, dont l'ingérence étrangère, la cybersécurité, l'espace et les technologies émergentes, l'extrémisme violent et le terrorisme, la sécurité à la frontière, la sécurité environnementale et sanitaire ainsi que le lien entre le crime organisé et la sécurité nationale. Compte tenu du nouveau contexte de menace, le gouvernement du Canada est également conscient qu'il doit s'assurer que la boîte à outils pour protéger la sécurité nationale demeure souple et adaptable et peut ainsi continuer de prévenir et d'atténuer ces problèmes et défis et d'y répondre.

Recommandation 20 : ***Que, conformément à l'article 34 de la*** **Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement,** ***la Chambre des communes désigne le Comité permanent de la sécurité publique et nationale pour mener un examen approfondi des dispositions et de l'application de cette loi.***

Le gouvernement prend note de cette recommandation.

L'examen de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, qui doit être effectué cinq ans après son entrée en vigueur, n'a pas encore commencé. Les décisions concernant le moment où commencera l'examen et le comité qui s'en chargera relèvent du Parlement.

Recommandation 21 : ***Que le gouvernement du Canada présente au Parlement une évaluation annuelle des menaces touchant la sécurité nationale du pays.***

Le gouvernement accepte d'examiner cette recommandation plus en détail.

Le gouvernement du Canada, dans la poursuite des efforts de promouvoir la transparence, examine actuellement des opportunités de partager avec les Canadiens et Canadiennes une idée des priorités en matière de renseignement établies par le Cabinet. Les priorités en matière de renseignement du gouvernement sont définies chaque année au moyen de discussions et de consultations avec les ministres représentant le milieu canadien de la sécurité et du renseignement et fournissent des directives aux ministères et aux organismes ayant un mandat de collecte.

Outre les priorités en matière de renseignement, les ministères et les organismes représentant le milieu canadien de la sécurité et du renseignement publient des rapports non classifiés auxquels peuvent accéder facilement le Parlement et le public. À titre d'exemple, mentionnons le Rapport public du Service canadien du renseignement de sécurité (SCRS), le Rapport annuel sur la Police fédérale de la GRC, le Rapport annuel du Centre de la sécurité des télécommunications ainsi que les plans ministériels et le rapport sur les résultats ministériels annuels des ministères et des organismes fédéraux, dont Sécurité publique Canada.

Conclusion

Le gouvernement reconnaît la valeur des idées et des recommandations fournies par le Comité. Le présent Rapport constituera une ressource précieuse qui permettra au gouvernement de prendre des mesures pour contrer les menaces que pose la Russie pour la sécurité nationale du Canada.

Je vous prie d'agréer mes salutations distinguées,

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

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

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

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