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

John Brassard, député
Président du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique
Chambre des communes
Ottawa (Ontario)
K1A 0A6

Monsieur Brassard,

En tant que ministre de la Sécurité publique, des Institutions démocratiques et des Affaires intergouvernementales, et au nom du gouvernement du Canada, j'ai le plaisir de répondre au dixième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, intitulé « L'ingérence étrangère et les menaces entourant l'intégrité des institutions démocratiques de la propriété intellectuelle et de l'État canadien ».

Je tiens à saluer les efforts déployés par le Comité dans le cadre de son examen de l'ingérence étrangère au Canada. L'ingérence étrangère constitue l'une des plus grandes menaces pour la sécurité nationale, le mode de vie, la prospérité économique et la souveraineté du Canada. Le gouvernement accepte en principe la teneur générale et la majorité des recommandations du Comité. Bien que le gouvernement ne rejette aucune des recommandations, des études ou des examens plus poussés s'imposent dans certains cas.

Le gouvernement s'engage à lutter contre la menace posée par l'ingérence étrangère en modernisant le cadre stratégique et législatif canadien dans une façon qui corresponde à nos valeurs nationales, respecte les droits et libertés des Canadiens, et tienne compte d'une grande diversité de points de vue et d'expériences. Le gouvernement a déjà pris plusieurs mesures afin d'adapter la boîte à outils du Canada pour lutter contre l'ingérence étrangère de manière à mettre l'accent sur la transparence et l'engagement citoyen. À titre d'exemple, les consultations publiques sur la création d'un registre pour la transparence en matière d'influence étrangère se sont conclues le 9 mai 2023. Le 24 novembre 2023, le gouvernement du Canada a aussi lancé des consultations publiques sur des modifications possibles à la *Loi sur le Service canadien du renseignement de sécurité*, au *Code criminel*, à la *Loi sur la protection de l'information* et à la *Loi sur la preuve au Canada* en vue de renforcer la capacité du gouvernement de lutter contre l'ingérence étrangère.

Ces initiatives, parallèlement aux autres engagements pris par le gouvernement du Canada pour contrer la menace posée par l'ingérence étrangère, sont mentionnées dans la réponse du gouvernement aux 22 recommandations du Comité, ci-jointe.

Une fois de plus, au nom du gouvernement du Canada, je tiens à remercier les membres du Comité permanent de l’accès à l’information, de la protection des renseignements personnels et de l’éthique pour leur diligence et leur engagement dans la réalisation de leurs travaux.

Veuillez agréer, Monsieur le Président, l’expression de mes sentiments distingués.

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

Recommandation 1 : Que le gouvernement du Canada améliore le système de déclassification des documents historiques, tel que recommandé dans son rapport sur l'état du système d'accès à l'information publié en juin 2023, et établisse et mette en œuvre des directives de classification plus claires pour les documents portant sur la sécurité nationale.

Le gouvernement accepte cette recommandation.

Le gouvernement reconnaît que la déclassification des documents historiques, y compris les documents archivés ayant trait à la sécurité nationale, constitue un élément essentiel de la transparence gouvernementale. Celle-ci est indispensable à la sécurité nationale et à la lutte contre l'ingérence étrangère (IE) en favorisant la confiance des Canadiens à l'égard des institutions démocratiques.

Le gouvernement dispose d'un modèle permettant de classer l'information selon la Norme sur la catégorisation de sécurité établie dans la *Directive sur la gestion de la sécurité*. Le processus de catégorisation de sécurité tient compte des critères d'exception et d'exclusion prévus dans la *Loi sur l'accès l'information* et la *Loi sur la protection des renseignements personnels* pour éviter que des ressources ne soient déployées en vue de protéger de l'information pouvant être rendue publique.

Afin de favoriser encore davantage la déclassification et le déclassement des documents au sein des institutions, en décembre 2023, le gouvernement a publié un avis de mise en œuvre intitulé « Tirer parti de l'accès à l'information pour promouvoir la déclassification et le déclassement des documents gouvernementaux ». L'avis permet d'orienter les institutions fédérales sur la manière de tirer parti des processus et formations en place en matière d'accès à l'information pour promouvoir la déclassification ou le déclassement de la catégorie de sécurité attribuée aux ressources d'information. La capacité de déclassifier les documents de façon uniforme à l'échelle du gouvernement du Canada permettra d'alléger le fardeau qui pèse sur le système d'accès à l'information et de clarifier les mesures que les ministères et organismes doivent prendre à ce chapitre.

En outre, le milieu de la sécurité nationale et du renseignement, Bibliothèque et Archives Canada, le Secrétariat du Conseil du Trésor (CST), le ministère de la Justice et Sécurité publique Canada (SPC) collaborent en ce moment à une série d'initiatives axées sur la déclassification systématique des documents historiques en général et des documents portant sur la sécurité nationale en particulier. Ces initiatives visent notamment à :

- Créer un groupe de travail interministériel spécial sur la déclassification, lequel formule des conseils sur la déclassification systématique et proactive des documents historiques liés à la sécurité nationale et au renseignement, et oriente les travaux stratégiques en matière de déclassification dans l'ensemble de l'appareil

gouvernemental;

- Élaborer l'ébauche d'un cadre de déclassification national des documents liés à la sécurité nationale et au renseignement en vue de l'adoption d'une approche uniforme et systématique pour la déclassification des documents historiques, en fonction des pratiques exemplaires existantes et des conseils formulés par le groupe de travail mentionné ci-dessus.

Recommandation 2 : Que le gouvernement du Canada modifie la *Loi sur l'accès à l'information* afin de préciser que le système d'accès à l'information repose sur une culture d'ouverture et de transparence et qu'il mette en œuvre les autres recommandations du Comité dans son rapport sur l'état du système d'accès à l'information publié en juin 2023.

Le gouvernement prend bonne note de cette recommandation.

Le gouvernement souligne qu'en septembre 2023, il a présenté une réponse exhaustive au rapport du Comité ETHI sur l'état du système d'accès à l'information du Canada. Des travaux sont en cours afin de mettre en œuvre une série de mesures pour donner suite aux recommandations de ce rapport, dont plusieurs visant à améliorer l'ouverture et la transparence.

Recommandation 3 : Que le gouvernement du Canada demande un partage accru et régulier d'information pertinente au public par le Service canadien du renseignement de sécurité afin d'augmenter la littéracie en matière de sécurité nationale.

Le gouvernement accepte cette recommandation.

Le Service canadien du renseignement de sécurité (SCRS) s'est engagé à mobiliser et à sensibiliser les Canadiens à l'égard des questions de sécurité nationale. Étant donné le nombre croissant de menaces auxquelles le Canada doit faire face, le SCRS a déployé des efforts considérables afin d'accroître la sensibilisation aux menaces et continuera de le faire. Il s'agit notamment d'activités de mobilisation ciblées visant des groupes et associations communautaires, le secteur privé, les établissements d'enseignement supérieur et de recherche, et des organisations municipales et autochtones, de même que des activités de sensibilisation générale destinées au grand public.

Le SCRS est toutefois limité dans sa capacité de transmettre de l'information classifiée à des entités autres que le gouvernement du Canada. Ces contraintes l'empêchent de communiquer directement à des partenaires nationaux, comme le secteur privé et les établissements d'enseignement supérieur, de l'information qui les aiderait à renforcer leur résilience aux menaces d'IE et d'espionnage. C'est pour cette raison que le gouvernement consulte les Canadiens au sujet de possibles modifications à la *Loi sur le*

SCRS, qui autoriseraient le SCRS à communiquer de l'information à d'autres entités ou personnes, en plus de l'appareil gouvernemental, sur les menaces pour la sécurité du Canada, dans le but d'accroître la sensibilisation et la résilience dans ce domaine.

Néanmoins, afin de maintenir sa capacité d'enquêter sur les menaces et de formuler des conseils à cet égard, le SCRS a la responsabilité de protéger ses sources et ses méthodes. Par conséquent, bien qu'il se soit engagé à communiquer de l'information au public dans la mesure du possible et ait multiplié ses efforts en ce sens dans les dernières années, par des discours et d'autres activités, il y aura toujours des limites quant à l'information qu'il peut diffuser.

En collaboration avec le gouvernement fédéral, les gouvernements provinciaux, municipaux et autochtones, le secteur privé et le milieu universitaire, les groupes communautaires et l'ensemble des Canadiens ont tous un rôle à jouer pour accroître la littéracie et la résilience au chapitre de la sécurité nationale. Le gouvernement du Canada est disposé à établir de nouveaux partenariats dans ce but.

Recommandation 4 : Que le gouvernement du Canada renforce les règles et les sanctions encadrant les divulgations illicites d'information concernant la sécurité nationale.

Le gouvernement prend bonne note de cette recommandation.

La *Loi sur la protection de l'information* (LPI) est essentielle à la lutte contre l'espionnage. L'alinéa 4(1)(a) de la LPI (« communication illicite ») prévoit que commet une infraction quiconque communique de manière illicite des renseignements secrets ou officiels à des personnes qui ne sont pas autorisées à les recevoir. Le paragraphe 4(3) (« réception ») et l'alinéa 4(4)(b) (« permettre la possession ») prévoient quant à eux que commet une infraction quiconque reçoit de manière illicite des renseignements secrets ou remet de tels renseignements à des personnes qui ne sont pas autorisées à les recevoir.

En 2006, l'alinéa 4(1)(a), le paragraphe 4(3) et l'alinéa 4(4)(b) ont été contestés avec succès devant la Cour supérieure de justice de l'Ontario au motif qu'ils allaient à l'encontre de l'alinéa 2(b) (« liberté d'expression ») et de l'article 7 (« droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale ») de la *Charte*. Toutefois, le régime prévu aux articles 8 à 15 de la LPI est toujours en vigueur et a été invoqué afin d'obtenir des condamnations pour communication illicite de renseignements opérationnels spéciaux.

Le gouvernement étudie en ce moment s'il convient et s'il est opportun d'apporter des modifications à la LPI. Il sollicite l'opinion des Canadiens sur cette question par la tenue de consultations publiques sur les modifications à

la loi envisagées pour contrer la menace d'IE, comme il en est question dans la réponse à la recommandation 5.

Recommandation 5 : Que le gouvernement du Canada s'engage à ce que tous mécanismes législatifs élaborés dans le but de contrer l'ingérence étrangère tiennent compte des conséquences possibles sur des personnes et des communautés qui sont déjà victimisées ou ciblées par l'ingérence étrangère au Canada et qu'il s'engage à inviter ces communautés à participer à l'élaboration des mesures permettant de contrer les effets de l'ingérence qu'elles subissent.

Le gouvernement accepte cette recommandation.

Pour le gouvernement, il est crucial de comprendre en quoi divers groupes sont particulièrement ou disproportiellement touchés par l'IE afin de lutter contre cette menace. En vue de favoriser la transparence et la confiance, SPC a tenu des consultations en personne et en ligne sur la création d'un éventuel registre pour la transparence en matière d'influence étrangère (RTMIE) pour le Canada au printemps de 2023.

Le but des consultations était de solliciter l'opinion du grand public et des intervenants canadiens sur la façon dont le Canada pourrait s'y prendre pour concevoir et mettre en œuvre un RTMIE afin de renforcer la sécurité nationale grâce à une plus grande transparence et à la sensibilisation accrue du public à l'IE au Canada. Plus de 1 000 répondants en ligne et plus de 80 groupes d'intervenants clés ont participé aux consultations.

Le 24 novembre 2023, le gouvernement a lancé d'autres consultations sur des modifications législatives possibles à l'appui de la lutte contre l'IE. Le gouvernement a par la suite tenu une série de tables rondes avec les communautés touchées par les activités d'IE afin d'obtenir leur point de vue sur d'éventuels mécanismes législatifs. Parmi les participants figuraient des membres de la Table ronde transculturelle sur la sécurité et des représentants de personnes au Canada qui ont été ciblées par des États étrangers en raison de leur activisme.

Les modifications possibles dont il est question dans les consultations publiques comprennent des modifications à la *Loi sur le SCRS*, qui permettraient au SCRS de communiquer de l'information à des intervenants non fédéraux. Si le SCRS disposait d'une capacité accrue de communication de renseignements, il pourrait aider ces intervenants à accroître leur résilience à l'IE. D'autres modifications proposées visent à renforcer les lois visant à lutter contre les menaces de violence issues de l'influence étrangère à l'endroit de personnes et de créer de nouvelles infractions afin de protéger les processus démocratiques de l'IE à tous les échelons du gouvernement.

Les commentaires fournis par des groupes communautaires, des personnes et autres participants contribueront à orienter les éventuelles modifications législatives qui pourraient être présentées au Parlement en vue de contrer l'IE.

Recommandation 6 : Que le gouvernement du Canada révise et mette à jour la politique en matière de sécurité nationale du Canada et que cette nouvelle politique définisse les règles permettant au Service canadien du renseignement de sécurité d'avertir directement les membres du Parlement canadien de menaces liées à l'ingérence étrangère.

Le gouvernement prend bonne note de cette recommandation.

Le gouvernement évalue et adapte continuellement le cadre stratégique en matière de sécurité nationale du Canada. À l'heure actuelle, la *Loi sur le SCRS* limite les pouvoirs de communication de renseignements du SCRS, sauf dans quelques situations. Pour composer avec ces contraintes, le SCRS donne des séances d'information non classifiées de haut niveau sur les menaces générales aux personnes ciblées par l'ingérence étrangère. Par exemple, en 2021, le SCRS a offert 45 séances d'information à des parlementaires, soit deux sénateurs et 43 députés. En 2022, le SCRS a organisé 49 séances d'information avec des élus fédéraux. Le SCRS continuera d'offrir de telles séances aux élus en fonction des besoins, et toute menace pour la sécurité d'une personne sera toujours signalée immédiatement aux organismes d'application de la loi. Dans son rapport publié le 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 s'est engagé à mettre sur pied un nouveau programme de séances d'information non classifiées à l'intention des parlementaires et de leur personnel et à offrir des séances d'information aux parlementaires après leur assermentation ainsi que sur une base régulière par la suite. En mai 2023, le ministre de la Sécurité publique a publié des directives ministérielles dans lesquelles il indiquait que les menaces à la sécurité du Canada dirigées contre le Parlement et les parlementaires continueront de faire l'objet de la plus grande attention de la part du SCRS.

Créé en 2004 aux termes de la Politique canadienne de sécurité nationale, le Centre intégré d'évaluation du terrorisme (CIET), qui mène ses activités conformément aux pouvoirs de la *Loi sur le SCRS*, a aussi été appelé à fournir des évaluations de la menace élargies, au-delà de l'extrémisme violent, leur portée usuelle. Le CIET a publié 13 évaluations des menaces visant des fonctionnaires fédéraux et a offert quatre séances d'information aux personnes concernées. Ces évaluations portaient entre autres sur l'IE.

Le gouvernement s'efforcera de faire en sorte que tout examen éventuel ou toute mise à jour du cadre stratégique en matière de sécurité nationale, y compris les politiques touchant le SCRS, tiennent compte des menaces en évolution comme celles liées à l'IE.

Recommandation 7 : Que le gouvernement du Canada utilise pleinement la législation existante, comme la *Loi sur la protection de l'information* et d'autres lois pertinentes, en tant que ressources et outils d'application de la loi.

Le gouvernement accepte cette recommandation.

Le gouvernement tire pleinement parti des mesures législatives existantes pour s'attaquer aux divers types de menaces issues de l'IE qui pèsent contre le Canada. Les organismes d'enquête et d'application de la loi peuvent s'appuyer sur la LPI, la *Loi sur les infractions en matière de sécurité* (LIMS), le *Code criminel* et d'autres lois afin d'enquêter sur des actes criminels liés à l'IE. À titre d'exemple, la LPI comporte de nombreuses infractions portant sur l'IE, qui permettent d'intenter des poursuites criminelles contre les individus complices d'espionnage économique, de communication de renseignements classifiés, et de menaces et de violence issues de l'influence étrangère. De même, le *Code criminel* comporte des infractions pour, entre autres, abus de confiance, harcèlement criminel, utilisation non autorisée d'ordinateur, intimidation et corruption, qui permettent d'enquêter sur les acteurs qui se livrent à l'IE et leurs alliés, de les poursuivre en justice et de les condamner. La GRC mène des enquêtes sur les activités criminelles liées à l'IE et travaille de concert avec le Service des poursuites pénales du Canada pour porter des accusations lorsqu'il y a lieu de le faire. Des accusations d'espionnage économique ont été déposées pour la première fois en novembre 2022.

Même lorsqu'il n'est pas possible d'intenter des poursuites criminelles contre les acteurs qui se livrent à l'IE, le gouvernement du Canada peut mettre à profit tous les autres outils législatifs à sa disposition pour perturber et prévenir les activités liées à l'IE. À titre d'exemple, la *Loi sur Investissement Canada* prévoit un mécanisme d'examen qui permet au gouvernement d'examiner les investissements étrangers pour vérifier qu'ils ne portent pas atteinte à la sécurité nationale du Canada. Cet examen vise notamment à s'assurer que les investissements ne serviront pas à promouvoir les objectifs stratégiques d'États étrangers au détriment de la sécurité et de la prospérité économique du Canada. Dans la même veine, le *Décret sur les passeports canadiens* permet au gouvernement du Canada d'annuler ou de révoquer le passeport d'une personne soupçonnée de se livrer à des activités liées à l'IE.

Recommandation 8 : Que le gouvernement du Canada mette à jour sa politique de sécurité nationale afin d'y inclure une politique sur les menaces causées par l'utilisation de l'intelligence artificielle par des acteurs étrangers.

Le gouvernement examinera cette recommandation de façon approfondie.

Le gouvernement du Canada se positionne pour être prêt à réagir aux menaces en évolution causées par l'utilisation de l'intelligence artificielle (IA) par des acteurs étrangers par l'entremise de diverses initiatives, et être en mesure de le faire.

Par exemple, le Centre de sécurité de la recherche de SPC examine les demandes de subventions, y compris celles qui mettent en jeu des technologies d'IA, conformément aux Lignes directrices sur la sécurité nationale pour les partenariats de recherche, produit et fournit des conseils sur la protection de la recherche et fournit des conseils spécialisés aux institutions de recherche en fonction de leurs besoins particuliers. Par ailleurs, le Centre de la sécurité des télécommunications Canada (CST), Affaires mondiales Canada (AMC), la Gendarmerie royale du Canada (GRC) et le SCRS ont tous mis en œuvre des initiatives qui sont en cours et qui permettent de faire des recherches afin d'établir des lignes directrices visant l'utilisation responsable de l'IA dans leurs organisations respectives.

SPC dirige également l'élaboration d'une version mise à jour de la Stratégie nationale de cybersécurité (ci-après « la Stratégie ») en collaboration avec les intervenants du milieu fédéral de la cybersécurité. À mesure que l'IA évolue, il est important de prendre en considération ses liens actuels et éventuels avec la cybersécurité nationale. La nouvelle Stratégie décrirait l'approche à long terme utilisée par le Canada pour protéger sa sécurité et son économie, dissuader les auteurs de menaces et promouvoir l'adoption, sur la scène internationale, d'un comportement fondé des normes dans le cyberespace.

Recommandation 9 : Que le gouvernement du Canada investisse dans les connaissances et les capacités numériques stratégiques du Canada et de ses agences de sécurité nationale afin d'améliorer les capacités à détecter et contrer les activités d'ingérence étrangère menées avec l'aide de l'intelligence artificielle.

Le gouvernement accepte cette recommandation.

Le gouvernement du Canada continuera de demeurer informé des menaces en évolution, de les évaluer et d'y réagir, y compris des menaces découlant des nouvelles technologies comme l'IA, qui peuvent accélérer ou renforcer les activités d'IE.

Le gouvernement investit à l'heure actuelle dans des programmes et il mène des campagnes de sensibilisation pour accroître la littératie numérique au Canada, et ce, dans le but de réagir aux cybermenaces et à la désinformation venant de différents fronts. Le Centre canadien pour la cybersécurité du CST, qui est l'autorité technique du Canada en matière de cybersécurité, mène des campagnes de sensibilisation comme « Pensez cybersécurité » et diffuse régulièrement des évaluations des menaces et des documents d'orientation pour éduquer les Canadiens sur la gamme de cybermenaces auxquelles ils peuvent être confrontés, comme celles qui découlent de l'IA. Les documents d'orientation du CST comprennent les suivants : l'Évaluation des cybermenaces nationales, Cybermenaces contre le processus démocratique du Canada, les Conseils sur l'IA générative et le Rapport annuel du CST, ainsi que des alertes et des avis réguliers.

Patrimoine canadien a également investi plus de 21 millions de dollars depuis 2019 pour les activités liées aux médias numériques et à l'éducation civique au Canada dans le cadre du Programme de contributions en matière de citoyenneté numérique (PCCN). Le PCCN aide à financer des projets dirigés par des chercheurs et des organisations de la société civile pour mieux comprendre la désinformation en ligne, y compris la désinformation liée à l'IA, et renforcer la résilience à cet égard. Le dernier appel de propositions du PCCN a pour but d'appuyer les projets qui visent à élaborer et à publier des outils qui aideront la population canadienne à repérer le contenu créé et diffusé par des robots ou par la technologie de l'IA, et de renforcer la résilience à la mésinformation et à la désinformation découlant du ciblage de Canadiens par les gouvernements étrangers, notamment les communautés de la diaspora.

Pour favoriser les capacités de création canadiennes en matière d'IA, le CST investit également dans des compétences techniques et soutient la recherche et le développement en matière d'AI. Par exemple, le CST et le Conseil de recherches en sciences naturelles et en génie du Canada ont établi un partenariat pour financer les communautés de recherche sur des technologies d'IA robustes, sûres et sécurisées. En plus de contribuer à l'ensemble des connaissances sur l'IA, le financement aidera à produire une nouvelle génération de scientifiques et d'ingénieurs de données qui sont sensibles aux enjeux relatifs à des technologies d'IA robustes sûres et sécurisées. Le CST finance aussi la formation en matière d'IA dont les employés du gouvernement du Canada ont besoin pour acquérir les compétences nécessaires à l'exploitation des capacités de l'IA et être en mesure de se protéger contre les risques tout en bâtissant la confiance dans le déploiement de technologies d'IA dans les contextes organisationnels. Les efforts susmentionnés contribuent tous à renforcer les capacités du Canada en matière de cybersécurité.

Recommandation 10 : Que le gouvernement du Canada s'assure que le Service canadien du renseignement de sécurité offre davantage de formation et d'information aux parlementaires et fonctionnaires canadiens sur les menaces que représentent l'ingérence étrangère au Canada, les différentes tactiques utilisées par des acteurs étrangers et les moyens de se protéger contre celles-ci.

Le gouvernement accepte cette recommandation.

Dans le cadre de son mandat prévu par sa loi habilitante, le SCRS offre aux parlementaires le plus de détails possible pour atténuer les menaces d'IE. Par exemple, en 2021, le SCRS a offert 45 séances d'information à deux sénateurs et 43 députés.. En 2022, le SCRS a donné 49 séances d'information à des représentants élus fédéraux. Le SCRS continuera de donner des séances d'information aux représentants au besoin, et les situations de menaces à la sécurité personnelle continueront d'être renvoyées immédiatement aux organismes d'application de la loi.

D’autres ministères du gouvernement du Canada s’assurent que les parlementaires sont au courant de la menace d’IE, puisque la lutte contre celle-ci est un effort pansociétal. Par exemple, dans le cadre du plan pour protéger la démocratie canadienne, les partis politiques reconnus à la Chambre des communes sont en mesure de nommer des membres du personnel clés qui se verront accorder une autorisation de sécurité leur permettant de recevoir des séances d’information classifiées durant la période électorale. Dans le 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 s’est engagé à donner des séances d’information non classifiées aux parlementaires et à leur personnel et à offrir des séances d’information aux parlementaires à la suite de leur assermentation ainsi que sur une base régulière à l’avenir. Le gouvernement s’est également engagé à mettre en œuvre une trousse d’outils contre la désinformation et à offrir une formation sur l’IE aux parlementaires. Les travaux visent à concrétiser ces engagement sont en cours. Certains organismes gouvernementaux, par exemple le CST, AMC, l’École de la fonction publique du Canada et le SCT ont depuis déployé des efforts pour produire des connaissances sur l’IE et les transmettre aux parlementaires.

Recommandation 11 : Que le gouvernement du Canada mette sur pied un programme de sensibilisation sur l’ingérence étrangère à l’usage des établissements d’enseignement et de recherche.

Le gouvernement accepte cette recommandation.

Dans le budget de 2022, SPC a reçu du financement pour établir le Centre de la sécurité de la recherche, qui est chargé de sensibiliser les établissements universitaires, les gouvernements provinciaux et les chercheurs des quatre coins du Canada sur la sécurité de la recherche. Par l’entremise d’un réseau de six conseillers régionaux situés à divers endroits dans le pays, le Centre de la sécurité de la recherche diffuse des conseils, donne des ateliers sur la sécurité de la recherche et aide des intervenants externes à accéder aux services et à l’information du gouvernement du Canada. Le programme « Science en sécurité », qui offre des ateliers à la communauté scientifique et universitaire et donne un aperçu général des menaces pour la sécurité de la recherche et des mesures d’atténuation.

Les efforts susmentionnés sont complétés par le programme de liaison-recherche et collaboration avec les intervenants du SCRS. Le programme vise à transmettre de l’information au plus grand nombre de personnes possible, tout en respectant les limites législatives et en matière de sécurité. Par exemple, le SCRS présente régulièrement des séances d’information sur la sécurité et les stratégies d’atténuation à des représentants des universités et des membres du corps enseignant universitaire sur le contexte de la menace. Le SCRS a donné des séances d’information à plus de 200 organisations et à plus de 1 000 personnes sur les menaces éventuelles et leur a présenté des outils pour qu’elles puissent se protéger, ainsi que protéger leurs projets de

recherche et leurs employés. Le SCRS a également des engagements bilatéraux réguliers avec plus de 70 universités, collèges et associations universitaires et collégiales. Cela permet aux intervenants, y compris à la communauté universitaire, de travailler en partenariat avec le gouvernement du Canada et de bâtir la résilience à l'égard des activités constituant des menaces, y compris l'IE sur les campus.

Innovation, Sciences et Développement économique (ISDE) dirige le Groupe de travail mixte du gouvernement du Canada et des universités, qui est composé de plusieurs partenaires du gouvernement du Canada ainsi que d'établissements de recherche canadiens et qui sert de table de consultation sur les politiques de sécurité de la recherche. ISDE se charge également de la tenue à jour du portail Protégez votre recherche, qui est mis à jour régulièrement et qui présente de l'information utile, des conseils et des cours en ligne sur la façon la plus efficace de protéger la recherche et la propriété intellectuelle. Le budget de 2022 prévoyait également un financement permanent de 25 millions de dollars pour le Fonds de soutien à la recherche, pour renforcer la capacité des établissements d'enseignement postsecondaire de cerner, d'évaluer et d'atténuer les risques à la sécurité de la recherche.

En plus de déployer des efforts continus pour s'assurer que les principaux intervenants sont au courant des menaces pour la sécurité de la recherche, le CST et son Centre pour la cybersécurité sont une source unifiée d'avis, de conseils, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiens et les organisations canadiennes, y compris les établissements d'enseignement supérieur. La GRC, par l'entremise du groupe Mobilisation stratégique et sensibilisation de la Police fédérale (MSS-PF) participe également à des activités de mobilisation avec le secteur universitaire. Le groupe MSS-PF collabore avec des intervenants, dont notamment des universitaires, pour distribuer des publications et tenir des séances d'information opérationnelles en personne sur les secteurs d'exécution de la loi de la Police fédérale, notamment l'IE.

Recommandation 12 : Que le gouvernement du Canada, en collaboration avec les agences de sécurité nationale, établisse des mécanismes rigoureux visant à s'assurer que tout accord contractuel entre le Canada et des fournisseurs étrangers ne crée pas de risque élevé pour la sécurité nationale.

Le gouvernement fera un examen approfondi de cette recommandation.

Le gouvernement reconnaît l'importance d'atténuer les menaces pour la sécurité nationale dans l'approvisionnement en biens et en services et a mis en place des mécanismes pour repérer les risques et les gérer. Par exemple, la Liste de vérification des exigences relatives à la sécurité (LVERS) sert à cerner les exigences en matière de sécurité puis à déterminer les dispositions en matière de sécurité qu'il faut inclure dans les contrats.

Le gouvernement tente également d'établir des accords de sécurité bilatéraux avec des gouvernements étrangers partenaires pour garantir

l'échange d'information réciproque sur les fournisseurs étrangers. Compte tenu de ce qui précède, le CST mène des évaluations de l'intégrité de la chaîne d'approvisionnement (ICA) pour l'acquisition de technologies de l'information et des communications (TIC) utilisées par le gouvernement du Canada. Ces évaluations visent à repérer les menaces et les risques associés à la chaîne d'approvisionnement ainsi que les vulnérabilités de celle-ci, et elles comprennent une évaluation de la propriété, du contrôle ou de l'influence de l'étranger visant à atténuer le risque d'IE dans les renseignements et les biens classifiés du gouvernement. Le programme d'ICA s'élargit pour englober les risques pour la chaîne d'approvisionnement numérique dans les infrastructures essentielles, à l'appui du projet de loi C-26.

Par ailleurs, le SCRS accorde la priorité aux enquêtes sur les activités économiques hostiles potentielles parrainées par des acteurs étatiques. Le SCRS appuie les partenaires du gouvernement du Canada dans leurs pratiques de gestion du risque relatives à la propriété, au contrôle ou à l'influence ainsi qu'au Programme des marchandises contrôlées. Le SCRS travaille également en étroite collaboration avec des partenaires du gouvernement pour s'assurer que le plus grand nombre possible d'entreprises canadiennes et de différents ordres de gouvernement sont informés sur l'environnement de la menace et disposent de l'information dont ils ont besoin pour mettre en œuvre des mesures de sécurité préventives. La mobilisation par le SCRS auprès de Chaîne d'approvisionnement Canada et d'autres groupes connexes de l'industrie sur les risques pour la chaîne d'approvisionnement logistique est un exemple des mesures que prend le SCRS pour mobiliser un vaste éventail d'intervenants et s'assurer que les Canadiens sont en sécurité et que leurs intérêts sont protégés des menaces.

Pour réagir aux risques pour la sécurité nationale qui évoluent sans cesse, le gouvernement envisage la possibilité d'élaborer des outils et des processus rigoureux pour gérer particulièrement les risques pour la sécurité nationale. Services publics et Approvisionnement Canada a établi un groupe de travail qui collaborera avec les organismes canadiens ayant un mandat de sécurité nationale, y compris le CST, en ce qui concerne la création potentielle d'un questionnaire d'examen des risques pour la sécurité avant l'évaluation (outil de vérification). L'outil de vérification serait utilisé à l'étape des demandes préalables à la demande de soumission pour relever les exigences qui posent un risque élevé, moyen ou faible pour la sécurité nationale. En fonction du niveau de risque établi, des mesures d'atténuation seraient incluses dans la stratégie d'approvisionnement, notamment une évaluation de l'ICA élargie, qui s'appliquerait à un plus grand nombre de produits ayant des composantes des technologies de l'information et des communications. Utilisé conjointement avec les outils en place, ce nouvel outil permettrait de réagir plus efficacement aux menaces à la sécurité nationale.

Recommandation 13 : Que le gouvernement du Canada collabore avec les communautés linguistiques minoritaires affectées par les activités d'ingérence étrangère au Canada afin de leur fournir, dans

la langue qu'elles comprennent le mieux, des informations fiables sur le processus démocratique canadien, y compris des informations sur les politiques et les programmes gouvernementaux qui peuvent les concerner, et que le gouvernement engage un dialogue avec les médias locaux et ethniques pour fournir cette information.

Le gouvernement étudiera davantage cette recommandation.

Le gouvernement du Canada s'engage à veiller à ce que des informations sur ses institutions démocratiques ainsi que sur les politiques et les programmes de son gouvernement soient à la disposition de tous les Canadiens. Le gouvernement du Canada fournit de l'information sur ses institutions démocratiques, sur le fonctionnement du Parlement, sur le fonctionnement élémentaire du processus électoral et sur la façon dont les Canadiens sont représentés en ligne, sur Canada.ca. Ces informations sont fournies en anglais et en français, conformément à la *Loi sur les langues officielles*. Le gouvernement étudiera la possibilité de traduire des ressources sur les institutions démocratiques du Canada dans d'autres langues utilisées au Canada, notamment en travaillant avec des communautés linguistiques minoritaires.

En 2018, la *Loi sur la modernisation des élections* a élargi le mandat d'Élections Canada pour y inclure la communication avec le public afin d'améliorer sa connaissance du processus électoral. Le mandat d'Élections Canada inclut l'exécution de campagnes d'information du public sur l'inscription des électeurs, l'exercice du droit de vote et la marche à suivre pour présenter sa candidature. Selon *le* Rapport sur la 44e élection générale du 20 septembre 2021 préparé par Élections Canada, le « *Guide pour l'élection fédérale* » de l'organisation a été traduit vers 49 langues différentes, dont 16 langues autochtones. Le gouvernement du Canada accueille favorablement les initiatives prises par Élections Canada pour veiller à ce que tous les Canadiens aient accès à des informations fiables sur le processus électoral.

Plusieurs organisations du gouvernement du Canada, dont le SCRS, AMC et Patrimoine canadien, déploient des efforts considérables pour communiquer avec le public, notamment par l'élaboration de ressources accessibles au public. Le SCRS a inclus des renseignements sur l'IE dans tous ses rapports publics annuels des 30 dernières années, et il a publié des rapports non classifiés, y compris « Interférence étrangère et vous », dans six langues afin de rejoindre le plus de Canadiens possible. Les produits du SCRS sont publiés dans toute une gamme de langues étrangères pour veiller à ce que les communautés vulnérables puissent accéder à des renseignements sur les menaces dans la langue de leur choix.

Lorsque nécessaire, AMC publie des déclarations publiques sur l'IE et communique avec les personnes concernées issues de communautés linguistiques minoritaires dans la langue qu'elles comprennent le mieux. En

août et octobre 2023, AMC a publié des déclarations publiques dans les deux langues officielles et les a distribuées à une liste de personnes-ressources des médias en mandarin, et ce, à l'issue de deux campagnes distinctes dans le cadre desquelles AMC a jugé probable que la République populaire de Chine (RPC) ait participé à des activités ciblant des parlementaires canadiens. La première campagne a ciblé un député sur WeChat, et la deuxième campagne a ciblé plus de 40 parlementaires et un dissident d'origine chinoise vivant au Canada sur diverses plateformes de médias sociaux.

Patrimoine canadien a investi plus de 21 millions de dollars depuis 2019 pour soutenir des activités de culture civique et des médias sociaux au Canada par l'entremise du Programme de contributions en matière de citoyenneté numérique (PCCN). Le PCCN offre une aide financière d'une durée limitée à des projets dirigés par des chercheurs et des organisations de la société civile afin d'approfondir la compréhension de la désinformation en ligne, y compris la désinformation associée à l'IE, d'accroître la résilience à cette désinformation et de soutenir la démocratie canadienne. Beaucoup des projets appuyés dans le cadre du PCCN ont précisément visé à offrir aux communautés linguistiques minoritaires les outils dont elles ont besoin pour accroître leur résilience à la désinformation en ligne. L'appel de propositions du PCCN de l'automne 2023 vise des projets d'élaboration et de publication d'outils qui permettront d'accroître la résilience à la mésinformation et à la désinformation en provenance de gouvernements étrangers, comme ceux de la RPC et de Russie, qui ciblent des personnes au Canada, dont des communautés de la diaspora, entre autres priorités.

Recommandation 14 : Que le gouvernement du Canada insère dans le *Code criminel* des mesures pénales qui englobent toutes les activités d'ingérence étrangère, y compris le harcèlement et l'intimidation au nom d'un État étranger, et qu'il prévoie des sanctions adéquates pour y répondre.

Le gouvernement accepte le principe de cette recommandation.

Le gouvernement a lancé des consultations publiques sur de possibles modifications à la *Loi sur le SCRS*, au *Code criminel*, à la LPI et à la LPC le 24 novembre 2023 dans le cadre de ses efforts de lutte contre l'IE.

Le document de consultation publique du ministère de la Justice contient plusieurs propositions de modifications à la LPI, notamment :

- création de nouvelles infractions liées à l'IE, y compris une infraction générale pour IE, afin de mieux atténuer les risques d'IE que court le Canada, ainsi que les risques de répression transnationale ciblant des personnes vivant au Canada et des membres de leur famille vivant à l'étranger, et pour voir à ce que les activités hostiles secrètes soient pleinement prises en charge par le droit pénal;

- élargissement des infractions liées aux actes préparatoires (article 22), qui incluent l'accomplissement de tout acte en vue ou en préparation de la perpétration d'une infraction, de façon à y inclure toutes les infractions prévues par la LPI et à accroître les sanctions existantes.

Les modifications proposées au *Code criminel* incluent la modernisation de l'infraction de sabotage en clarifiant les types d'infrastructures essentielles qui pourraient être la cible d'actes de sabotage. On considère aussi proposer la création d'une infraction de sabotage pour le compte d'un État étranger.

Recommandation 15 : Que le gouvernement du Canada clarifie l'objectif des dispositions de la *Loi sur la protection de l'information* visant à contrer les activités d'ingérence étrangère et des mesures de sanction afférentes, et qu'il émette une politique permettant aux Canadiens de mieux comprendre comment la *Loi sur la protection de l'information* permet de protéger le Canada de l'ingérence étrangère.

Le gouvernement accepte le principe de cette recommandation.

Dans le cadre des efforts de lutte contre l'IE déployés par le gouvernement du Canada, le 24 novembre 2023, des consultations publiques sur de possibles modifications à la *Loi sur le SCRS*, au *Code criminel*, à la LPI et à la LPC ont été annoncées.

Le document de consultation publique du ministère de la Justice connexe explique des modalités clés de la *Loi sur la protection de l'information* qui portent sur des aspects de la répression transnationale :

- Selon l'article 20 de la *Loi sur la protection de l'information*, commet une infraction quiconque, sur l'ordre d'un État étranger, en collaboration avec lui ou pour son profit, incite une personne par menaces, accusations ou violence à accomplir ou à faire accomplir quelque chose.

- L'article 22 porte sur les actes préparatoires et établit que commet une infraction quiconque accomplit un acte en vue ou en préparation de la perpétration de certaines autres infractions prévues par la *Loi sur la protection de l'information*, y compris des infractions liées à l'IE.

Recommandation 16 : Que le gouvernement du Canada tienne les plateformes numériques responsables pour la diffusion d'information fausse ou trompeuse et qu'il élabore des politiques de soutien de l'écosystème médiatique dans les diasporas et autres communautés linguistiques minoritaires et non représentées par les grands médias afin de s'assurer que les communautés vulnérables ne soient pas revictimisées.

Le gouvernement prend bonne note de cette recommandation.

Étant résolu à mettre en œuvre dès que possible une loi visant à lutter contre

les formes graves de contenu préjudiciable en ligne, le gouvernement a mené de vastes consultations pour en orienter l'élaboration : consultation publique en ligne, groupe consultatif d'experts, assemblée de citoyens et série de vingt tours de table, de juillet à novembre 2022.

À l'issue de ces consultations, le gouvernement a retenu que la nouvelle loi devra préserver un juste équilibre entre la volonté d'assurer un environnement en ligne sain et digne de confiance et la protection de la liberté d'expression garantie par la *Charte canadienne des droits et libertés*. Dans le même ordre d'idées, le gouvernement a pris note que les Canadiens et les intervenants estiment que, même si la circulation d'information fausse et trompeuse en ligne peut avoir d'importantes conséquences, le fait de créer une loi et des politiques restreignant ou limitant autrement les discours en fonction de la véracité de l'information viendrait miner la liberté d'expression dans une mesure inacceptable.

Heureusement, la loi n'est pas le seul outil de lutte contre l'information fausse ou trompeuse dont dispose le gouvernement, qui s'engage à contrer la désinformation en ligne et ses effets sur les collectivités du pays. Pour ce faire, le ministère du Patrimoine canadien a mis en œuvre l' « *Initiative de citoyenneté numérique* » dans le cadre du Plan pour protéger la démocratie au Canada. Cette initiative vise à fournir aux chercheurs et aux organisations de la société civile une aide financière d'une durée limitée en vue d'étudier les origines, la diffusion et l'incidence de la désinformation en ligne, ainsi que d'accroître la résistance des citoyens face à celle-ci. Grâce au programme de contributions de l'Initiative, le Programme de contributions en matière de citoyenneté numérique (PCCN), un investissement de 21 millions de dollars a été réalisé à l'appui de 109 projets, dont bon nombre s'inscrivent dans les efforts visant à accroître la résistance à la désinformation des communautés qui y sont vulnérables.

En juin 2023, le gouvernement a annoncé qu'il investirait 5,5 millions de dollars dans la création du Réseau canadien de recherche sur les médias numériques (RCRMN), que l'Université de Toronto et l'Université McGill administrent de façon indépendante. En vue d'accroître davantage la résistance des Canadiens en matière d'information, le RCRMN étudiera la façon dont la qualité de l'information, notamment les récits de désinformation, influence l'attitude et le comportement des Canadiens, et soutiendra les efforts menés au Canada sur le plan des connaissances numériques.

Recommandation 17 : Que le gouvernement du Canada, en collaboration avec les agences de sécurité nationale, explore la possibilité d'imposer des sanctions ciblées à l'endroit d'entreprises canadiennes qui exportent ou vendent des produits technologiques à des pays qui les utilisent pour mener des activités d'ingérence étrangère.

Le gouvernement prend bonne note de cette recommandation et convient que certaines technologies peuvent accroître la portée et l'efficacité des activités d'IE. Le Canada, qui demeure résolu à jouer un rôle de chef de file pour maintenir et renforcer l'ordre international fondé sur des règles, envisage l'imposition de sanctions dans le cadre de cette approche.

Le Canada dispose d'un processus rigoureux de diligence raisonnable pour évaluer les circonstances qui pourraient justifier le recours aux sanctions. Le gouvernement tient également compte du contexte politique et international général au moment de décider s'il y a lieu de faire appel aux sanctions ou à tout autre outil en matière de politique étrangère dont il dispose. Les recommandations liées aux sanctions font l'objet d'un examen par AMC, qui tient compte des exigences sur le plan législatif et de la preuve disponible pour déterminer si la situation se prête à l'imposition de sanctions au titre des lois encadrant les sanctions autonomes canadiennes, la *Loi sur la justice pour les victimes de dirigeants étrangers corrompus* (LJVDEC) et la *Loi sur les mesures économiques spéciales* (LMES).

En raison de la conception, de la structure et de l'objet des lois encadrant les sanctions autonomes canadiennes, il ne serait pas approprié d'avoir recours aux sanctions à titre d'outil en matière de politique étrangère pour agir contre les entreprises canadiennes qui vendent des technologies à des pays qui s'en servent à des fins d'ingérence étrangère ou qui y en exportent. Au titre de la LJVDEC, seules des personnes (et non des entités) peuvent faire l'objet de sanctions, notamment pour violations flagrantes des droits de la personne et actes de corruption graves.

La LMES permet d'imposer des sanctions à des entités. Toutefois, pour ce faire, l'entité qui se livre à de l'ingérence étrangère doit correspondre à la définition de « personne désignée », à savoir toute personne ou entité qui se trouve dans un pays étranger ou qui est ou était un de ses nationaux ne résidant habituellement pas au Canada. Ainsi, on ne peut imposer de sanctions à une entreprise canadienne en vertu de la LMES. Le fait de désigner une entreprise canadienne ou d'y imposer des sanctions au titre d'un règlement pris en vertu de la LMES nuirait aux Canadiens et aux entreprises canadiennes affiliés à l'entité désignée. Parmi les sanctions imposées au titre de cette loi, mentionnons l'interdiction de conclure des transactions avec les personnes et entités désignées (ce qui gèle pour ainsi dire leurs avoirs au Canada), des restrictions ou des interdictions concernant les échanges commerciaux, ainsi que des restrictions sur les transactions financières ou d'autres activités économiques. Il serait donc difficile pour d'autres Canadiens de traiter avec une personne désignée au Canada, ce qui aurait de nombreuses répercussions concrètes. Par exemple, un employé canadien d'une entreprise visée par des sanctions ne pourrait pas recevoir de rémunération de la part de son employeur. Par ailleurs, il ne faut pas oublier que l'imposition de sanctions visant une entreprise nuirait à ses opérations,

puisqu'il serait interdit de conclure toute transaction financière avec elle (les banques cesseraient ainsi toute opération et l'entreprise ne pourrait pas acquitter ses comptes), ce qui pourrait éventuellement entraîner la faillite de l'entreprise.

Recommandation 18 : Que le gouvernement du Canada mette en place un registre des agents étrangers le plus rapidement possible.

Le gouvernement accepte en principe cette recommandation.

Le Canada dispose d'un cadre robuste de transparence en matière de lobbying, qui n'a toutefois pas été conçu pour faire face à la menace de l'influence étrangère malveillante. Certains gouvernements étrangers ont recours à des personnes ou à des entités pour tenter d'influencer secrètement, ou d'une façon non transparente, les politiques gouvernementales canadiennes ou l'opinion publique au Canada; c'est pour cette raison qu'en mars 2023, le gouvernement du Canada a lancé des consultations auprès du grand public et des intervenants sur un registre pour la transparence en matière d'influence étrangère (RTMIE). À l'issue de ces consultations en ligne d'une durée de 60 jours, près de 1 000 réponses ont été obtenues de la part d'une grande variété de répondants. Les commentaires recueillis sont en cours d'examen par des représentants de SPC en vue d'orienter la conception du RTMIE et d'une loi connexe. On procède actuellement à tables rondes et à des discussions bilatérales portant sur le RTMIE avec des intervenants, de même que sur l'IE en général avec, notamment, des organismes communautaires, des groupes autochtones et des intervenants provinciaux et territoriaux. La rétroaction recueillie dans le cadre de ces consultations sert à orienter la prise de décisions et l'élaboration de nouvelles mesures que l'on pourrait promouvoir.

Recommandation 19 : Que le gouvernement du Canada modifie la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* pour exiger que chaque rapport annuel présenté à chaque chambre du Parlement comprenne un examen annuel des menaces d'ingérence étrangère au Canada, telles que le harcèlement et l'intimidation de certaines communautés canadiennes par des États étrangers.

Le gouvernement prend bonne note de cette recommandation.

Le gouvernement tient à mettre en évidence le mandat d'examen existant du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). Ce dernier a la capacité d'examiner les cadres législatif, réglementaire, stratégique, administratif et financier de la sécurité nationale et du renseignement, les activités des ministères liées à la sécurité nationale ou au renseignement (à moins que l'examen ne porte atteinte à la sécurité nationale) et toute question liée à la sécurité nationale et au renseignement que lui transmet un ministre fédéral. Il s'agit d'un vaste mandat, qui offre au CPSNR une latitude pour se pencher sur des questions comme l'IE.

Plusieurs examens du CPSNR se sont déjà traduits par des recommandations concernant la réponse du Canada à l'IE. Par exemple, en mars 2023, le Comité a évalué la mesure dans laquelle il y a eu IE dans le processus électoral fédéral. En 2018, il a également publié un rapport spécial portant sur l'IE dans le cadre de la visite du premier ministre en Inde cette même année. Par ailleurs, dans ses rapports annuels de 2019, de 2021 et de 2022, le CPSNR a examiné et proposé des recommandations concernant l'IE. De 2018 à 2023, un total de 26 recommandations visant à améliorer la réponse du gouvernement à l'IE a été fait dans le cadre de ces rapports. D'importants travaux ont été réalisés pour mettre plusieurs de ces recommandations en œuvre, et les efforts se poursuivent pour donner suite aux autres recommandations.

Le fait d'incorporer à la loi des exigences précises régissant l'examen annuel du CPSNR pourrait nuire à l'évolution de ses examens au fil du temps, à mesure qu'évolue le contexte de la menace. Le gouvernement tient à souligner l'importance de préserver l'autonomie et l'impartialité du CPSNR à titre d'organe d'examen, lesquelles sont essentielles au maintien de la confiance des Canadiens.

La création du CPSNR résulte du projet de loi C-22 (*Loi constituant le Comité des parlementaires sur la sécurité nationale et le renseignement et modifiant certaines lois en conséquence*) de 2017, lequel prévoit que les dispositions et l'application de la *Loi* doivent faire l'objet d'un examen cinq ans après son entrée en vigueur. Les recommandations, notamment celles liées à l'IE, pourraient également être prises en considération lors d'une éventuelle révision du projet de loi C-22. La *Loi* prévoit que l'examen exhaustif soit réalisé par un comité de la Chambre des communes, du Sénat ou des deux Chambres du Parlement désigné ou établi par la Chambre des communes, le Sénat ou les deux Chambres du Parlement, selon le cas.

Recommandation 20 : Que le gouvernement du Canada crée un comité du Cabinet chargé de la sécurité nationale.

Le gouvernement accepte cette recommandation.

Comme l'a annoncé le premier ministre le 26 juillet 2023, un nouveau comité du Cabinet chargé de la sécurité nationale a été mis sur pied : le Conseil de la sécurité nationale, présidé par le premier ministre, qui sert de tribune pour la prise de décisions stratégiques et pour la présentation de l'analyse du renseignement dans son contexte stratégique.

Recommandation 21 : Que le gouvernement du Canada renforce les mécanismes de signalement pour les victimes de harcèlement ou d'intimidation par des entités étrangères, pour assurer une meilleure coordination de la réponse du gouvernement à de tels incidents et la prise d'actions appropriées à l'égard des plaintes individuelles.

Le gouvernement accepte cette recommandation.

Le gouvernement du Canada, qui dispose de divers mécanismes de signalement d'incidents d'IE présumée, réalise des investissements pour aider à en protéger les cibles et assurer une réaction fédérale plus coordonnée face à ces menaces. À l'échelle fédérale, la Gendarmerie royale du Canada (GRC) enquête sur les menaces potentielles de violence, de harcèlement et d'intimidation impliquant un acteur étatique, en plus de collaborer avec les services de police compétents pour déceler et contrer ces menaces. La GRC demande aux responsables des communautés de rester vigilants et de lui signaler toute activité suspecte, ou d'en faire part à leur service de police local. Tous peuvent communiquer avec le Réseau info-sécurité nationale de la GRC par téléphone au 1-800-420-5805, ou par courriel à l'adresse RCMP.NSIN-RSIN@rcmp-grc.gc.ca. Tout membre du public qui se trouve en danger immédiat doit composer le 911 ou communiquer avec le service de police de sa région. En addition aux mécanismes existants, le budget de 2023 prévoyait l'octroi, à la GRC, de 48,9 millions de dollars sur trois ans pour l'aider à protéger davantage les Canadiens contre le harcèlement et l'intimidation de la part d'acteurs étrangers, accroître sa capacité d'enquêter et mobiliser de façon plus proactive les communautés particulièrement susceptibles d'être ciblées.

Par ailleurs, le Service Canadien du renseignement de sécurité (SCRS) met à la disposition des Canadiens une ligne d'aide générale et un mécanisme de signalement en ligne sur son site Web pour signaler toute préoccupation, notamment en lien avec l'IE. Pour joindre la ligne d'aide générale, il suffit de composer le 613-993-9620 ou le 1-800-267-7685 (sans frais), ou encore le 613-991-9228 pour les services ATS. L'outil de signalement en ligne se trouve sur la page Web du SCRS (www.canada.ca/fr/service-renseignement-securite), à la section « Signaler des informations relatives à la sécurité nationale ». Pour assurer la sécurité des Canadiens, le SCRS continue à déployer d'importants efforts en vue de renforcer, par la mobilisation, ses relations avec le milieu universitaire, représentants d'entreprises, provincial, territorial, municipales, gouvernements autochtones, les membres et les représentants des communautés et les groupes de revendication susceptibles d'être dans la mire des acteurs malveillants. Le SCRS mobilisera différentes communautés canadiennes en vue de recueillir des points de vue et opinions uniques et de fournir de l'information importante aux cibles potentielles d'IE.

Pour améliorer la coordination au sein du gouvernement fédéral, le premier ministre a annoncé, en mars 2023, la nomination d'un coordonnateur national de la lutte contre l'IE au sein de Sécurité Publique Canada (SPC). Son rôle vise à porter une attention particulière à l'IE et à renforcer les partenariats avec les intervenants externes au gouvernement fédéral, notamment à accroître la sensibilisation à l'égard de la menace que représente l'IE et des outils dont dispose le public pour signaler les menaces observées. Dans le cadre du budget de 2023, le gouvernement a octroyé à l'initiative 13,5 millions de dollars sur cinq ans, ainsi que 3,1 millions de dollars en financement continu.

Bien qu'il ne tienne pas le grand public à jour des résultats du signalement des menaces en raison de la nature délicate des enquêtes, le gouvernement du Canada prend ces préoccupations au sérieux et accorde de l'importance à toute l'information qu'on lui signale. D'abord et avant tout, le gouvernement du Canada continuera d'assurer la protection des renseignements personnels et la sécurité des personnes qui signalent de telles menaces.

Recommandation 22 : Que le gouvernement du Canada consulte les membres des communautés affectées par les activités d'ingérence étrangère au Canada dans toute enquête portant sur l'ingérence étrangère.

Le gouvernement accepte cette recommandation.

Le 7 septembre 2023, à l'issue de vastes consultations menées auprès de tous les partis reconnus à la Chambre des communes, le gouvernement a annoncé la mise sur pied d'une enquête publique sur l'IE dans le processus électoral fédéral et les institutions démocratiques. L'honorable Marie-Josée Hogue, juge puînée de la Cour d'appel du Québec, dirige l'enquête; son travail à titre de commissaire a débuté le 18 septembre 2023. Nommée en vertu de la *Loi sur les enquêtes*, elle mène ses activités sans l'intervention du gouvernement et détient une gamme complète de pouvoirs, notamment celui de convoquer des témoins et de les contraindre à témoigner sur des questions de ressort fédéral. La commissionnaire Hogue a le mandat de formuler toute recommandation qu'elle juge nécessaire pour protéger les processus démocratiques du Canada contre l'IE, concernant, entre autres, les mesures de soutien et de protection offertes aux membres des diverses diasporas qui pourraient s'avérer particulièrement vulnérables à l'IE dans le cadre des processus démocratiques du Canada.