Enquête publique
sur l'ingérence étrangère
dans les processus
électoraux et les institutions
démocratiques fédéraux

L'honorable Marie-Josée Hogue,
commissaire

VOLUME 3 CHAPITRES 10-13

La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 1/2)

Enquête publique sur l'ingérence étrangère
dans les processus électoraux et les
institutions démocratiques fédéraux

Rapport final
28 Janvier 2025

Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux. Rapport final. Volume 3 : La capacité du gouvernement à détecter, prévenir et contrer l'ingérence étrangère (faits et analyse 1/2).

This publication is also available in English:
Volume 3: The Government's Capacity to Detect, Deter and Counter Foreign Interference (Facts and Analysis 1/2).

CP32-169/2-2025F-3-PDF
ISBN 978-0-660-75088-0

(Ensemble) CP32-169/2-2025F-PDF

Note concernant la traduction

Plusieurs notes de bas de page du rapport contiennent des références aux transcriptions des audiences de la Commission. Ces notes de bas de page réfèrent à la pagination de la version bilingue des transcriptions (version « plancher » telle que prononcée) et non à la pagination de la version traduite en français.

Par ailleurs, aux fins du rapport, les citations originales anglaises tirées des transcriptions bilingues ont été traduites en français par la Commission. Les citations traduites dans le rapport peuvent être différentes des citations qu'on retrouve dans la version française des transcriptions.

Pour alléger le texte, nous avons évité d'identifier les citations traduites avec la mention « [traduction] ». Nous avons seulement utilisé des guillemets.

Finalement, il est possible que des notes de bas de page réfèrent uniquement à des documents rédigés en anglais. Cette situation s'explique habituellement par le fait qu'aucune version française de ces documents n'est accessible ou que la Commission n'a pas été en mesure de l'obtenir à temps pour le dépôt du rapport.

Table des matières

CHAPITRE 10

La menace d’ingérence étrangère

Les informations peuvent être incomplètes : *des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

10.1 Introduction

Pour comprendre la capacité du gouvernement à répondre à l'ingérence étrangère, il est essentiel de comprendre la nature de la menace d'ingérence étrangère elle-même. Il s'agit notamment de percevoir l'éventail des acteurs qui s'y livrent et les tactiques qu'ils utilisent.

Comprendre la menace d'ingérence étrangère peut s'avérer difficile pour un certain nombre de raisons. L'un des défis que j'ai constatés au cours de mon travail est la zone grise qui existe entre l'ingérence étrangère, d'une part, et les activités légitimes des États, d'autre part.

Un deuxième défi tient au fait que la plupart de ce que nous savons au sujet de l'ingérence étrangère provient du renseignement. Et comme je l'ai mentionné précédemment dans ce rapport, le renseignement est une source d'information qui présente des limites inévitables.

Dans ce chapitre, je donne une vue d'ensemble de la menace d'ingérence étrangère telle qu'elle existe actuellement.

10.2 L'ingérence étrangère au-delà du mandat de la Commission

Comme nous l'avons vu au chapitre 3 (volume 2), l'ingérence étrangère revêt de nombreux aspects, mais le mandat de la Commission fixe la portée de mon enquête. Il me demande de me concentrer sur un sous-ensemble de l'ingérence étrangère – celle qui vise les institutions et les processus démocratiques. Beaucoup d'éléments ne sont pas inclus, comme l'ingérence étrangère dans l'économie, l'industrie, les forces armées et les universités, l'espionnage et de nombreuses formes de répression transnationale.

Toutefois, les activités d'ingérence étrangère ne sont pas cloisonnées. Par exemple, la répression transnationale impliquant un politicien peut également constituer de l'ingérence dans un processus démocratique. En outre, certaines tactiques de répression transnationale visant des membres de communautés issues des diasporas peuvent interférer avec les processus démocratiques du Canada. J'en ai tenu compte dans l'exercice de mon mandat.

À titre d'exemple, la Commission a demandé des informations concernant certains exemples d'ingérence étrangère actuels et connus du public, comme l'assassinat de Hardeep Singh Nijjar. La Commission a également rencontré des Canadiennes et des Canadiens membres des communautés issues des diasporas pour connaître leur expérience de la répression transnationale. Ces questions ne relèvent pas entièrement du mandat de la Commission, mais les informations obtenues m'ont permis de mieux comprendre la menace de l'ingérence étrangère et la réponse du Canada à cet égard. Ces informations m'ont également aidée à formuler mes recommandations.

10.3 Les acteurs menaçants qui ciblent le Canada

Le contexte de la menace est influencé par des forces historiques, des réalités contemporaines, des relations complexes, ainsi que les objectifs et intérêts stratégiques du Canada. C'est pourquoi, pour faire face aux acteurs menaçants, il faut comprendre nos relations historiques ainsi que les événements plus récents et leurs effets. Il faut également comprendre les intérêts stratégiques qu'a le Canada dans une série d'États étrangers, ainsi que les intérêts qu'ont ces derniers au Canada.

La République populaire de Chine (RPC)

Au moment de rédiger ce rapport, la République populaire de Chine (la « **RPC** ») est l'État le plus actif en matière d'ingérence étrangère visant les institutions démocratiques canadiennes.

La RPC est aussi un acteur incontournable sur la scène mondiale. Elle se concentre sur la promotion de ses intérêts nationaux et sur la protection de la légitimité et de la stabilité du Parti communiste chinois (le « **PCC** »). Ses valeurs et ses intérêts diffèrent de plus en plus de ceux du Canada. Néanmoins, il s'agit d'un partenaire essentiel pour le Canada dans le traitement de questions communes aux deux États. La capacité du Canada à travailler avec la RPC sur des enjeux mutuels et à soulever des objections et des préoccupations exige que le Canada maintienne des canaux de communication fonctionnels.

La RPC considère le Canada comme une cible hautement prioritaire. Le Canada est un membre important d'alliances comme celle du Groupe des cinq (Canada, Royaume-Uni, États-Unis, Australie et Nouvelle-Zélande). Nous jouissons d'une solide réputation internationale que la RPC pourrait vouloir utiliser pour promouvoir ses intérêts. Nous sommes aussi un partenaire commercial fiable et ouvert, doté d'une économie avancée qui peut soutenir

les objectifs de développement de la RPC. Le Canada abrite par ailleurs l'une des plus importantes communautés issues de la diaspora chinoise. Selon le Service canadien du renseignement de sécurité (le « **SCRS** »), la RPC souhaite que le Canada soutienne ses intérêts, qu'il donne d'elle une image positive et qu'il fasse preuve de déférence à l'égard de son autorité.

Les relations du Canada avec la RPC ont changé radicalement en décembre 2018 lorsque la RPC a détenu arbitrairement les Canadiens Michael Spavor et Michael Kovrig (les « **deux Michael** »). Jusqu'à leur libération en septembre 2021, les relations du Canada avec la RPC ont été centrées sur leur détention.

Il s'agissait également d'un événement important du point de vue de la RPC. Historiquement, la RPC se concentrait sur les interactions politiques avec le pouvoir exécutif au Canada. Cependant le sous-ministre des Affaires étrangères, David Morrison, a expliqué que la détention des deux Michael avait sérieusement terni l'image de la RPC aux yeux du public canadien et augmenté l'activité critique à son égard de ce pays au sein de l'organe législatif. Cela a pu amener la RPC à s'intéresser aux membres du pouvoir législatif canadien, un intérêt qu'elle ne jugeait pas nécessaire auparavant. Il s'agit là d'un contexte important pour comprendre l'intérêt de la RPC envers les députés canadiens, un sujet que j'aborde plus en détail au chapitre 14 (volume 4) dans le cadre de mon examen du document connu sous le nom de « Document sur le ciblage ».

Depuis la libération des « deux Michael » en 2021, le Canada et la RPC tentent de surmonter les difficultés de leur relation. Le Canada a notamment exprimé ses préoccupations quant aux activités d'ingérence étrangère de la RPC au pays.

L'ingérence étrangère de la RPC est de grande envergure. Elle vise tous les ordres de gouvernement au Canada. Les fonctionnaires canadiens chargés de la sécurité et du renseignement considèrent que la RPC ne fait généralement pas de distinction entre les partis, c'est-à-dire qu'elle soutient ceux qu'elle juge utiles à ses intérêts du moment et ceux qu'elle estime susceptibles d'accéder au pouvoir sans égard au parti politique dont ils sont membres.

Selon le renseignement, la RPC fait appel à un large éventail d'acteurs pour s'ingérer à l'étranger. Parmi ses institutions nationales, le ministère de la Sécurité de l'État et le ministère de la Sécurité publique opèrent secrètement à l'étranger. La RPC agit également par l'intermédiaire de ses diplomates.

Le Département du travail du front uni, officiellement un département du PCC, tente de contrôler et d'influencer les communautés issues de la diaspora chinoise au Canada, de façonner les opinions internationales et d'influencer les politiciens pour qu'ils soutiennent les politiques de la RPC.

Au-delà des institutions officielles de l'État et du parti, la RPC s'appuie sur des mandataires, c'est-à-dire des personnes ou des organisations qui reçoivent des instructions explicites ou implicites de sa part pour se livrer à

de l'ingérence étrangère. Elle tente de tirer parti des Canadiennes et des Canadiens d'origine chinoise, des réseaux existants établis par son ambassade et ses consulats, ainsi que d'autres acteurs (qu'ils soient ou non d'origine chinoise).

La RPC représente également la cybermenace la plus sophistiquée et la plus active pour le Canada.

Le SCRS estime en outre que la RPC utilise de plus en plus les médias sociaux et Internet pour des campagnes de désinformation concernant les élections.

Malgré une surveillance accrue de tentatives d'ingérence étrangère au Canada, les agences de renseignement et de sécurité canadiennes ont conclu que la RPC a toujours la capacité et l'intention de s'ingérer dans les élections.

Inde

L'Inde est le deuxième acteur étatique le plus actif en matière d'ingérence étrangère électorale au Canada.

Tout comme la RPC, l'Inde est un acteur incontournable sur la scène mondiale. C'est un acteur mondial de plus en plus important qui est en mesure de contester l'hégémonie de la RPC en Asie. Le Canada et l'Inde collaborent depuis des décennies, mais leurs relations ont connu des difficultés. Récemment, ces difficultés sont devenues plus aiguës. Nombre de ces difficultés existent depuis longtemps et influencent les activités d'ingérence de l'Inde.

Depuis l'attentat à la bombe perpétré en 1985 contre un vol d'Air India en provenance du Canada, l'Inde considère que le Canada ne prend pas suffisamment au sérieux ses préoccupations en matière de sécurité nationale concernant le séparatisme khalistanais (qui a pour objectif d'établir un territoire sikh indépendant dans le nord de l'Inde nommé « Khalistan »). Il existe une tension fondamentale entre le point de vue de l'Inde, qui considère certaines activités comme du terrorisme, et celui du Canada, qui reconnait et protège les libertés fondamentales d'expression et d'association des Canadiennes et des Canadiens. Le gouvernement indien ne semble faire aucune distinction entre les activités licites de défense des intérêts politiques du Khalistan et l'extrémisme violent khalistanais issu du Canada, qui est relativement rare.

L'Inde a tenté de faire pression sur le Canada pour qu'il fasse fi de la législation canadienne afin de contrer les partisans d'un Khalistan indépendant. Les activités d'ingérence de l'Inde ont pour objet de tenter d'aligner les positions du Canada sur celles de l'Inde au sujet de questions clés, notamment en ce qui concerne les partisans du séparatisme khalistanais.

Pour atteindre ces objectifs, l'Inde concentre ses activités d'ingérence étrangère sur la communauté indo-canadienne et sur des personnalités non indo-canadiennes. Cette ingérence aurait visé tous les niveaux de gouvernement.

Comme la RPC, l'Inde s'ingère par l'intermédiaire de ses fonctionnaires au Canada et de ses mandataires au Canada. Des éléments de renseignement indiquent que des agents mandataires du gouvernement de l'Inde ont pu verser clandestinement et pourraient continuer de verser un financement illicite à divers politiciens canadiens dans le but de faire élire des candidats qui lui sont favorables ou d'influencer des candidats qui entrent en fonction. La communauté canadienne du renseignement a observé des actes d'ingérence du gouvernement indien cherchant à influencer des processus d'investiture et des décisions prises au Parlement. Le renseignement n'indique pas nécessairement que les élus ou les candidats concernés étaient au courant des tentatives d'ingérence ni que ces tentatives ont nécessairement été couronnées de succès.

L'Inde utilise également la désinformation comme forme clé d'ingérence étrangère contre le Canada, une tactique qu'elle est susceptible d'utiliser plus souvent. L'Inde continue de développer ses cybercapacités. Le SCRS estime que l'Inde cherchera probablement à promouvoir un discours pro-Inde et anti-Khalistan au Canada en utilisant des techniques de guerre cognitive.

Jusqu'à récemment, le Canada, dans le cadre de sa Stratégie pour l'Indo-Pacifique, essayait d'améliorer ses relations bilatérales avec l'Inde. Cependant, l'assassinat de Hardeep Singh Nijjar en juin 2023 a fait dérailler ces efforts.

En septembre 2023, le premier ministre Trudeau a annoncé que les organismes de sécurité canadiens détenaient des allégations crédibles concernant un lien potentiel entre des agents du gouvernement indien et la mort de M. Nijjar. L'Inde a nié ces allégations à plusieurs reprises. La réaction de l'Inde a été extrême et ses relations avec le Canada restent tendues depuis lors. J'aborde les événements entourant l'assassinat de M. Nijjar plus en détail au chapitre 17 (volume 4).

Plus récemment, en octobre 2024, le Canada a expulsé six diplomates et fonctionnaires indiens en réponse à une campagne ciblée visant des citoyens canadiens menée par des agents liés au gouvernement de l'Inde.

Russie

La relation du Canada avec la Russie est conflictuelle.

Au lendemain de la Guerre froide, le Canada a progressivement entretenu des relations avec la Russie. Cette situation a changé après l'invasion de la Crimée par la Russie en 2014. Les relations diplomatiques entre les deux pays ont alors considérablement diminué. Le Canada a suspendu pratiquement

tous les contacts officiels après l'invasion de l'Ukraine par la Russie en 2022. Aujourd'hui, les relations diplomatiques se limitent généralement à l'expression par le Canada de son mécontentement à l'égard du comportement de la Russie. Le Canada a imposé des sanctions économiques à plus de 3 000 entités et personnes affiliées à la Russie qui soutiennent la guerre contre l'Ukraine.

Les relations de la Russie avec de nombreux autres États occidentaux sont tout aussi conflictuelles.

Les activités d'ingérence étrangère de la Russie cherchent à déstabiliser ou à délégitimer les États démocratiques. La Russie s'attaque à la démocratie par le biais de campagnes de mésinformation et de désinformation et, de plus en plus, par l'entremise de l'intelligence artificielle générative (l'« **IA** »). Elle dispose également de cybercapacités sophistiquées. Au cours des deux dernières années, la guerre menée par la Russie en Ukraine a été à l'origine d'une grande partie de ses efforts de désinformation.

Le gouvernement estime actuellement que la Russie a la capacité de se livrer à d'importantes activités d'ingérence étrangère contre le Canada. Toutefois, elle ne semble pas en avoir l'intention puisque la Russie ne perçoit pas le Canada comme une menace existentielle pour elle. Jusqu'à présent, le gouvernement n'a pas observé d'ingérence russe propre aux processus démocratiques du Canada. Néanmoins, la Russie mène depuis longtemps une campagne visant à discréditer les démocraties occidentales en général, et plus particulièrement les États-Unis et leurs alliés. Par exemple, RT, un média contrôlé par l'État russe, aurait secrètement financé et dirigé une société américaine pour publier des vidéos en anglais sur plusieurs plateformes de médias sociaux dans le but d'amplifier les divisions entre les Américains.

Le Centre de la sécurité des télécommunications (le « **CST** ») a observé des cybermenaces russes au Canada, mais pas contre les institutions démocratiques canadiennes. Des témoins du SCRS ont noté que le soutien ferme du Canada à l'Ukraine pourrait avoir une incidence sur les tentatives de la Russie d'influencer les prochaines élections fédérales. Les efforts importants de la Russie pour s'ingérer dans les élections en Europe démontrent sa capacité continue d'ingérence.

Pakistan

Les activités d'ingérence étrangère du Pakistan sont opportunistes et sont liées aux mauvaises relations entre le Pakistan et l'Inde. Le Pakistan se livre à de l'ingérence étrangère au Canada afin de promouvoir sa propre stabilité et de contrer l'influence croissante de l'Inde. Ses activités visent diverses facettes de la société canadienne et tous les ordres de gouvernement. Pour l'instant, le Pakistan est plus susceptible de s'appuyer sur des éléments communautaires locaux, plutôt que sur des cybermesures ou sur l'intelligence artificielle, pour faciliter ses activités d'ingérence étrangère.

Iran

La relation du Canada avec l'Iran est très limitée. Les relations diplomatiques ont été rompues en 2012 lorsque le Canada a fermé son ambassade à Téhéran et expulsé du Canada tous les diplomates iraniens en raison de préoccupations concernant le bilan de l'Iran en matière de droits de la personne et son soutien au terrorisme. Il n'y a actuellement pratiquement aucun contact officiel de gouvernement à gouvernement entre les deux pays.

L'Iran n'est pas actuellement, et n'a jamais été historiquement, un acteur important d'ingérence étrangère dans les élections fédérales canadiennes ou d'autres institutions démocratiques. L'Iran se concentre plutôt sur la répression transnationale pour empêcher la critique de son gouvernement.

L'Iran s'appuie sur des groupes criminels pour mener à bien ses activités d'ingérence et procède à du harcèlement psychologique en ligne. Le SCRS a reconnu que ces tactiques peuvent très bien empêcher les gens de participer aux processus démocratiques canadiens, mais il est difficile de le déterminer avec certitude.

Les témoins du SCRS ont également noté que le Canada a récemment inscrit le Corps des Gardiens de la révolution islamique de l'Iran sur la liste des entités terroristes. Parmi les réactions potentielles de l'Iran, ce geste pourrait entraîner une augmentation des activités d'ingérence étrangère à l'approche d'une élection.

Autres acteurs menaçants

La Commission a entendu des témoignages et reçu des informations sur d'autres acteurs menaçants susceptibles de se livrer à de la répression transnationale. Ces pays s'intéressent très peu aux institutions démocratiques du Canada et cherchent plutôt à contrôler les membres de la diaspora et à réduire les dissidents au silence. Au chapitre 17 (volume 4), je discute de ce que j'ai entendu au sujet de la répression transnationale au Canada.

10.4 Les tactiques répandues d'ingérence étrangère

Les États étrangers ont recours à l'ingérence pour semer la discorde, biaiser l'élaboration des politiques et les décisions, et influencer l'opinion publique pour qu'elle soutienne leurs programmes. Les tactiques utilisées et les cibles choisies varient.

Cultiver à long terme

Les acteurs menaçants consacrent des ressources considérables à cultiver des relations profondes et durables avec des cibles comme les parlementaires ou les candidats aux élections, souvent par l'intermédiaire de mandataires ou de collaborateurs qui cachent leur affiliation à un État étranger. Le renseignement indique que les États étrangers cherchent à cultiver des relations avec les politiciens et à les aider lorsqu'ils pensent que ces politiciens auront du pouvoir ou de l'influence au sein du gouvernement. L'aide peut prendre de nombreuses formes, notamment l'octroi de ressources, de conseils et le déploiement de campagnes de désinformation qui peuvent aider un candidat aux dépens d'un autre. En se rapprochant des décideurs politiques, les États étrangers peuvent soutenir ou supprimer des positions politiques particulières.

Obtenir des informations

Les acteurs menaçants peuvent essayer de manipuler les personnes pour qu'elles partagent des informations précieuses avec eux. Un acteur menaçant peut communiquer des informations confidentielles en espérant que la personne lui rendra la pareille. Ici aussi, les politiciens peuvent représenter des cibles attrayantes. Les responsables de campagne, le personnel politique et d'autres personnes peuvent également devenir des cibles en raison de leur accès à des informations confidentielles.

Financer de manière occulte

Les agences de renseignement ont vu des partis politiques et des candidats recevoir des dons qui semblaient provenir d'une Canadienne ou d'un Canadien, mais qui, en réalité, provenaient d'un acteur menaçant étranger. La raison la plus évidente expliquant de tels dons est le désir de soutenir des candidats considérés comme réceptifs aux intérêts de l'État étranger, ou d'aider à vaincre des candidats opposés considérés comme hostiles à l'état étranger. Dans certains cas, le candidat ne sait même pas qu'il reçoit du soutien financier d'un État étranger.

D'autres fois, le financement peut être utilisé pour que le candidat se sente redevable envers l'État étranger ou ses mandataires. Le financement fourni par l'intermédiaire d'un mandataire peut contribuer à consolider la perception que ce dernier est le gardien du soutien de la communauté. Le financement peut contribuer à établir un lien durable entre l'acteur menaçant et le candidat ou le titulaire d'une fonction. Évidemment, cela est vrai dans la mesure où le candidat sait qu'il a reçu ce soutien financier.

Mobiliser les organisations communautaires et en tirer parti

Certains acteurs menaçants utilisent les réseaux communautaires locaux pour faciliter les activités d'ingérence étrangère. La République populaire de Chine (la RPC), par exemple, s'appuie sur des membres des communautés issues des diasporas et sur les réseaux existants établis par ses ambassades et ses consulats. Les représentants d'États étrangers peuvent également diriger ou intimider secrètement des groupes communautaires pour qu'ils fassent pression en leur nom, ou identifier et marginaliser secrètement des candidats ou des politiciens qui ne soutiennent pas l'État étranger. Ainsi, les organisations communautaires peuvent être à la fois les victimes de l'ingérence étrangère et le vecteur de cette ingérence. Il faut donc veiller à ne pas attribuer aveuglément aux organisations communautaires la responsabilité de l'ingérence étrangère, et garder à l'esprit que la plupart d'entre elles sont des victimes et non des participantes actives.

Exploiter les possibilités offertes par les partis politiques

Chaque parti politique dispose de son propre processus d'investiture des candidats et de sélection des chefs. Ces processus ne sont généralement pas réglementés. Ils sont en grande partie sous le contrôle des partis.

Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (voir le **chapitre 11**) a estimé que les processus d'investiture des candidats et de sélection des chefs étaient vulnérables à des acteurs étatiques hostiles. Par exemple, les circonscriptions considérées comme des « sièges sûrs » peuvent s'avérer attrayantes pour les États qui cherchent à influencer la politique. Aider quelqu'un à remporter l'investiture du parti dans une telle circonscription garantit probablement son succès électoral.

J'examine de manière plus détaillée le rôle que les règles et les processus des partis politiques peuvent jouer dans l'ingérence étrangère au **chapitre 13**.

Recourir à l'extorsion et aux menaces

Les États peuvent recourir à des tactiques d'ingérence plus agressives, comme l'extorsion ou les menaces. Ces tactiques sont souvent utilisées comme outils de répression transnationale. Par exemple, un État étranger peut contraindre quelqu'un en menaçant les membres de sa famille qui vivent dans cet État. Les États peuvent également tenter d'extorquer ou de menacer des représentants élus afin d'influencer leurs activités officielles.

Recourir aux cybermenaces

La communauté de la sécurité et du renseignement du Canada estime que les cybermenaces qui pèsent sur les institutions démocratiques du pays sont de plus en plus nombreuses et sophistiquées. Le Centre canadien pour la cybersécurité (le « **CCC** ») du CST constate que des États étrangers se livrent à des activités cybernétiques non seulement contre les infrastructures du gouvernement fédéral, mais aussi contre les infrastructures provinciales, territoriales et municipales, et contre des infrastructures non gouvernementales.

Les acteurs menaçants peuvent s'introduire dans un réseau en le piratant ou en trompant un utilisateur pour qu'il leur donne accès. Une fois qu'un acteur menaçant a obtenu l'accès, son objectif est généralement le cyberespionnage (voler la propriété intellectuelle ou collecter d'autres informations). Dans d'autres cas, l'acteur menaçant peut ne pas exploiter l'accès immédiatement, mais se positionner en vue d'une future cyberactivité.

Le CCC a détecté plusieurs tentatives d'acteurs étatiques étrangers qui ont voulu sonder l'infrastructure électorale du Canada, mais qui n'ont pas réussi à la compromettre. Cependant, la puissance croissante de la technologie augmente la menace de cyberattaques sur l'infrastructure, ainsi que, j'ajouterais, le risque que ces cyberattaques réussissent éventuellement.

L'influence des médias, la mésinformation et la désinformation

L'influence d'un État étranger sur les médias peut constituer un outil puissant d'ingérence étrangère. Le SCRS a décrit une « prise de contrôle » par la RPC des médias de langue chinoise au Canada, qui s'est étalée sur plusieurs décennies. Le SCRS estime que le Parti communiste chinois (PCC) tente de façonner le discours qu'il veut entendre par l'entremise des médias. De cette manière, l'espace pour les voix dissidentes peut devenir limité, des mesures incitatives économiques peuvent être donnés aux médias pour soutenir les positions du PCC, et l'autocensure peut augmenter.

Les acteurs menaçants étrangers manipulent les médias sociaux et traditionnels pour diffuser de la désinformation, amplifier un message particulier ou provoquer les utilisateurs. Les gens qui ignorent l'origine du contenu ou l'intention de l'acteur menaçant peuvent involontairement propager la désinformation. Dans ce cas, il s'agit de mésinformation.

Cela peut entraîner des conséquences importantes lorsque les acteurs menaçants utilisent les médias sociaux. Par exemple, en mai 2023, le Mécanisme de réponse rapide du Canada (le « **MRR du Canada** ») a découvert qu'un réseau de comptes amplifiait un grand nombre de récits faux ou trompeurs sur M. Chong, notamment en diffusant de faux récits sur son

identité et des commentaires et affirmations sur ses antécédents, ses positions politiques et son héritage familial. Au total, le MRR du Canada a évalué qu'entre deux et cinq millions d'utilisateurs de WeChat ont vu ce contenu faux ou trompeur. Le MRR du Canada était confiant que la campagne de désinformation était liée à la RPC.

Les progrès de l'intelligence artificielle (IA) générative et de la technologie des hypertrucages (imitations générées par l'IA, ou « *deep fakes* ») représentent un changement important survenu depuis les deux dernières élections fédérales. Le CCC a constaté une augmentation des contenus synthétiques en ligne (vidéos, sons et images manipulés ou fabriqués) en période électorale. L'IA générative facilite la manipulation des informations. Elle permet également de créer et de diffuser des contenus plus rapidement et plus facilement et, j'ajouterais, plus efficacement.

J'ai entendu des témoignages concernant un cas où le MRR du Canada a appris l'existence d'un réseau de robots (« *bots* ») qui, dans le cadre d'une campagne de camouflage de pourriels (« *spamouflage* »), a fait circuler trois vidéos YouTube considérées comme étant des hypertrucages de Xin Liu, un critique bien connu du PCC. Les vidéos montraient M. Liu en train de faire des allégations particulièrement virulentes et vilipendant le premier ministre canadien. Le MRR du Canada a estimé que les répercussions sur M. Liu avaient possiblement été très élevées. Il a probablement reçu des centaines de milliers d'alertes de Facebook, Twitter et YouTube avec de fausses allégations selon lesquelles il aurait diffamé des douzaines de parlementaires.

Le MRR du Canada est d'avis que l'utilisation d'une technologie sophistiquée d'hypertrucages dans une campagne de camouflage de pourriels était importante, suggérant une nouvelle tactique de la part de la RPC et augmentant la probabilité que le camouflage de pourriels puisse être plus persuasif pour un public élargi.

10.5 Les six cas détectés d'ingérence étrangère soupçonnée dans les processus démocratiques du Canada

Préparation de la liste

Dans le cadre de son enquête, la Commission a demandé au gouvernement canadien d'énumérer et de décrire tous les cas majeurs d'ingérence étrangère suspectée ciblant les processus démocratiques du Canada de 2018 à aujourd'hui, y compris les actions, les dates, les cibles, les pays, les acteurs clés, la circulation d'information et la réponse donnée.

Pour y répondre, le Bureau du Conseil privé a mené une série de consultations avec de hauts fonctionnaires du SCRS, d'Affaires mondiales Canada (« **AMC** »), du CST et de Sécurité publique Canada.

Le gouvernement a indiqué qu'il surveille généralement les modèles de comportement au fil du temps plutôt que de se concentrer sur des incidents précis et que pour cette raison, il a d'abord dû décider ce qui constituait un « cas » d'ingérence étrangère. Il a conclu que, entre autres critères, pour être un « cas d'ingérence étrangère », un cas doit répondre à la définition de la *Loi sur le Service canadien de renseignement de sécurité*, soit être une activité influencée par l'étranger qui constitue une menace pour la sécurité du Canada[1], et le gouvernement doit disposer de renseignement quant à l'incidence de l'activité. L'activité devait également être circonscrite, par opposition à des événements qui se déploient sur une plus longue période, comme l'entretien continu de relations avec un individu.

L'obligation de satisfaire à ces critères signifie que la liste fournie n'est pas un catalogue exhaustif des actes d'ingérence étrangère potentiels dans les institutions démocratiques du Canada, y compris les processus électoraux. En effet, ces exigences ont pu entraîner l'exclusion de certaines activités ou actions d'ingérence étrangère.

L'établissement de cette liste a fait l'objet de discussions au sein de la communauté de la sécurité nationale et du renseignement. Le SCRS a dressé une liste préliminaire. De hauts fonctionnaires ont ensuite recensé les cas qui répondaient à la définition de l'ingérence étrangère et qui avaient une incidence tangible sur les processus ou les institutions démocratiques. Les cas considérés comme des activités diplomatiques légitimes ont été exclus.

La liste définitive représente le consensus résultant de ces discussions.

La liste des six cas soupçonnés

Le gouvernement a remis à la Commission une liste de six cas majeurs d'ingérence étrangère soupçonnée.

Quatre de ces six cas concernent des soupçons d'ingérence étrangère dans les élections de 2019 ou de 2021 et sont examinés aux chapitres 7 et 8 (volume 2). Il s'agit des cas suivants :

- Des représentants du gouvernement pakistanais auraient tenté d'influencer clandestinement la politique fédérale canadienne avant les élections fédérales de 2019 afin de favoriser les intérêts du Pakistan au Canada.

[1] *Loi sur le Service canadien du renseignement de sécurité*, art. 2. Les activités influencées par l'étranger sont définies au paragraphe b) de la définition de « menaces envers la sécurité du Canada ».

- Un représentant d'un gouvernement étranger serait soupçonné d'ingérence étrangère à l'encontre d'un candidat du Parti libéral du Canada (le « **Parti libéral** »).
- La RPC aurait activement soutenu la course à l'investiture fédérale d'un candidat du Parti libéral dans la circonscription de Don Valley-Nord (Ontario) en 2019, notamment en utilisant un agent mandataire.
- Le gouvernement indien aurait eu recours à des agents mandataires pour apporter un soutien financier clandestin à certains candidats de trois partis politiques lors d'une élection fédérale.

La Commission a enquêté sur deux autres cas recensés sur cette liste et a reçu et examiné les rapports de renseignement du SCRS concernant ceux-ci.

La Commission a également interrogé à huis clos le SCRS et d'autres représentants du gouvernement concernant ceux-ci. Ces cas étant fondés sur des informations hautement confidentielles, les descriptions ci-dessous représentent le maximum d'informations que je peux divulguer publiquement. J'aborde ces deux cas présumés plus en détail dans le complément classifié qui accompagne le présent rapport.

Dans le premier cas, il a été signalé qu'un gouvernement étranger avait entrepris plusieurs actions, y compris de l'ingérence, pour réduire les chances d'élection d'un candidat du Parti libéral. Le gouvernement étranger est soupçonné d'avoir agi de la sorte en raison du soutien apporté par le candidat à des enjeux perçus comme contraires aux intérêts de cet État.

Les activités du gouvernement étranger se sont probablement étendues au-delà de la campagne électorale et ont vraisemblablement eu une incidence négative sur la carrière politique de la personne. Ces informations ont été communiquées pour alerter des fonctionnaires fédéraux des efforts agressifs du gouvernement étranger pour contrecarrer la campagne du candidat.

La preuve tend à indiquer qu'aucune information à ce sujet n'a été communiquée au niveau politique du gouvernement jusqu'à ce que la liste demandée par la Commission soit préparée. Le premier ministre s'est dit stupéfait de ne pas avoir été informé de ces événements, étant donné qu'ils impliquaient son parti et que l'information aurait été pertinente pour lui en tant que chef de parti. Il s'est dit préoccupé par le fait qu'il n'ait pas été breffé, malgré son interaction permanente avec des responsables gouvernementaux au sujet de l'ingérence étrangère. Toutefois, il est convaincu qu'il aurait été informé de l'incident si les procédures actuelles pour la transmission de l'information avaient été en place. Je partage la stupéfaction du premier ministre de ne pas avoir été avisé de cet incident au moment des événements et, en fait, jusqu'aux travaux de la Commission.

Le deuxième cas concerne un ancien parlementaire de l'opposition qui est soupçonné d'avoir tenté d'influencer les travaux parlementaires au nom d'un gouvernement étranger. Un représentant d'un gouvernement étranger lui aurait demandé d'entreprendre une action particulière, ce qu'il aurait fait.

Les six cas mentionnés ci-dessus sont des évaluations basées sur des rapports de renseignement, et ne constituent pas des cas avérés. Des éléments du tableau peuvent manquer. Des témoins du SCRS m'ont expliqué que leurs enquêtes étaient généralement axées sur les acteurs menaçants, et non sur les candidats ou les élus qui interagissent avec eux. Le renseignement comporte donc souvent des lacunes en ce qui concerne les activités, le degré de connaissance et les motivations de ces candidats ou de ces représentants élus. En outre, les évaluations reposent sur les informations dont disposait le gouvernement à l'époque, et ces évaluations peuvent évoluer, parfois radicalement, au fil du temps.

Le septième cas

La liste initialement fournie à la Commission en juillet 2024 contenait un septième cas d'ingérence étrangère présumée. Le renseignement sous-jacent à ce septième cas indiquait qu'un représentant d'un gouvernement étranger aurait incité un député à entreprendre dans son rôle de parlementaire une action particulière qui soutiendrait les intérêts du gouvernement étranger. Les rapports indiquent en outre que des tactiques coercitives auraient été utilisées pour que le parlementaire agisse dans l'intérêt du gouvernement étranger.

Au début du mois de septembre 2024, pour des raisons qu'il dit ne pas être liées à l'enquête de la Commission, le SCRS a examiné des documents publics liés à ce cas. Il a alors constaté que des informations publiques contredisent directement un élément important du renseignement à l'origine du cas présumé. Le député n'avait pas, en fait, entrepris les actions indiquées dans le renseignement. Un témoin du SCRS a expliqué que le SCRS n'avait pas originalement vérifié les informations publiques pour savoir si le député avait effectivement entrepris les actions en question, car ce dernier ne faisait pas l'objet de l'enquête.

Je souligne que le renseignement qui soutient ce cas soupçonné d'ingérence étrangère indiquait à l'origine qu'il avait été recueilli auprès de sources jugées fiables. Pourtant, les informations transmises par ces sources se sont révélées inexactes.

Le SCRS a évidemment mis à jour son évaluation sur la base des informations publiquement accessibles et a communiqué son évaluation actualisée aux hauts fonctionnaires qui ont convenu que le cas devait être retiré de la liste. Le gouvernement en a informé la Commission peu de temps après. Toutefois, le SCRS a continué à considérer les événements comme un cas soupçonné de tentative d'ingérence d'un gouvernement étranger dans les processus démocratiques du Canada.

La découverte d'informations publiques a directement contredit un élément important du renseignement à l'origine du septième cas présumé et a finalement modifié l'évaluation du SCRS. Cela illustre à la fois les limites et la fragilité du renseignement.

En l'occurrence, le SCRS disposait de comptes rendus de conversations entre le fonctionnaire étranger et le député, ainsi qu'entre le fonctionnaire étranger et un autre fonctionnaire étranger. Cependant, il ne disposait pas d'informations directes permettant de savoir si le député avait effectivement entrepris l'action demandée. En effet, le SCRS n'a pas vérifié les informations accessibles au public pour savoir si le député avait effectivement entrepris l'action alléguée, car celui-ci ne faisait pas l'objet de l'enquête. Ceci a causé une lacune dans le renseignement qui aurait dû être comblée avant de tirer toute conclusion concernant les actions du député. L'omission de vérifier l'information a conduit à une conclusion erronée.

Cette situation illustre également la fragilité du renseignement. Cette fragilité existe même lorsque les informations sont recueillies auprès de sources considérées comme fiables. Par exemple, dans ce cas-ci, ces nouvelles informations, découvertes plusieurs années plus tard, mais accessibles à l'époque, ont complètement changé la compréhension du gouvernement quant à ce qui s'était passé et les conclusions à en tirer.

En fin de compte, les limites et la fragilité du renseignement exigent une très grande prudence lorsqu'on s'y fie pour tirer des conclusions ou formuler des allégations à l'égard d'une personne. Faire preuve de cette prudence est particulièrement important lorsque les allégations ou les conclusions qu'on en a tirées peuvent entraîner des conséquences importantes pour la personne et pour la confiance du public envers les institutions canadiennes.

10.6 Points de vue sur l'ingérence étrangère

Le concept d'« ingérence étrangère » est beaucoup plus facile à définir qu'à appliquer à des circonstances précises. Dans cette section, j'examine les difficultés rencontrées lorsqu'il s'agit de déterminer ce qu'est l'ingérence étrangère et la manière dont ces difficultés posent de véritables défis aux gouvernements lorsqu'ils cherchent à y répondre.

La ligne entre l'ingérence étrangère et l'influence étrangère légitime peut être difficile à tracer

Les décisions gouvernementales peuvent entraîner des conséquences au-delà des frontières nationales, par exemple sur le climat, le développement et la défense. Il en résulte que les pays tentent de s'influencer mutuellement pour protéger leurs propres intérêts. Même des tentatives d'influence agressives peuvent se révéler légitimes.

Par exemple, dans des limites appropriées, les États sont en droit d'utiliser des diplomates pour faire pression sur des gouvernements, des politiciens et des citoyens étrangers. Les diplomates peuvent agir directement ou par le biais d'intermédiaires. En fonction des lois de leur pays d'accueil, ils peuvent faire du lobbying, assister à des événements, faire de la publicité et financer des recherches. Les États se livrent également à de nombreuses autres activités légitimes pour influencer d'autres pays, par exemple lors de réunions internationales, comme le G7.

Ces activités sont légitimes parce qu'elles se déroulent ouvertement et n'impliquent pas de menaces pour des individus ou des groupes. L'ingérence étrangère est différente parce qu'elle est secrète ou menaçante.

La ligne entre l'influence étrangère (légitime) et l'ingérence étrangère (illégitime) peut sembler facile à tracer. Or, dans la pratique, ce n'est pas le cas. Certains témoins entendus par la Commission ont parlé d'une « zone grise » entre l'influence étrangère clairement légitime et l'ingérence étrangère clairement illégitime. Autrement dit, l'ingérence et l'influence étrangères s'inscrivent dans un continuum. La situation devient encore plus complexe lorsque des pays se livrent à la fois à de l'influence et à de l'ingérence.

Un exemple provenant d'un document d'Affaires mondiales Canada (AMC) illustre la difficulté à distinguer l'influence légitime de l'ingérence illégitime :

> Un diplomate du pays X, en poste au Canada, demande à un éminent universitaire canadien de rédiger un article d'opinion s'opposant à l'approche du gouvernement du Canada sur une question internationale particulière et invitant les Canadiennes et les Canadiens à ne pas être d'accord non plus. L'universitaire rédige l'article d'opinion, qui est publié dans un journal national à grand tirage. [...] L'universitaire ne divulgue pas sa relation avec la personne employée par le gouvernement étranger.[2]

Il n'y a rien de mal à ce qu'un diplomate discute de la politique gouvernementale avec un universitaire. Il n'y a rien de mal à ce qu'un diplomate tente de convaincre des Canadiennes et des Canadiens influents de se ranger à son avis. Il n'y a rien de mal non plus à ce que des universitaires rédigent des articles d'opinion critiquant le Canada.

Cependant, si le diplomate demande à l'universitaire de cacher leur relation, l'activité devient de l'ingérence étrangère en raison de ce secret. Et qu'en est-il si le diplomate n'a pas expressément demandé de cacher leur relation, mais que l'universitaire a implicitement compris qu'il devait le faire? Cela complique la distinction entre l'influence légitime et l'ingérence illégitime. En

[2] Affaires mondiales Canada, *Influence and Interference: Distinctions in the context of diplomatic relations and democratic processes* (« Influence et ingérence : Distinctions dans le cadre de relations diplomatiques et de processus démocratiques »), p. 6, CAN008822.

outre, un observateur extérieur n'aurait probablement jamais connaissance de cette relation, de sorte qu'il serait difficile pour lui de conclure que les activités qui en résultent constituent de l'ingérence étrangère de la part d'un État donné.

Il est également important de reconnaître qu'il n'existe pas de définition internationale commune de l'ingérence étrangère. Les témoins d'AMC ont indiqué qu'une telle définition ne serait pas possible dans le contexte géopolitique actuel. Le Canada peut considérer certaines activités comme de l'influence ou de l'ingérence étrangères alors que ses adversaires peuvent être d'un avis contraire.

Par exemple, la République populaire de Chine (RPC) maintient qu'il s'agit d'ingérence étrangère lorsque les autres pays la critiquent en affirmant qu'elle ne respecte pas les obligations internationales en matière de droits de la personne. AMC considère ces critiques comme un moyen légitime de demander des comptes à la RPC en tant que membre de la communauté internationale. AMC a déclaré qu'une telle critique se distingue des activités secrètes des fonctionnaires ou des agences de la RPC au Canada. On m'a dit que cette différence philosophique peut poser des problèmes lorsqu'AMC interagit avec la RPC au sujet de l'ingérence étrangère.

Le sous-ministre des Affaires étrangères, David Morrison a déclaré que les interprétations divergentes de l'ingérence étrangère signifient qu'AMC devrait en faire davantage pour s'assurer que les fonctionnaires étrangers au Canada savent ce que le Canada considère comme une activité diplomatique acceptable par rapport à de l'ingérence étrangère. Le Canada peut, par exemple, communiquer clairement où sont les lignes à ne pas franchir, et établir qu'il réagira si ces lignes sont transgressées. Je suis d'accord avec lui et je reviendrai sur cette question dans mes recommandations.

Un même concept vu sous des angles différents

Au Canada, la définition de travail de l'ingérence étrangère étatique est généralement semblable entre les ministères et les agences du gouvernement. Elle comprend les activités influencées par un État étranger au sein du Canada ou en relation avec celui-ci, qui sont préjudiciables aux intérêts du Canada et qui sont clandestines, trompeuses ou qui impliquent une menace pour quelqu'un.

Cependant, les différents ministères et agences peuvent toutefois diverger sur la question de savoir si un ensemble de faits constitue de l'ingérence étrangère et, dans l'affirmative, sur la gravité de cette ingérence.

Cela n'est pas surprenant. Les ministères et les agences appliquent cette définition dans l'optique de leurs mandats et de leurs pouvoirs respectifs. Ces optiques peuvent, à leur tour, amener les fonctionnaires à considérer un ensemble de faits différemment de leurs collègues de la fonction publique.

Par exemple, en dehors d'une période électorale, le personnel d'un consulat étranger peut demander à un membre de la communauté canadienne de faire pression sur un député pour qu'il vote d'une certaine manière. Le SCRS peut considérer qu'il s'agit d'un État qui utilise secrètement un mandataire pour se livrer à de l'ingérence étrangère. Mais AMC peut, du point de vue de la politique étrangère, considérer la demande comme une activité diplomatique légitime tant que le renseignement ne suggère pas que la demande était destinée à être secrète, clandestine, trompeuse ou menaçante.

Des perspectives différentes ne sont pas nécessairement source de vulnérabilité

Tant qu'il ne paralyse pas la prise de décision, le débat au sein du gouvernement à savoir si quelque chose constitue ou non de l'ingérence étrangère peut représenter un atout. Les tensions entre les ministères ou les agences existent dans tous les travaux du gouvernement, et pas seulement dans ceux relatifs à l'ingérence étrangère.

La discussion et le débat sont nécessaires à un bon gouvernement. L'ancien directeur du SCRS, David Vigneault, s'exprimant sur l'ingérence étrangère, a déclaré qu'il est sain dans une démocratie que les agences de renseignement n'aient pas toujours le dernier mot dans les discussions sur la sécurité nationale, car il est dangereux d'accorder trop de poids à un seul point de vue. Différents points de vue facilitent une réponse coordonnée qui tient compte de l'ensemble des risques, priorités, des valeurs et des intérêts pertinents, et, en général, favorise l'atteinte d'un meilleur résultat. Cela dit, il faut éviter que le débat et la discussion se poursuivent indéfiniment sans qu'aucune décision ne soit prise.

Le gouvernement reconnaît parfois expressément dans la législation la nécessité de tenir compte de différents points de vue dans la prise de décision. Par exemple, la *Loi sur le Centre de sécurité des télécommunications* permet au ministre de la Défense nationale de délivrer une autorisation de cyberopérations actives pour contrer les activités d'un État étranger, ou d'autres menaces précises, seulement si le ministre des Affaires étrangères demande ou consent à ce qu'elle soit délivrée[3]. La *Loi sur le Service canadien du renseignement de sécurité* (la « *Loi sur le SCRS* ») exige qu'avant de prendre une mesure de réduction de la menace (une « **MRM** »), le SCRS consulte, au besoin, d'autres agences ou ministères fédéraux afin d'établir s'ils sont en mesure de réduire la menace[4].

Des vérifications supplémentaires sont parfois mises en œuvre du fait d'une politique, même si la législation ne le requiert pas. Par exemple, les directives ministérielles exigent que le SCRS consulte d'autres ministères, comme AMC, le ministère de la Justice et Sécurité publique Canada, pour évaluer le

[3] *Loi sur le Centre de la sécurité des télécommunications*, art. 30(2).
[4] *Loi sur le Service canadien du renseignement de sécurité*, art. 12.1(3).

degré de risque d'une MRM dans quatre domaines : juridique, politique étrangère, opérationnel et réputationnel. Si la MRM présente un risque élevé et a un lien avec l'étranger, le SCRS ne peut aller de l'avant qu'avec l'approbation du sous-ministre ou du ministre des Affaires étrangères.

Les comités interministériels au niveau des sous-ministres, des sous-ministres adjoints et des directeurs généraux, sont constitués pour aider le gouvernement à bénéficier de différents points de vue. De même, le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections et le Panel des cinq (voir le **chapitre 11**) sont des forums où le gouvernement rassemble délibérément des points de vue différents sur les questions d'ingérence étrangère.

Lorsqu'il s'agit de répondre à une menace d'ingérence étrangère et de décider quand le faire, le gouvernement doit avoir une vision globale et ne pas envisager les choses uniquement sous l'angle de la menace, de la politique étrangère ou de l'application de la loi. Il est essentiel que les agences et les ministères apportent leurs propres points de vue lorsqu'ils abordent des cas d'ingérence étrangère potentielle. La prise en compte de points de vue variés permet de prendre des décisions plus éclairées. Cela est particulièrement important dans le contexte de l'ingérence étrangère où le renseignement, dont la qualité et la fiabilité peuvent varier considérablement, est pris en compte et où les tactiques d'ingérence étrangère sont en constante évolution. Bien entendu, lorsque des informations crédibles et fiables font état d'une menace requérant une réponse immédiate, telle qu'une menace pour l'intégrité physique d'une personne, les considérations sont différentes. Dans ce cas, la priorité devrait être d'agir le plus rapidement possible.

J'ai aussi entendu que l'intensification des discussions au cours des trois ou quatre dernières années a conduit à un accord plus large et à une meilleure compréhension des différents points de vue au sein du gouvernement sur ce qui constitue de l'ingérence étrangère. M. Vigneault a cité en exemple la compréhension actuelle qu'ont les dirigeants politiques et le SCRS de l'ingérence étrangère dans les processus d'investiture. Puisque l'on m'a dit que le gouvernement travaille actuellement à développer une compréhension de l'ingérence étrangère à l'échelle du gouvernement, je m'attends à ce qu'il y ait plus d'opinions communes dans certains domaines, mais je m'attends aussi à ce qu'un débat sain se poursuive. Il s'agit d'une caractéristique positive du système, et non d'un bogue dysfonctionnel. Cependant, un débat cesse d'être sain lorsqu'il entrave indûment la prise de décision.

10.7 Conclusion

Dans ce chapitre, j'ai décrit à vol d'oiseau la nature de la menace d'ingérence étrangère à laquelle le Canada est confronté. Dans le chapitre suivant, j'examine la manière dont le Canada répond à cette menace.

CHAPITRE 11

Comment le Canada se protège contre l’ingérence étrangère

Les informations peuvent être incomplètes : *des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

11.1 Introduction

Au chapitre 6 (volume 2), j'ai abordé les différentes entités fédérales concernées par l'ingérence étrangère. Dans le présent chapitre, je détaille les pouvoirs et autorités spécifiques dont disposent ces entités pour répondre à l'ingérence étrangère. J'aborde également la façon dont la coordination entre ces entités est assurée.

11.2 Le cycle du renseignement

La communauté gouvernementale de la sécurité nationale et du renseignement comprend des producteurs et des consommateurs de renseignement. Les producteurs collectent et évaluent le renseignement avant de communiquer leurs produits aux consommateurs. Les consommateurs reçoivent des produits de renseignement de la part des producteurs de renseignement.

Les produits de renseignement sont créés selon un processus appelé « cycle du renseignement », qui vise à faire en sorte que le renseignement soit pertinent pour les responsables des orientations politiques, les décideurs et les intérêts nationaux du Canada. La collecte et l'évaluation du renseignement sont guidées par les priorités du gouvernement ainsi que par ses capacités et ressources. Le cycle du renseignement est abordé plus en détail au chapitre 5 (volume 2).

Le Cabinet fixe les priorités en matière de renseignement tous les deux ans. Ces priorités sont développées sur la base de consultations menées à l'échelle du gouvernement. Le Bureau du conseil privé (le « **BCP** ») supervise ce processus par l'intermédiaire de son Secrétariat de la sécurité et du renseignement.

Le Comité du Cabinet chargé des affaires internationales et de la sécurité publique régit et surveille la mise en œuvre des priorités en matière de renseignement avec le soutien de comités composés de hauts fonctionnaires. Le Cabinet a confié à ces comités la responsabilité de définir les besoins précis en cette matière, de superviser l'évaluation des performances et de lui recommander de nouvelles priorités.

Une fois ces priorités approuvées, les ministres des Affaires étrangères, de la Défense nationale ainsi que de la Sécurité publique et de la Protection civile formulent des directives ministérielles à l'intention des ministères et organismes qui sont sous leur responsabilité.

Sur le plan opérationnel, chaque ministère définit ses besoins en matière de renseignement d'après les priorités du Cabinet. Il s'agit des besoins précis liés aux priorités. Ces besoins contribuent à la planification opérationnelle par les producteurs de renseignement. Alors que les priorités sont générales et restent valables pendant deux ans, les besoins liés au renseignement sont plus précis et peuvent être modifiés à tout moment.

Au cours du cycle de renseignement de deux ans, le Cabinet reçoit deux mises à jour. La première a lieu un an après le début du cycle. Elle permet de recueillir les commentaires des consommateurs de renseignement sur le degré de soutien reçu en réponse à leurs besoins. La mise à jour de fin de cycle est similaire et est communiquée au Cabinet lorsqu'il commence à mettre à jour les priorités pour le cycle de renseignement suivant.

11.3 Acteurs clés de la communauté de la sécurité nationale et du renseignement

Le Service canadien du renseignement de sécurité (SCRS)

Le Service canadien du renseignement de sécurité (le « **SCRS** ») est le service de renseignement intérieur du Canada. Son mandat principal, énoncé à l'article 12 de la *Loi sur le Service canadien du renseignement de* sécurité (la « ***Loi sur le SCRS*** »), est de recueillir, d'analyser et de conserver les informations et le renseignement sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces pour la sécurité du Canada.

Le SCRS fait ensuite rapport au gouvernement et le conseille sur ces menaces. L'ingérence étrangère est une menace pour la sécurité du Canada. Le SCRS peut enquêter sur des menaces à l'intérieur ou à l'extérieur du Canada.

En plus de son mandat touchant les menaces envers la sécurité du Canada, le SCRS a un mandat très limité en matière de renseignement étranger. Selon l'article 16 de la *Loi sur le SCRS*, le SCRS peut recueillir du renseignement étranger à la demande du ministre des Affaires étrangères ou de la Défense nationale et avec le consentement du ministre de la Sécurité publique, le

SCRS peut recueillir du renseignement étranger[5]. Cela signifie essentiellement que ces ministres peuvent demander au SCRS de les aider à recueillir du renseignement étranger. Cependant, le SCRS ne peut le faire que dans les limites du Canada.

Avant l'adoption de la *Loi sur la lutte contre l'ingérence étrangère* (présentée comme le projet de loi C-70), la collecte effectuée par le SCRS selon l'article 16 était aussi limitée aux informations se trouvant à l'intérieur du Canada. La *Loi sur la lutte contre l'ingérence étrangère* a modifié cela en ajoutant l'article 16(1.1) à la *Loi sur le SCRS,* lequel prévoit, au sujet de l'assistance fournie au titre de l'article 16(1) : « Si elle vise une personne ou un objet qui se trouve au Canada ou un individu qui se trouvait au Canada et qui se trouve temporairement à l'extérieur du Canada, l'assistance [...] peut notamment viser la collecte, depuis le Canada, d'informations ou de renseignements qui se trouvent à l'extérieur du Canada. »

Collecte du renseignement

Le renseignement est recueilli par les bureaux régionaux du SCRS en fonction des priorités du Cabinet en matière de renseignement et des besoins des ministères. Les bureaux régionaux et l'administration centrale travaillent ensemble pour s'assurer que les régions recueillent les informations les plus utiles aux clients gouvernementaux.

Le SCRS recueille également du renseignement sur les menaces mondiales émergentes.

Le SCRS recueille des informations auprès de diverses sources, notamment humaines et techniques, ainsi que des éléments provenant de sources ouvertes.

Le SCRS utilise les pouvoirs qui lui sont conférés par la loi pour enquêter sur des menaces précises en ayant recours à différents outils et techniques opérationnels nécessitant divers niveaux d'approbation interne.

Le SCRS peut également recourir à des mandats, qui lui permettent de mener des enquêtes plus intrusives. Ces mandats peuvent être à usage multiple (par exemple, pour autoriser une surveillance continue) ou, depuis l'adoption de la *Loi sur la lutte contre l'ingérence étrangère,* à usage unique (par exemple, pour extraire les données d'un seul appareil électronique).

Enfin, le SCRS peut s'associer à d'autres pour faire avancer ses enquêtes. Par exemple, il travaille avec des organismes canadiens et un grand nombre de services de renseignement étrangers pour mettre à profit leur expertise et leurs moyens techniques et opérationnels.

---

[5] Le renseignement étranger est défini comme le renseignement qui, dans les domaines de la défense et de la conduite des affaires internationales du Canada, est relatif aux moyens, aux intentions ou aux activités de personnes, d'États étrangers ou de groupes d'États étrangers, ou de toute personne autre qu'un citoyen canadien, un résident permanent, ou une personne morale constituée sous le régime d'une loi fédérale ou provinciale.

Évaluation et analyse du renseignement

Une fois le renseignement collecté, le SCRS l'évalue, l'analyse et produit divers produits de renseignement qui sont partagés au sein du gouvernement. Jusqu'à l'automne 2023, le SCRS envoyait ses produits par courriel sur le Réseau canadien Très secret. Comme je l'explique au chapitre 14 (volume 4), j'ai entendu des témoignages indiquant que ce n'était souvent pas un moyen efficace de transmettre du renseignement. Le SCRS utilise maintenant la base de données centralisée actualisée du Centre de la sécurité des télécommunications pour partager des informations.

Les produits de renseignement du SCRS sont destinés à éclairer l'élaboration des politiques gouvernementales et le contexte plus large de la sécurité nationale.

Le renseignement du SCRS peut également contribuer à la prise de décisions gouvernementales sur le plan opérationnel. Par exemple, si le SCRS dispose de renseignement indiquant qu'un candidat à un poste diplomatique au Canada est impliqué dans des activités d'espionnage, le gouvernement peut lui refuser l'entrée au pays. Le SCRS effectue également des évaluations de sécurité pour les personnes qui ont besoin d'avoir accès à des informations classifiées au sein du gouvernement. Ces évaluations concernent à la fois les fonctionnaires et les politiciens dont la candidature est envisagée pour un poste au Parlement ou au Cabinet. Le cabinet du premier ministre considère que cette procédure de vérification est un contexte important dans lequel il reçoit du renseignement.

Outils d'intervention

Mesures de réduction de la menace

Depuis 2015, le SCRS a l'autorisation de mettre en œuvre des mesures de réduction de la menace (des « **MRM** ») pour atténuer les menaces pesant sur la sécurité du Canada, notamment en communiquant des informations classifiées à des personnes qui n'ont pas d'autorisation de sécurité et qui ne font pas partie du gouvernement fédéral.

Pour mettre en œuvre une MRM, le SCRS doit avoir des motifs raisonnables de croire que l'activité visée par la mesure constitue une menace pour la sécurité du Canada, et la MRM doit nécessairement servir à la réduire. Ce seuil signifie que le SCRS ne peut pas utiliser son pouvoir relatif aux MRM pour fournir des informations classifiées à n'importe qui, y compris des élus, à moins que l'objectif de la communication de ces informations soit de réduire une menace.

Le SCRS dispose de trois types de MRM :

- **Les messages.** Le SCRS transmet des informations au sujet, directement ou indirectement, pour influencer son comportement. Il peut s'agir de rencontrer l'associé d'un acteur menaçant et de lui dire que le SCRS est au courant des activités de l'acteur menaçant, dans le but que l'associé lui rapporte cette conversation.

- **L'influence**. Le SCRS communique des informations à un tiers (par exemple, une plateforme en ligne) pour lui permettre d'agir contre l'activité menaçante reconnue (par exemple, la mésinformation). L'objectif est d'entraver l'activité liée à la menace, mais les moyens sont laissés à la discrétion du tiers.
- **L'obstruction**. Le SCRS influe directement sur la capacité d'un sujet de faire quelque chose (par exemple, il l'empêche d'atteindre une cible). L'objectif est d'entraver l'activité liée à la menace.

Les MRM doivent être raisonnables et proportionnelles à la nature et à la gravité de la menace.

Avant de mettre en œuvre une MRM, le SCRS consulte d'autres organismes comme Affaires mondiales Canada (« **AMC** »), le ministère de la Justice, la Gendarmerie royale du Canada (la « **GRC** ») et Sécurité publique Canada sur les risques posés par l'action proposée. Le SCRS évalue les MRM proposées en fonction de quatre catégories de risque :

- le risque opérationnel
- le risque lié à la politique étrangère, évalué en consultation avec AMC
- le risque juridique, évalué en consultation avec le ministère de la Justice
- le risque d'atteinte à la réputation, évalué en consultation avec Sécurité publique Canada.

Les risques sont classés sur une échelle comportant les niveaux faible, moyen et élevé, ce qui détermine le niveau d'approbation requis pour la MRM.

Selon l'article 12.1 de la *Loi sur le SCRS*, si une MRM risque de limiter une liberté ou un droit garanti par la *Charte des droits et libertés*, le SCRS doit obtenir un mandat avant de prendre des mesures. Depuis 2015, le SCRS a entrepris 20 MRM liées à l'ingérence étrangère ne nécessitant pas l'obtention d'un mandat. Il n'a entrepris aucune MRM liée à l'ingérence étrangère nécessitant l'obtention d'un mandat.

À titre d'exemple, en 2021, le SCRS a mis en œuvre une MRM relative aux activités d'ingérence étrangère de l'Inde. L'objectif était de protéger les institutions démocratiques en informant les députés, actuels et anciens, des activités d'ingérence étrangère de l'Inde au Canada. Cela impliquait des breffages classifiés et non classifiés, et des entretiens menés auprès des députés.

Tous les breffages visaient une sensibilisation générale à l'ingérence étrangère et aux efforts de l'Inde, tandis que certains ont aussi communiqué des informations ciblées sur les enjeux d'ingérence étrangère liés à l'Inde, notamment la promotion clandestine d'un programme favorable au gouvernement indien et le financement clandestin de candidats politiques, y compris par l'intermédiaire de mandataires.

Échange d'informations pour renforcer la résilience

En juillet 2024, la *Loi sur la lutte contre l'ingérence étrangère* a élargi les capacités du SCRS en matière de partage d'information. Il peut désormais communiquer des informations obtenues dans l'exercice de ses fonctions à toute personne ou entité aux fins de renforcer la résilience face aux menaces à la sécurité du Canada, si les conditions suivantes sont respectées :

- Les informations ont déjà été communiquées à un ministère ou à un organisme fédéral qui exerce des fonctions pour lesquelles elles sont pertinentes.
- Les informations ne contiennent pas de renseignements personnels autres que ceux concernant la personne qui reçoit les informations.
- Les informations ne contiennent pas le nom d'une société canadienne autre que celle à laquelle l'information est communiquée.

Cette nouvelle autorisation permet au SCRS de communiquer des informations classifiées à des personnes qui n'ont pas d'autorisation de sécurité et qui ne font pas partie du gouvernement fédéral. Il reste à voir dans quelle mesure et de quelle façon cela sera fait.

Breffages préventifs de sécurité

Le SCRS peut également échanger des informations non classifiées en fournissant à des individus un breffage préventif de sécurité (un « **BPS** »). Ces breffages ont pour but de sensibiliser un individu à la nature de la menace à laquelle il pourrait être confronté. Il s'agit presque toujours de breffages non classifiés, dérivés d'informations classifiées. Le SCRS a organisé des BPS à l'intention des députés avant les élections de 2021. J'aborde les BPS plus en détail au chapitre 15 (volume 4).

Échange d'information sur les menaces à l'intégrité physique d'une personne

Lorsque le SCRS dispose d'informations concernant une menace à l'intégrité physique d'une personne, il peut les transmettre aux forces de l'ordre, qui peuvent alors avertir la personne de la menace, en vertu de leur devoir de mise en garde, ou prendre d'autres mesures afin de remédier à la menace. En transmettant ces informations, le SCRS peut suggérer un moyen d'avertir la personne à propos de la menace sans communiquer d'information classifiée, y compris en fournissant à la police un document non classifié à utiliser pour avertir la personne de la menace.

Le SCRS n'a pas de politique concernant précisément la transmission à la police d'informations relatives à des menaces de mort. Cependant, des témoins du SCRS ont dit que, lorsqu'il dispose d'informations sur une menace d'atteinte à l'intégrité physique ou à la vie d'une personne, le SCRS fait immédiatement appel aux autorités policières pour s'assurer que la personne est protégée physiquement, tout en prenant des mesures pour protéger la source de l'information. Les témoins ont expliqué qu'il existe des

canaux de communication avec les forces de l'ordre et que le SCRS est en mesure de transmettre l'information rapidement.

Par exemple, selon le cadre Une Vision, qui régit l'échange d'informations entre le SCRS et la GRC (que j'examine plus en détail dans le volume 4, chapitre 14**),** la GRC peut agir sur la base d'informations transmises verbalement par le SCRS concernant une menace imminente pour la vie ou une menace de lésions corporelles graves. Il s'agit d'une exception à la règle normale selon laquelle la GRC ne peut agir sur la base d'informations reçues du SCRS tant que celui-ci n'a pas fourni une « lettre d'utilisation » officielle. Le cadre Une Vision met également l'accent sur la coopération le plus tôt possible et sur le fait que la sécurité publique est la priorité absolue des deux organisations.

Le Centre de la sécurité des télécommunications (CST)

Le Centre de la sécurité des télécommunications (CST) est l'agence de renseignement d'origine électromagnétique étrangère (dit « **SIGINT** ») du Canada et l'autorité technique en matière de cybersécurité et d'assurance de l'information. Son mandat comporte cinq aspects, énoncés aux articles 16 à 20 de la *Loi sur le Centre de la sécurité des télécommunications* :

- Le renseignement étranger, qui permet au CST d'exercer ses activités de SIGINT.
- La cybersécurité et l'assurance de l'information, qui permet de fournir des avis, des conseils et des services en matière de cybersécurité pour protéger les systèmes fédéraux et certains systèmes non fédéraux désignés.
- Les cyberopérations défensives, qui permettent au CST de prendre des mesures en ligne pour protéger les systèmes fédéraux et des systèmes non fédéraux désignés contre les cybermenaces étrangères.
- Les cyberopérations actives, qui permettent au CST de prendre des mesures en ligne pour perturber les capacités des acteurs menaçants étrangers.
- L'assistance technique et opérationnelle, qui permet au CST d'aider les forces de l'ordre canadiennes et les agences de sécurité, les Forces armées canadiennes et le ministère de la Défense nationale.

Le CST recueille du SIGINT en interceptant des communications et des informations électroniques, y compris sur Internet. Il s'emploie à déterminer les capacités, les intentions et les activités des entités étrangères conformément aux priorités du gouvernement en matière de renseignement. Le CST ne peut pas viser des Canadiennes et Canadiens ni quiconque au Canada lorsqu'il conduit ses activités SIGINT.

Le CST analyse le SIGINT pour informer le gouvernement des menaces étrangères pesant sur la sécurité du Canada, y compris l'ingérence étrangère, et pour soutenir la politique étrangère et la prise de décision.

Le CST fournit également des conseils et une assistance pour la défense contre les cyberattaques, il participe à des cyberopérations défensives et actives, et peut fournir une assistance technique à diverses entités fédérales.

Lorsque le CST assiste les agences de sécurité et les organismes d'application de la loi, notamment le SCRS et la GRC, il est soumis aux pouvoirs de l'entité requérante. Lorsqu'une entité requérante a le pouvoir de cibler des personnes au Canada, y compris des Canadiennes ou Canadiens, le CST peut assister cette entité en collectant du SIGINT portant sur ces personnes. Toute information obtenue par le CST appartient à l'entité requérante et non au CST.

Collecte du renseignement

Le CST s'appuie actuellement sur des autorisations ministérielles pour trois types de collecte de renseignement étranger :

- **Activités d'accès passif**. Le CST déploie des équipements pour recueillir secrètement des copies d'informations ou de transmissions transitant par l'infrastructure mondiale de l'information. L'accès passif représente le fondement de la majorité des activités de renseignement étranger du CST.
- **Activités d'exploitation de réseaux**. Le CST apporte des modifications ciblées à certaines parties de l'infrastructure mondiale de l'information ou en exploite les faiblesses. Les opérations sur les réseaux constituent la principale source de renseignements du CST. En 2023, elles représentaient la majeure partie de ses rapports sur la collecte de renseignement pour le compte du Canada.
- **Autres activités de renseignement étranger.** Le troisième mode de collecte de renseignement étranger n'est pas public et est décrit dans le supplément classifié de mon rapport.

Dans le cadre de son mandat en matière de renseignement étranger, le chef du CST sollicite une autorisation ministérielle pour permettre au CST de recueillir du renseignement étranger d'une manière qui pourrait violer les lois du Canada et qui pourrait, par inadvertance, porter atteinte aux attentes raisonnables en matière de protection de la vie privée des Canadiennes et Canadiens ainsi que des personnes se trouvant au Canada.

Évaluation et analyse du renseignement

Les rapports du CST sont fondés sur des faits et ne comportent pas d'évaluation ni d'analyse du renseignement. Les personnes qui reçoivent le renseignement du CST en évaluent la pertinence et l'importance. Le CST a commencé à prendre des mesures pour rendre ses produits plus accessibles aux clients, notamment

en les faisant précéder d'un bref résumé. Il a également regroupé plusieurs de ses rapports et des rapports du Groupe des cinq (communément appelé *Five Eyes*) dans des produits autonomes et a créé une nouvelle gamme de rapports appelée « produits de renseignement adaptés ».

Ces initiatives aideront certainement les différents acteurs à échanger leurs points de vue, et devraient permettre aux décideurs de saisir plus facilement et plus rapidement l'importance de certains éléments de renseignement.

Outils d'intervention

Capteurs sur les systèmes gouvernementaux

Le Centre canadien pour la cybersécurité (le « **CCC** ») du CST dispose de divers capteurs automatisés sophistiqués pour défendre les systèmes du gouvernement fédéral. Ces capteurs surveillent les informations en provenance et à destination des systèmes gouvernementaux. Ils aident à détecter les activités suspectes et les cyberattaques. Le programme a été déployé sur plusieurs années et couvre maintenant la plupart des ministères fédéraux. Le CCC a récemment commencé à installer ces capteurs sur les ordinateurs portables du gouvernement, ce qui a augmenté sa capacité à détecter et à prévenir les menaces.

Le cyberprogramme du CCC est efficace. Il arrête chaque jour près de six milliards (6 000 000 000) de cyberincidents malveillants contre le gouvernement fédéral. Chaque incident est une occasion pour le CST de découvrir des informations sur l'activité menaçante.

Depuis 2015, le CCC collabore avec Élections Canada pour renforcer l'infrastructure électorale canadienne. Depuis 2019, il utilise des capteurs sur l'infrastructure d'Élections Canada.

Le CCC travaille également sur demande avec les gouvernements provinciaux et territoriaux, notamment en utilisant des capteurs dans leurs systèmes. Il le fait en vertu d'une autorisation ministérielle.

Cyberopérations actives (CA)

Les cyberopérations actives (les « **CA** ») dégradent, perturbent ou influencent les capacités, les intentions ou les activités d'États, d'individus ou de groupes étrangers susceptibles de constituer une menace pour la sécurité nationale du Canada. Le CST s'appuie sur des autorisations ministérielles pour mener à bien ses CA.

Le CST mène actuellement des CA visant des entités étrangères. Par exemple, le CST a récemment mis en œuvre une CA pour contrer les activités d'une entité étrangère qui portait atteinte aux intérêts du Canada en matière de sécurité. Pour mener à bien ces opérations, le CST utilise diverses techniques, y compris des activités lui permettant d'accéder à des comptes ou à des réseaux en ligne.

Cyberopérations défensives (CD)

Les cyberopérations défensives (les « **CD** ») permettent au CST de prendre des mesures en ligne pour perturber les cybermenaces étrangères afin de protéger les infrastructures canadiennes ou les infrastructures d'importance pour le gouvernement. Le CST était prêt à mener des CD pour protéger les systèmes d'Élections Canada pendant les élections générales de 2019 et 2021. Heureusement, cela n'a pas été nécessaire.

Attribution des cyberattaques

Le CST utilise son expertise technique pour identifier les responsables d'un cyberévénement. L'attribution publique liée à un acteur étranger relève en dernier ressort de la décision d'Affaires mondiales Canada (AMC) (voir plus loin la description du cadre de cyberattribution d'AMC).

Cependant, il n'est pas toujours possible pour le CST d'attribuer une cyberattaque. L'attribution des cyberévénements est difficile et la majorité des cybermenaces ne sont pas attribuées. Toutefois, plus le CST dispose d'informations sur le contexte de la menace, les techniques courantes et un cyberincident précis, mieux il peut l'attribuer. Il se peut que le CST ait besoin de plus de temps pour attribuer un comportemetn nouveau à une entité étrangère.

L'attribution des campagnes de mésinformation et de désinformation est plus difficile. Quand le CST tente d'attribuer un cyberincident, il obtient souvent du renseignement étranger et des détails techniques sur l'incident, ce qui facilite l'attribution. En ce qui concerne les campagnes de mésinformation et de désinformation, le CST ne peut généralement pas obtenir les informations techniques pour faire une attribution parce qu'elles n'existent pas ou que l'entreprise de médias sociaux ne les fournit pas.

Je note également qu'en raison de son mandat, le CST est seulement impliqué dans les tentatives d'attribution des campagnes de mésinformation et de désinformation si elles comportent un caractère « étranger ». En effet, le CST ne peut pas collecter de renseignement SIGINT sur des Canadiennes et des Canadiens ou des individus qui se trouvent au Canada. Par conséquent, lorsque des entités étrangères ont recours à des mandataires au Canada pour diffuser de la mésinformation ou de la désinformation, le rôle du CST dans l'effort d'attribution de l'activité est limité.

Conseils aux partis politiques

Le Centre canadien de cybersécurité (CCC) a produit un guide de sécurité à l'intention des équipes de campagne, et, sur demande, le CST conseille ces dernières, de même que les partis politiques, en matière de cybersécurité. Les services offerts incluent :

- un examen de l'architecture du réseau et des conseils
- un examen de la sécurité des appels d'offres dans le domaine des technologies de l'information
- des conseils sur les tiers fournisseurs de services de cybersécurité qui respectent les principales normes de sécurité informatique, et évaluation de ces fournisseurs.

Le CST dispose également d'une cyberligne d'assistance pour les membres des partis politiques. Un seul problème a été signalé pendant la période électorale de 2019. Aucun n'a été signalé pendant les élections de 2021. Je note que cela ne signifie pas qu'aucun problème de ce type ne s'est produit. Cela est d'autant plus vrai que l'existence de la cyberligne d'assistance n'est pas très connue. Les partis politiques paraissent également ne pas connaître les conseils techniques et les services offerts via le CST.

Affaires mondiales Canada (AMC)

AMC est le ministère chargé des relations internationales du Canada. Il est l'un des plus grands consommateurs de renseignement au sein du gouvernement fédéral. Il se concentre sur le renseignement relatif aux capacités, aux intentions et aux activités des États étrangers. Il reçoit du renseignement d'organismes gouvernementaux comme le SCRS et le CST, ainsi que des homologues étrangers.

Collecte du renseignement

AMC est avant tout un consommateur et non un producteur de renseignement, mais il recueille néanmoins certains éléments de renseignement.

Les agents de liaison du renseignement d'AMC travaillent à découvert dans les consulats et les ambassades du Canada et reçoivent des informations des pays hôtes qui connaissent leur rôle. AMC rend également compte des informations confidentielles que les diplomates obtiennent de leurs contacts locaux. Cela inclut des informations reçues dans le cadre du Programme d'établissement de rapports sur la sécurité mondiale, qui fournit des rapports diplomatiques spécialisés sur les questions de sécurité. Ce sont des informations de nature sensible qui peuvent être classifiées ou non.

De plus, comme expliqué ci-dessus, le ministre des Affaires étrangères peut demander au SCRS de recueillir du renseignement étranger au Canada selon l'article 16 de la *Loi sur le SCRS*. Cette autorisation a été utilisée pour collecter du renseignement relatif à certains pays et à l'ingérence étrangère.

Évaluation et analyse du renseignement

La Direction générale du renseignement d'AMC évalue le renseignement et le communique à l'interne et à l'externe. La Direction générale était une petite équipe jusqu'en 2019 lorsque le financement a augmenté, lui permettant ainsi d'accroître sa capacité d'évaluation. Les évaluations du renseignement par AMC adoptent une perspective de politique étrangère ou de relations internationales. Elles servent deux objectifs principaux : évaluer la menace qui pèse sur les missions et les actifs canadiens à l'étranger, et informer et soutenir l'élaboration de la politique étrangère.

Outils d'intervention

Le Canada entretient des relations avec les pays étrangers conformément à deux conventions internationales : la *Convention de Vienne sur les relations diplomatiques* et la *Convention de Vienne sur les relations consulaires* (la « **CVRC** »). Le sous-ministre des Affaires étrangères, David Morrison, a décrit ces conventions comme étant les « règles du jeu » pour les interactions entre les États, notamment en ce qui concerne les ambassades et les consulats. Si des pays ne respectent pas la CVRC ou s'ils présentent autrement une menace pour la sécurité du Canada, AMC peut recourir à sa boîte à outils diplomatique.

De plus, le Mécanisme de réponse rapide du Canada (voir plus loin) contribue à la réponse du pays en matière d'ingérence étrangère en surveillant les informations en ligne accessibles au public afin de détecter la mésinformation et la désinformation pendant les périodes d'élections fédérales et, comme mentionné ci-dessus, AMC travaille également avec le CST à l'attribution de la responsabilité des cyberattaques menées contre le gouvernement fédéral.

Outils de réponse diplomatiques

AMC dispose de nombreux outils diplomatiques pour détecter, prévenir ou contrer l'ingérence étrangère. Ces outils sont utilisés en coordination avec le reste du gouvernement.

Les décisions du gouvernement concernant les outils diplomatiques à utiliser dans différentes situations dépendent de divers facteurs, dont la question en jeu, les intérêts concernés, l'incidence de leur utilisation sur les relations bilatérales ou multilatérales, ainsi que la disponibilité et l'efficacité d'autres solutions. Les réponses diplomatiques sont donc adaptées. Elles vont de la diplomatie discrète à la rupture totale des relations diplomatiques.

Les efforts diplomatiques commencent souvent de manière discrète, puis s'intensifient en fonction des besoins. Par exemple, le fait de soulever à plusieurs reprises un problème auprès d'un État et de le porter à l'attention des échelons supérieurs peut servir d'avertissement, tandis que le refus d'accorder des visas à des diplomates peut servir de conséquence.

Les principaux outils d'AMC sont les actions bilatérales réactives. Il peut s'agir de communications avec des gouvernements étrangers par le biais de notes ou de démarches diplomatiques. Les démarches sont des communications officielles d'État à État par voie diplomatique par lesquelles des informations, une demande ou une position sur une question sont transmises.

Les démarches sont hiérarchisées. Un appel téléphonique d'un fonctionnaire de niveau intermédiaire à une mission étrangère a moins de poids qu'un appel du ministre des Affaires étrangères. De plus, un appel téléphonique peut receler moins d'importance qu'une note diplomatique ou qu'une réunion en face à face.

Un autre exemple de communication diplomatique a eu lieu avant les élections de 2019 et de 2021, lorsqu'AMC a envoyé une circulaire rappelant aux missions étrangères leurs devoirs en vertu de la CVRC de respecter les lois et règlements canadiens et de ne pas s'ingérer dans les affaires intérieures du Canada. Les médias ont également rapporté qu'AMC a récemment breffé les diplomates étrangers au sujet de l'ingérence étrangère.

Parmi les autres mesures bilatérales réactives, citons : l'annulation d'une visite, d'un accord ou d'une entente; le retrait d'un événement; le refus de délivrer des visas aux diplomates ou de les prolonger; le refus de créer des postes ou des missions diplomatiques; le rappel de l'ambassadeur du Canada dans un pays; la fermeture de missions étrangères au Canada et de missions du Canada à l'étranger; ainsi que la rupture des relations diplomatiques.

AMC peut également déclarer le personnel diplomatique ou consulaire *persona non grata* (« **PNG** »). Les déclarations de statut de *persona non grata* sont souvent publiques, mais elles peuvent être faites en privé. Un pays n'a pas à donner de raison pour faire une telle déclaration, et cette déclaration n'est pas nécessairement une réponse aux actions de la personne déclarée *persona non grata*.

De plus, AMC peut imposer des sanctions à des entreprises ou à des individus. Jusqu'à présent, AMC n'a pas utilisé de sanctions pour contrer l'ingérence étrangère ciblant les institutions et les processus démocratiques, mais elles sont assez courantes dans d'autres circonstances. Par exemple, le Canada a imposé des sanctions à des oligarques russes en réponse aux campagnes de désinformation russes qu'ils ont parrainées au sujet de la guerre en Ukraine.

Au-delà des mesures bilatérales réactives, les autres outils à la disposition d'AMC sont les suivants :

- **Réponses proactives**. Les exemples incluent les cyberopérations actives et les restrictions à l'exportation.
- **Réponses bilatérales et multilatérales proactives**. Il s'agit de partenariats ou d'échanges d'informations avec d'autres gouvernements de manière bilatérale ou dans le cadre de tables

multilatérales comme le G7 ou le Groupe des cinq (*Fives Eyes*), ou encore de partenariats avec la société civile. Par exemple, le Canada a collaboré avec les Pays-Bas pour élaborer la Déclaration mondiale sur l'intégrité de l'information en ligne, qui compte aujourd'hui 30 signataires.

- **Communications publiques**. Il s'agit d'exposer les positions canadiennes dans les déclarations officielles, les médias sociaux ministériels et les activités de défense des intérêts. On parle ici, par exemple, d'attribuer publiquement des activités à des acteurs étrangers, d'utiliser les médias sociaux pour mettre en lumière les campagnes de mésinformation et de désinformation, de vérifier les faits derrière les discours véhiculés et de proposer des contre-discours.

Les mesures diplomatiques peuvent être utilisées pour communiquer avec d'autres pays ou avec le public, en plus de l'État concerné. Par exemple, une déclaration publique désignant un individu *persona non grata* indique aux autres États que les conséquences sont réelles.

Cependant, David Morrison, le sous-ministre des Affaires étrangères, a fait remarquer que l'essence de la diplomatie est de maintenir les échanges avec les États étrangers, même adversaires, afin de promouvoir les intérêts du Canada. Ainsi, si des mesures publiques, comme déclarer un diplomate *persona non grata* ou imposer des sanctions à un diplomate ou à un pays, peuvent contribuer à dissuader ou à contrer l'ingérence étrangère, elles peuvent aussi entraîner un coût important pour le Canada.

Utilisation des outils diplomatiques d'AMC pour dissuader et contrer l'ingérence étrangère de la RPC

Les relations du Canada avec la République populaire de Chine (la « **RPC** ») illustrent la manière dont AMC utilise les outils diplomatiques pour dissuader et contrer l'ingérence étrangère tout en maintenant des relations avec un État étranger. Les témoins d'AMC ont expliqué que, compte tenu du poids mondial et économique de la RPC, la relation du Canada avec elle est importante pour la sécurité et la prospérité canadiennes. M. Morrison a fait remarquer que le Canada peut soit rester sur la touche et observer, soit s'engager et tenter de moduler le comportement de la RPC dans l'intérêt du Canada. L'engagement diplomatique participe d'une telle modulation.

Actions bilatérales réactives : démarches et autres représentations

J'ai entendu qu'il y a eu une activité diplomatique en réponse à l'ingérence étrangère de la RPC avant le retour de Michael Spavor et de Michael Kovrig (les « **deux Michael** »), bien qu'elle n'ait pas toujours été visible publiquement.

Selon AMC, le Canada s'est défendu et a trouvé des moyens d'augmenter le coût des tentatives d'ingérence étrangère pour la RPC. Le gouvernement a régulièrement fait part à la RPC de ses préoccupations concernant l'ingérence étrangère et a refusé de délivrer des visas à des diplomates de la

RPC. Cependant, jusqu'au retour des deux Michael, la priorité du Canada était de les ramener au pays. Il devait donc se montrer prudent dans ses interactions avec la RPC. Immédiatement après le retour des deux Michael en septembre 2021, l'ingérence étrangère est passée au premier plan de l'ordre du jour d'AMC et le Canada a profité des réunions diplomatiques prévues au calendrier pour soulever la question.

AMC a systématiquement averti la RPC que l'ingérence étrangère était une question centrale pour le Canada et que, si la RPC ne cessait pas, il y aurait des conséquences. Entre décembre 2021 et mars 2023, le Canada a fait 31 représentations à tous les niveaux hiérarchiques, y compris par le premier ministre auprès du président Xi Jinping, au sujet de l'ingérence étrangère de la RPC, de la surveillance et d'autres questions impliquant la sécurité du Canada.

Par exemple, un appel s'est tenue le 17 janvier 2022 entre la sous-ministre des Affaires étrangères de l'époque et son homologue de la RPC. Il s'agissait de la première interaction officielle de haut niveau entre les deux après le retour des deux Michael. La sous-ministre a alors mis les représentants de la RPC en garde en dénonçant les activités d'ingérence étrangère de leur pays. Les témoins d'AMC ont déclaré qu'il était significatif, et probablement surprenant pour la RPC, que le Canada ait fait de l'ingérence étrangère le sujet principal de cette réunion.

Depuis l'automne 2021, le Canada a adressé quatre notes diplomatiques à la RPC, dont deux concernant les postes de police à l'étranger de la RPC (voir le volume 4, chapitre 17**).** Après avoir émis des avertissements par le biais de multiples réunions et notes, la réponse du Canada a évolué vers des actions concrètes, comme le refus de délivrer des visas aux représentants de la RPC et d'approuver une demande de longue date de la RPC visant à créer un nouveau poste au sein de son ambassade au Canada.

De plus, à l'automne et à l'été 2023, les fonctionnaires d'AMC ont fait des démarches auprès de l'ambassadeur de la RPC au sujet de la campagne de désinformation sur WeChat visant le député Michael Chong et d'une campagne de camouflage de pourriels qui a ciblé divers députés (voir le volume 4, chapitre 15). AMC a ensuite émis des déclarations publiques pour dénoncer ces deux campagnes.

Certains pourraient être d'avis que la plupart des mesures diplomatiques ne sont pas suffisantes pour dissuader les activités d'ingérence étrangère, mais il faut garder à l'esprit que prendre des mesures vigoureuses fait généralement en sorte que le pays concerné prend des mesures similaires à l'encontre du Canada.

Déclaration de Zhao Wei comme *persona non grata*

Le 8 mai 2023, le Canada a pris une mesure très publique en réponse à l'ingérence étrangère de la RPC et a déclaré le diplomate de la RPC Zhao Wei *persona non grata*. Le 1er mai 2023, le Globe and Mail avait publié un article sur l'intérêt porté par M. Zhao envers le député Michael Chong et sa famille.

J'ai entendu un certain nombre de témoins sur ce qui a conduit à la déclaration de *persona non grata*.

Les hauts fonctionnaires et le personnel politique d'AMC ont dit que M. Zhao avait été déclaré *persona non grata* dans le cadre d'une série de mesures diplomatiques croissantes prises pour la plupart de manière non publique, afin de condamner et de dissuader la RPC de mener des activités d'ingérence étrangère. J'ai décrit plusieurs de ces efforts plus haut.

Les témoins d'AMC m'ont dit qu'une déclaration de *persona non grata* était déjà envisagée lorsque l'article du Globe and Mail a été publié. M. Morrison a évoqué une réunion interministérielle qui s'est tenue en avril 2023 et au cours de laquelle toutes les options ont été envisagées, y compris l'expulsion d'un diplomate.

Lorsque l'article sur les activités de M. Zhao a été publié, la Direction générale du renseignement d'AMC a cherché à mettre à jour ses connaissances sur les activités des diplomates de la RPC afin de déterminer s'ils se livraient à des activités d'ingérence étrangère.

Le 2 mai 2023, la Direction générale du renseignement d'AMC a produit une évaluation du renseignement sur les activités de M. Zhao. Dans une note de service fondée sur cette évaluation et envoyée le même jour à la ministre des Affaires étrangères, AMC présente une série de réponses possibles que la ministre pourra considérer :

- une démarche
- une démarche assortie d'une demande de départ immédiat de M. Zhao
- une démarche suivie d'une déclaration de *persona non grata*.

Le 3 mai 2023, au cours de l'examen plus large des activités des diplomates de la RPC, AMC a reçu d'autres rapports du SCRS concernant M. Zhao. C'est à ce moment-là que les hauts fonctionnaires d'AMC auraient pris connaissance d'un produit de renseignement du SCRS datant de 2021. Le SCRS avait déjà transmis ce produit de renseignement à AMC en 2021, mais avec une distribution limitée. Selon le directeur général de la Direction générale du renseignement d'AMC, ce rapport ne constituait pas une preuve irréfutable, mais il fournissait des informations supplémentaires sur les activités d'ingérence étrangère de la RPC. Il ne mentionnait rien quant à un lien entre M. Zhao et M. Chong.

Une fois que les hauts fonctionnaires d'AMC ont vu les rapports supplémentaires, y compris le produit du SCRS de 2021, la Direction générale du renseignement d'AMC a préparé une évaluation révisée du renseignement concernant M. Zhao. Les conclusions de l'évaluation révisée étaient différentes de celles de l'évaluation du 2 mai 2023.

La preuve documentaire indique que des fonctionnaires d'AMC ont rencontré le SCRS, le Bureau du Conseil privé, le cabinet du premier ministre et le premier ministre le 6 mai 2023 pour décider s'il y aurait une déclaration de

persona non grata. J'ai entendu que bien que l'approbation du premier ministre ne soit pas nécessaire pour faire une déclaration de *persona non grata*, celui-ci est généralement consulté étant donné la gravité et la rareté relative de ces situations.

Le premier ministre a témoigné qu'une fois que le comportement de M. Zhao au Canada a été rendu public, le Canada devait réagir. Il n'était plus tolérable que M. Zhao occupe un poste diplomatique au Canada. AMC a également conclu qu'avec la publication de l'article, il était devenu moins risqué et moins lourd de conséquences pour le Canada de déclarer M. Zhao *persona non grata*.

La déclaration visait à envoyer un message à la RPC et à d'autres pays sur les conséquences des activités d'ingérence étrangère au Canada et à contribuer au rétablissement de la confiance du public.

Le 4 mai 2023, M. Morrison a convoqué l'ambassadeur de la RPC pour une démarche officielle, en personne, portant sur les préoccupations du Canada en matière d'ingérence étrangère de la RPC. Il a informé les représentants de la RPC que le maintien en poste de M. Zhao au Canada n'était plus tenable. AMC a demandé à la RPC de retirer volontairement M. Zhao, car cela permettait d'éviter l'expulsion d'un diplomate canadien de la RPC en retour. Les représentants de la RPC ont refusé. En fin de compte, la RPC a réagi en expulsant un diplomate canadien de rang comparable à celui de M. Zhao.

Le 8 mai 2023, M. Morrison a signé une note de service à l'intention de la ministre des Affaires étrangères, qui comprenait l'évaluation mise à jour de M. Zhao et recommandait officiellement de le déclarer *persona non grata*. La déclaration officielle a été faite plus tard dans la journée.

Compte tenu du moment de cette déclaration, certains, y compris M. Chong, ont raisonnablement considéré qu'il s'agissait d'une réponse à l'article du Globe and Mail paru le 1er mai 2023. Les témoins d'AMC ont déclaré que, bien que l'article du Globe and Mail ait rendu la position de M. Zhao au Canada intenable, il y avait une divergence entre ce que le journal avait rapporté et ce que le renseignement suggérait.

M. Morrison a déclaré que la communauté du renseignement et de la sécurité nationale au Canada s'accorde à dire que Zhao Wei ne s'est pas livré à des activités d'ingérence étrangère à l'égard de M. Chong. M. Morrison a dit que le fait d'effectuer des recherches et de recueillir des informations ne constitue pas en soi de l'ingérence étrangère. J'aborde le sujet des recherches de la RPC sur les députés au chapitre 14 (volume 4).

Le Mécanisme de réponse rapide du Canada (le MRR du Canada) et la mésinformation et la désinformation

Comme je l'ai expliqué au chapitre 1 (volume 2), en 2018, les membres du G7 se sont entendus pour créer le Mécanisme de réponse rapide (le « **MRR** ») afin de prévenir, déjouer et contrer les menaces malveillantes et évolutives qui pèsent sur les démocraties du G7, en mettant en commun des informations et des analyses, et en déterminant les possibilités de réponses coordonnées.

Le MRR Canada est le secrétariat permanent du MRR du G7. Le MRR Canada surveille les informations en ligne de source ouverte (accessibles au public) et les analyse afin de détecter de potentielles manipulations par des acteurs étrangers. Le MRR Canada se concentre principalement sur les informations internationales en ligne. Toutefois, lors des élections générales et partielles au niveau fédéral, le MRR Canada surveille également l'environnement en ligne domestique pour y détecter d'éventuelles fausses informations ou de la désinformation. À ce titre, le MRR Canada est membre du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (le « **Groupe de travail** ») depuis sa création. Le rôle du Groupe de travail et celui du MRR Canada sont examinés plus en détail au **chapitre 12**.

Le MRR Canada entretient un dialogue permanent avec de nombreuses plateformes de médias sociaux afin de recevoir et de communiquer des informations pertinentes. Ce dialogue n'est pas toujours efficace. Par exemple, le 8 septembre 2023, le MRR Canada a fait un suivi auprès de Tencent, la société mère de WeChat, au sujet de la campagne de désinformation menée contre Michael Chong. Cependant, le MRR Canada ne sait pas si Tencent a pris des mesures sur la base de l'information et n'a pas eu d'autres interactions avec elle.

Le MRR Canada n'effectue pas de surveillance de base de l'environnement en ligne domestique en dehors des périodes électorales. Cependant, s'il apprend quelque chose de ses partenaires internationaux ou s'il découvre un quelconque élément d'intérêt dans le cadre de son travail de surveillance internationale, il en fait part au Groupe de travail.

Cadre de la cyberattribution

Le Canada utilise le Cadre de la cyberattribution, créé en 2019, pour décider s'il faut attribuer publiquement une cyberattaque malveillante dirigée contre des réseaux canadiens ou alliés à un État. AMC dirige le Cadre de la cyberattribution.

Le processus d'attribution commence par une évaluation technique par le CST de la probabilité qu'un cyberincident ait été causé par un acteur étatique. Ensuite, Sécurité publique Canada ou le ministère de la Défense nationale évalue l'incidence de l'attribution publique sur les activités des organismes nationaux. Enfin, AMC procède à une évaluation juridique afin de déterminer si l'activité a enfreint le droit international ou les normes des Nations Unies en matière de comportement acceptable dans le cyberespace.

AMC procède ensuite à une évaluation des risques en matière de politique étrangère, puisque l'attribution publique consiste en fait à « pointer du doigt » un État pour son comportement aux yeux du monde. Enfin, AMC adresse une recommandation au ministre des Affaires étrangères concernant l'attribution publique ou d'autres actions. La décision d'aller de l'avant appartient au ministre des Affaires étrangères.

Jusqu'à présent, il n'y a pas eu d'attribution publique concernant la cyberingérence étrangère dans les institutions démocratiques.

J'ai entendu des témoignages concernant deux cyberincidents, pas nécessairement liés à de l'ingérence étrangère dans les institutions démocratiques, pour lesquels il a finalement été décidé de ne pas procéder à une attribution publique. Dans un cas, les données étaient insuffisantes pour attribuer l'événement à un acteur étatique étranger. Dans l'autre cas, la décision a été prise pour des raisons tactiques.

La Gendarmerie royale du Canada (GRC)

La GRC détecte, dissuade et contrecarre l'ingérence étrangère en appliquant un certain nombre de lois, notamment : (1) la *Loi sur l'ingérence étrangère et la protection de l'information* (la « ***LIEPI*** »; anciennement la *Loi sur la protection de l'information*); (2) le *Code criminel*; et (3) la *Loi électorale du Canada*. La *LIEPI* et le *Code criminel* ont été modifiés par la *Loi sur la lutte contre l'ingérence étrangère* en juillet 2024 et comprennent désormais davantage d'infractions visant l'ingérence étrangère[6].

Les services de la Police fédérale de la GRC s'occupent des menaces criminelles les plus graves et les plus complexes pour la sécurité de la population canadienne et les intérêts canadiens, y compris les menaces ciblant les institutions démocratiques, l'intégrité économique, les infrastructures physiques et cybernétiques et l'ingérence étrangère[7]. Cinq secteurs de programme ont des rôles de gouvernance et de surveillance liés à l'ingérence étrangère : la Sécurité nationale de la Police fédérale (la « **SNPF** »), les Services de protection de la Police fédérale, le Renseignement national de la Police fédérale, les Opérations criminelles de la Police fédérale et la Gestion stratégique de la Police fédérale.

En 2018, la GRC a créé temporairement une équipe au sein de la SNPF dédiée à la lutte contre l'ingérence d'acteurs étrangers. Composée de sept membres, cette équipe est axée sur l'ingérence étrangère. L'équipe est devenue permanente en 2020 et dispose d'un financement propre depuis 2023. Elle forme et guide les unités d'enquête sur l'ingérence étrangère.

Pour l'instant, aucune formation particulière sur l'ingérence d'acteurs étrangers ne fait partie du programme d'études offert à la Division Dépôt. Les témoins de la GRC m'ont dit que ce programme est axé sur la préparation des recrues aux services de police de première ligne. Pour sa part, la formation donnée dans le cadre du cours d'enquêteur sur la sécurité nationale comprend un volet sur l'ingérence étrangère, et la GRC s'affaire à développer un cours avancé d'enquêteur criminel en matière de sécurité nationale ainsi

---

6 La *Loi sur la lutte contre l'ingérence étrangère*, présentée en tant que projet de loi C-70, est examinée en détail au chapitre 14.

7 La GRC utilise l'expression « ingérence d'acteurs étrangers » pour parler de l'ingérence étrangère.

qu'une formation plus spécialisée sur l'ingérence étrangère. Historiquement, les ressources allouées au programme de police fédérale de la GRC ont toujours été réacheminées pour financer d'autres priorités organisationnelles (comme la police contractuelle et les services de police autochtones). Il est toutefois de plus en plus reconnu qu'une expertise en matière d'ingérence étrangère et l'allocation de ressources dédiées à l'ingérence étrangère sont nécessaires.

Outils d'intervention

Enquêtes criminelles

La responsabilité première des enquêtes sur l'ingérence étrangère incombe à la SNPF. Les enquêtes sont menées par les Équipes intégrées de la sécurité nationale (les « **EISN** ») et les Sections de la sécurité nationale (les « **SSN** ») dans les divisions de la GRC à travers le Canada. Les SSN sont composées uniquement d'agents de la GRC, tandis que les EISN rassemblent des personnes des niveaux fédéral, provincial et municipal, issues des services de police et de la communauté de la sécurité nationale et du renseignement.

Les EISN travaillent en collaboration avec les services de police locaux. Les EISN et les SSN sont toutes deux dirigées par le quartier général de la GRC.

L'extraterritorialité pose un défi à la GRC en matière d'enquête. Cependant, la GRC dispose d'agents occupant des postes d'analyse et de liaison à l'étranger, ainsi que de partenariats internationaux (par exemple, avec Interpol) qui facilitent la coopération interorganismes dans les enquêtes internationales.

Les enquêtes criminelles portant sur certaines institutions publiques ou certaines personnes, comme des politiciens, doivent être approuvées au préalable par le commissaire adjoint du SNPF par le biais d'une demande concernant un secteur sensible. En effet, ce type d'enquête peut avoir une incidence négative sur une institution fondamentale de la société canadienne. En plus de la politique, les autres secteurs sensibles comprennent les institutions religieuses, les médias, le monde universitaire et les syndicats.

À ma demande, la GRC a examiné ses dossiers d'enquête depuis 2018 pour y recenser les activités portant sur l'ingérence étrangère. Elle a ainsi relevé plus de 100 enquêtes sur des activités d'ingérence étrangère dans divers domaines : intégrité économique, infrastructures essentielles, prolifération, répression transnationale, vol de propriété intellectuelle et d'informations protégées, désinformation et institutions démocratiques. Sur ce volume d'enquêtes, la GRC n'a identifié que six enquêtes portant sur des cas d'ingérence étrangère possible visant les processus démocratiques du Canada. Cinq d'entre elles ont été fermées parce que la GRC a conclu que les allégations n'étaient pas fondées. L'une d'entre elles est en cours.

Je note ici que la capacité de la GRC à enquêter se limite aux activités susceptibles de constituer une infraction ou, en d'autres termes, aux activités illégales. À ce titre, les nouvelles infractions pénales introduites par la *Loi sur la lutte contre l'ingérence étrangère* pouvant aider la GRC à enquêter sur les activités menaçantes d'ingérence étrangère.

Perturbation

Comme nous l'avons vu au chapitre 4 (volume 2), il existe des défis importants associés au fait d'entreprendre des poursuites pour des infractions liées à l'ingérence étrangère lorsqu'elles s'appuient sur du renseignement. C'est l'une des raisons pour lesquelles la GRC reconnaît que les poursuites ne sont plus nécessairement la référence absolue en matière d'atténuation des menaces.

Le sous-commissaire de la GRC, Mark Flynn, a déclaré que, lorsque les poursuites ne sont pas possibles ou ne constituent pas une utilisation efficace des ressources, la GRC doit chercher d'autres possibilités pour réduire la menace à la sécurité publique et les mettre en œuvre avec la même vigueur. Des mesures de perturbation, comme les sanctions réglementaires, l'intervention financière, l'interdiction de territoire aux immigrants et les services de police communautaire peuvent être utilisées dans le contexte de l'ingérence étrangère. La GRC a pour but de perturber et de démanteler les acteurs menaçants, et de les tenir responsables.

La réponse de la GRC aux postes de police étrangers de la République populaire de Chine est un exemple de perturbation. La GRC a envoyé des agents en uniforme dans les quartiers où se trouvaient des postes soupçonnés. L'objectif était de :

- mettre en lumière le problème pour faciliter les enquêtes
- montrer aux communautés concernées que la GRC prenait le problème au sérieux
- instaurer un climat de confiance avec les membres de la communauté.

Auparavant, la GRC aurait adopté une approche plus discrète avec une enquête moins visible. Les postes de police étrangers et l'intervention du gouvernement, y compris les différents points de vue sur la réponse de la GRC, sont examinés plus en détail au chapitre 17 (volume 4).

Sensibilisation du public et des parties prenantes

Un autre moyen pour la GRC de contrer l'ingérence étrangère est d'intervenir auprès du public et des parties prenantes au sein de la communauté pour renforcer la résilience. Les activités de sensibilisation de la GRC sont examinées plus en détail au chapitre 16 (volume 4).

Sécurité publique Canada

Sécurité publique Canada se penche sur les questions de sécurité nationale et conseille le ministre de la Sécurité publique à ce sujet. Le ministre est responsable de cinq organismes au sein de son portefeuille : la GRC, le SCRS, l'Agence des services frontaliers du Canada, le Service correctionnel du Canada et la Commission des libérations conditionnelles du Canada. Parmi ces organismes, le SCRS et la GRC sont ceux qui participent le plus directement à contrer l'ingérence étrangère. Comme je l'ai expliqué au chapitre 8 (volume 2), ces organismes relèvent directement du ministre de la Sécurité publique, mais pas du sous-ministre.

Élaboration et coordination des politiques

La fonction principale de Sécurité publique Canada est de coordonner les activités des organismes placés sous la responsabilité du ministre en élaborant des politiques. Elle conçoit des politiques visant à combler les lacunes dans la capacité du gouvernement à contrer les menaces et conseille le gouvernement sur la sécurité nationale, la sécurité communautaire et la justice pénale, ainsi que sur les questions de gestion des situations d'urgence.

Sécurité publique Canada n'est pas directement responsable des réponses opérationnelles au renseignement et ne dirige pas les réponses aux menaces immédiates. Plutôt, le ministère compile les informations et organise des discussions qui permettent au gouvernement d'interpréter les informations. Il contribue ainsi aux décisions concernant la réponse que le gouvernement donne.

Sécurité publique Canada est un consommateur de renseignement, pour qui le renseignement est contextuel et lui permet d'améliorer sa compréhension des défis opérationnels, ce qui soutient son travail d'élaboration de politiques. Lorsque les hauts fonctionnaires de Sécurité publique Canada assistent aux breffages du SCRS et de la GRC, l'un de leurs principaux rôles est de fournir le contexte actuel à l'organisme qui organise le breffage.

Le sous-ministre de la Sécurité publique, les sous-ministres adjoints et les directeurs généraux font partie (et, jusqu'à récemment, les présidaient ou coprésidaient) de plusieurs comités interministériels qui examinent les menaces à la sécurité du Canada. J'aborde la structure de gouvernance actuelle des comités interministériels plus loin dans ce chapitre.

En mars 2023, le gouvernement a nommé un coordonnateur national de la lutte contre l'ingérence étrangère (le « **CNLIE** ») au sein de Sécurité publique Canada. J'aborde son rôle plus loin dans le cadre de la coordination et de la gouvernance de la sécurité nationale.

Le Bureau du Conseil privé (BCP)

Le BCP coordonne le soutien offert par la fonction publique au premier ministre et au Cabinet. Il rend compte directement au premier ministre. Le BCP a des fonctions de convocation et d'analyse critique, et joue un rôle clé dans la coordination de la communauté de la sécurité nationale et du renseignement en ce qui concerne à la fois les politiques et les activités.

La fonction de convocation du BCP signifie qu'il est responsable de réunir la communauté gouvernementale de la sécurité et du renseignement afin d'assurer une coordination interministérielle et une compréhension des menaces et des réponses. Cela s'applique tant à l'élaboration des politiques qu'aux activités. Cette réunion de la communauté est essentielle, car il est rare qu'une question ou une politique proposée relève étroitement du mandat d'un seul ministre ou d'un seul ministère.

Le BCP a également la fonction d'analyse critique. Cela signifie qu'il pose des questions, offre des conseils et donne des orientations à d'autres ministères ou organismes en se basant sur une perspective large et pangouvernementale. Étant donné que le BCP n'a pas les mêmes obligations de reddition de comptes que les ministères ou les organismes qui relèvent directement des ministres, il peut offrir une vue d'ensemble.

Le BCP ne conçoit ni n'élabore de politique lui-même. Plutôt, il travaille sur des initiatives de politiques avec les ministères responsables afin que tous les ministères dont le travail est concerné par une question soient consultés avant que l'initiative ne soit soumise au Cabinet. Une partie de son rôle consiste à signaler aux ministres les points de tension et les priorités concurrentes afin de leur donner l'occasion de débattre, de discuter et de sous-peser les différentes considérations lors de la prise de décision.

Le BCP préside ou copréside de nombreux comités de gouvernance interministériels, notamment des comités qui coordonnent les réponses opérationnelles aux menaces à la sécurité nationale. J'aborde ces comités et la structure de gouvernance de la sécurité nationale plus en détail ci-dessous.

Le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) et les secrétariats associés

La branche du BCP la plus directement impliquée dans les questions de sécurité nationale est le bureau du conseiller à la sécurité nationale et au renseignement auprès du premier ministre (le « **CSNR** »).

Le CSNR fournit au premier ministre et au Cabinet des évaluations stratégiques, des conseils stratégiques et des conseils opérationnels en matière de sécurité nationale, de renseignement, de politique étrangère et de défense. Le CSNR agit comme coordonnateur au sein de la communauté de la sécurité nationale et du renseignement, et peut réunir les ministères et les sous-ministres pour examiner des questions particulières, réagir à des événements d'actualité et gérer des crises. Comme je l'explique au

chapitre 17 (volume 4), le CSNR est également responsable de la circulation du renseignement au sein du BCP et à l'intention du premier ministre.

Le CSNR relève directement du greffier du Conseil privé, qui est le sous-ministre du premier ministre, le secrétaire du Cabinet et le chef de la fonction publique fédérale. Le CSNR est secondé par un adjoint, poste créé en 2023 en raison de l'augmentation constante de la charge de travail et des déplacements du CSNR.

Le CSNR supervise un certain nombre de secrétariats, dont quatre sont concernés par l'ingérence étrangère.

Le **Secrétariat de la sécurité et du renseignement** (le « **SSR du BCP** ») conseille et soutient le CSNR au niveau stratégique sur les questions de sécurité nationale et de renseignement, notamment en coordonnant les réponses opérationnelles aux problèmes de sécurité nationale.

Par l'intermédiaire de son Unité de politique stratégique et planification, le SSR du BCP coordonne le développement des politiques de sécurité nationale et fournit des conseils en la matière. Il remplit la fonction d'analyse critique pour le BCP, en veillant à ce que les propositions ministérielles répondent aux besoins du Cabinet et soient cohérentes avec les orientations stratégiques générales du gouvernement. La fonction d'analyse critique s'exerce à tous les niveaux, des analystes aux plus hauts responsables.

Par l'intermédiaire de son unité opérationnelle, le SSR du BCP coordonne et donne des conseils sur les activités, les événements et les questions de sécurité et de renseignement. Pour ce faire, entre autres, il préside, copréside ou assure le secrétariat de comités interministériels clés dont le mandat comprend la coordination des réponses opérationnelles aux menaces à la sécurité nationale.

Le SSR est également chargé de coordonner l'élaboration des priorités du Cabinet en matière de renseignement.

Le **Secrétariat de l'Évaluation du renseignement** (le « **SER du BCP** ») produit des analyses et des évaluations stratégiques du renseignement concernant les tendances et les développements étrangers qui ont une incidence sur les intérêts canadiens. Le travail du SER du BCP est pertinent et neutre sur le plan des politiques, ce qui signifie que les évaluations du renseignement reflètent les besoins du gouvernement en matière de renseignement, mais ne sont pas influencées par les résultats souhaités sur le plan stratégique ou opérationnel. L'analyse s'appuie sur n'importe quelle source, y compris le renseignement classifié, les rapports diplomatiques et les sources ouvertes. Ces dernières années, le SER du BCP a commencé à intégrer le renseignement étranger et national dans ses évaluations.

Le **Secrétariat du Conseil de la sécurité nationale** soutient le CSNR en sa qualité de secrétaire du Conseil de la sécurité nationale, ce que j'aborde ci-dessous.

Le **Secrétariat de la politique étrangère et de la défense** suit, coordonne et conseille les hauts fonctionnaires du BCP et le premier ministre sur les questions de politique étrangère et de défense.

Renseignement de source ouverte (RSO)

Comme je l'explique au chapitre 7 (volume 2), le renseignement de source ouverte (le « **RSO** ») contient des informations accessibles au public qui, par le biais de la collecte et de l'analyse, peuvent être utilisées à des fins de renseignement. Plusieurs ministères disposent de capacités de RSO et les utilisent pour conseiller leurs ministres et sous-ministres. Cependant, il n'existe pas de secrétariat de l'évaluation du RSO national comme c'est le cas pour le renseignement étranger.

J'ai entendu dire que le gouvernement tente de déterminer si un changement sur le plan des politiques ou de la législation pourrait s'avérer nécessaire pour combler les lacunes dans la cohésion des activités de RSO menées au sein du gouvernement. Une possibilité serait de confier ce travail à Sécurité publique Canada, étant donné que le ministère est un acteur clé dans la réponse à l'ingérence étrangère. En effet, il compile déjà des informations et organise des discussions permettant au gouvernement d'interpréter les informations. Il contribue ainsi aux décisions sur la réponse du gouvernement.

Le RSO est considéré comme un outil de plus en plus précieux. Il occupe une place de plus en plus importante dans les considérations du gouvernement lorsqu'il s'agit de prendre des décisions en matière de sécurité nationale. Selon l'ancienne CSNR Jody Thomas, le RSO est essentiel pour comprendre la cohésion sociétale, l'incidence sur les processus démocratiques et la confiance du public envers les institutions, en particulier en ce qui concerne les médias sociaux.

Martin Green, un ancien secrétaire adjoint du Secrétariat de l'évaluation du renseignement du Bureau du Conseil privé (BCP), a fait remarquer que l'utilisation plus large du RSO représente un grand sujet de discussion au sein du Groupe des cinq (« *Five Eyes* »). Il a affirmé que le RSO pourrait être particulièrement utile au Canada, car les plus grands producteurs d'informations secrètes sont généralement d'autres pays, et non le Canada. Le RSO offre la possibilité de « canadianiser » notre renseignement, d'être moins dépendants de nos alliés et de rendre le renseignement plus facile à utiliser et à partager avec d'autres paliers de gouvernement.

L'extraction des données de source ouverte pose plusieurs enjeux, notamment des questions de définition et des enjeux juridiques, en particulier en ce qui concerne la protection de la vie privée. M. Green a fait remarquer que les Canadiennes et les Canadiens pourraient s'opposer à ce que le gouvernement recueille leurs données accessibles en ligne.

Toutefois, si quelque chose de terrible devait se produire (par exemple, si les manifestations du « Convoi pour la liberté » en 2022 avaient donné lieu à de graves violences), les Canadiennes et les Canadiens pourraient se demander

pourquoi le gouvernement ne surveillait pas les médias sociaux pour y déceler des signes avant-coureurs.

Selon M. Green, si nous abordons le RSO de la bonne manière, il pourrait donner aux décideurs de haut rang des outils pour communiquer avec le public et accroître la confiance de ce dernier envers le gouvernement.

11.4 Coordination et gouvernance en matière de sécurité nationale

La coordination de la communauté de la sécurité nationale, et de sa réponse à l'ingérence étrangère, représente un défi. Cette section décrit les structures mises en place par le gouvernement pour relever ce défi.

Le rôle des comités interministériels

Les comités interministériels, composés de hauts fonctionnaires, sont un instrument essentiel pour l'échange d'informations, la discussion sur les politiques et la coordination des réponses au sein du gouvernement. Étant donné que les questions concernent généralement plus d'un organisme ou d'un ministère, les comités interministériels sont des mécanismes indispensables de coordination horizontale pour les politiques, les opérations et l'évaluation du renseignement en matière de sécurité nationale. Ils jouent un rôle clé dans la manière dont les différents ministères et organismes concernés par la sécurité nationale communiquent entre eux, se tiennent mutuellement informés des problèmes et décident des mesures à prendre.

La composition, les domaines d'intérêt, la fréquence des réunions et le niveau de responsabilité des comités varient. Les comités au niveau des sous-ministres ont souvent leur équivalent au niveau des sous-ministres adjoints et des directeurs généraux, de sorte que les informations importantes sont relayées verticalement jusqu'aux niveaux les plus élevés de la fonction publique. Des comités ou groupes similaires existent également de manière moins formelle au niveau opérationnel.

Le nombre, le mandat et la composition des comités changent et évoluent au fil du temps. Le BCP a récemment mené un processus de rationalisation de la structure des comités interministériels, qui était devenue lourde et quelque peu redondante. En effet, les comités n'étaient pas formellement dissous lorsqu'ils devenaient inactifs avec le temps. L'objectif de la restructuration était d'améliorer la façon dont l'information circule et d'accroître l'efficience et l'efficacité globales. J'ajouterais que, de mon point de vue, il est essentiel d'éviter de multiplier inutilement les comités. Bien qu'ils soient à la fois utiles et nécessaires, ils

peuvent, comme la preuve l'a démontré, donner lieu à de longues discussions en vue de dégager un consensus, mais mener à peu d'actions.

Cet effort a commencé à l'automne 2023 et se poursuivait quand les audiences publiques de la Commission ont pris fin.

Ci-dessous, je décris d'abord les comités de l'ancienne structure les plus pertinents en matière d'ingérence étrangère, puis la structure révisée. Les comités qui s'occupent spécifiquement de la sécurité des élections ne sont pas inclus ici, car ils sont examinés au chapitre 16 (volume 4). Les comités suivis d'un astérisque (*) continuent d'exister sous la nouvelle structure de gouvernance. Dans la première section, je décris la manière dont ils fonctionnaient auparavant et, dans la seconde section, la manière dont ils fonctionnent actuellement.

Comité des sous-ministres sur la coordination opérationnelle (CSMCO)

Le Comité des sous-ministres sur la coordination opérationnelle (le « **CSMCO** ») était une assemblée informelle de sous-ministres présidée par le CSNR, qui se réunissait chaque semaine pour discuter d'une variété de questions opérationnelles. Les sous-ministres échangeaient du renseignement sur les incidents afin d'assurer une approche coordonnée des questions jugées importantes par le CSNR. Le CSMCO comptait un grand nombre de membres, au-delà des membres traditionnels de la communauté de la sécurité nationale et du renseignement : par exemple, il comprenait des représentants de Transports Canada, de la Garde côtière, ainsi que d'Immigration, Réfugiés et Citoyenneté Canada.

En appui au CSMCO, on retrouvait le Comité des sous-ministres adjoints sur les opérations de sécurité nationale (le « **CSMAOSN** »). Il était chargé de veiller à ce que la communauté de la sécurité et du renseignement ait une bonne connaissance de la situation en ce qui concerne les questions opérationnelles clés. Il facilitait également la coordination stratégique au sein du gouvernement en réponse aux événements de sécurité nationale ou aux situations d'urgence.

Comité des sous-ministres sur la gestion de l'intervention du renseignement (CSMGIR)

Le Comité des sous-ministres sur la gestion de l'intervention du renseignement (le « **CSMGIR** »), également présidé par le CSNR, a évolué à partir du CSMCO, en tant que forum pour un nombre plus restreint de sous-ministres (CST, SCRS, AMC, Sécurité publique Canada, GRC et Secrétariats de la politique étrangère et de la défense, de la protection civile, des institutions démocratiques et de l'appareil gouvernemental du BCP) afin de discuter d'informations particulièrement sensibles et/ou de rapports de renseignement.

Le CSMGIR avait pour mandat de déterminer et d'examiner le renseignement pertinent et exploitable, notamment sur les risques d'ingérence étrangère, et de décider comment y répondre par une action coordonnée sur le plan opérationnel, de l'application de la loi ou des politiques. Il examinait le renseignement opérationnel et tactique portant sur des questions précises, urgentes et à court terme nécessitant une réponse. Par exemple, le CSMGIR a été le principal forum par lequel le gouvernement a coordonné sa réponse à des incidents telle la campagne de désinformation sur WeChat qui a ciblé Michael Chong à l'été 2023, et à la campagne de camouflage de pourriels qui a ciblé des députés à l'automne 2023.

Le CSMGIR était soutenu par un sous-comité du CSMAOSN, appelé « CSMAOSN tactique », qui formulait des recommandations sur le renseignement qui devrait être discuté au CSMGIR, conseillait les sous-ministres sur les options pour réagir au renseignement et servait d'organe de coordination pour assurer le suivi des actions du CSMGIR.

De nombreux témoins ont souligné l'importance du CSMGIR. L'ancien directeur du SCRS, David Vigneault, a déclaré qu'il était devenu l'un des principaux moyens de déterminer que le renseignement était utile au travail des sous-ministres et d'en discuter de manière organisée.

Comité des sous-ministres sur le renseignement (CSMR)

Le rôle du Comité des sous-ministres sur le renseignement (le « **CSMR** »), également présidé par le CSNR, était d'examiner les évaluations du renseignement à plus long terme, de nature stratégique et orientées vers l'avenir. Il était soutenu par le Comité d'évaluation du renseignement des sous-ministres adjoints, qui examinait les produits d'évaluation du renseignement en provenance du Secrétariat de l'Évaluation du renseignement (SER du BCP) et d'autres sources.

Comité des sous-ministres sur la sécurité nationale (CSMSN)*

Le Comité des sous-ministres sur la sécurité nationale (le « **CSMSN** »), coprésidé par le CSNR et le sous-ministre de la Sécurité publique, examinait les questions et les priorités en matière de sécurité, de défense et de politique étrangère, ainsi que les liens existant entre elles. Il s'agissait d'un comité clé pour l'élaboration de la politique de sécurité nationale, qui coordonnait la réponse du gouvernement aux questions actuelles et émergentes. Ses principaux membres étaient les Forces armées canadiennes, l'Agence des services frontaliers du Canada, le SCRS, le CST, le ministère de la Justice, Innovation, Sciences et Développement économique Canada, le Secrétariat du Conseil du Trésor, le ministère de la Défense nationale, le BCP, Sécurité publique Canada et la GRC.

Le CSMSN était soutenu par le Comité des sous-ministres adjoints sur les politiques de la sécurité nationale (le « **CSMAPSN** ») et le Comité des sous-ministres adjoints sur le renseignement (le « **CSMAR** »). Sécurité publique

Canada et le BCP coprésidaient le CSMAPSN, qui était un forum de niveau stratégique permettant aux hauts responsables de la communauté de la sécurité nationale et du renseignement de se réunir pour élaborer et mettre en œuvre des politiques liées à la sécurité nationale. Le CSMAR était quant à lui chargé de la mise en œuvre, de la gestion et de la supervision des priorités et des besoins du gouvernement en matière de renseignement. Cela comprenait des discussions sur les besoins en renseignement du gouvernement, les lacunes opérationnelles et la coordination.

Comité des sous-ministres sur la cybersécurité (CSMC)

Le Comité des sous-ministres sur la cybersécurité (le « **CSMC** »), coprésidé par Sécurité publique Canada et le CST, a élaboré et dirigé les politiques et les opérations du Canada en matière de cybersécurité. Il était soutenu par le Comité des sous-ministres adjoints sur la cybersécurité.

Autres comités de sous-ministres

Il existait également des comités responsables de pays spécifiques, comme le Comité des sous-ministres sur la Chine. Présidé par AMC, ce comité se réunissait pour discuter de l'approche stratégique du Canada vis-à-vis de la Chine, y compris des questions de politique étrangère et, parfois, d'ingérence étrangère. Ce comité était soutenu par le Comité des sous-ministres adjoints sur la Chine.

La structure de gouvernance révisée

Comme je l'ai mentionné ci-dessus, le gouvernement a révisé cette structure de comités interministériels durant le mandat de la Commission. La Commission a demandé et reçu une mise à jour sur l'état de cette restructuration avant de finaliser ce rapport.

Ma compréhension est que la structure de gouvernance compte désormais cinq comités des sous-ministres au lieu, d'approximativement, une douzaine. Les nouveaux comités sont les suivants :

- Comité des sous-ministres sur la coordination opérationnelle (le « **CSCO** »)
- Comité des sous-ministres de l'action en matière de renseignement (le « **CSMAR** »)
- Comité des sous-ministres de la sécurité nationale, de la cyber et du renseignement (le « **CSSN** »)
- Comité de protection des sous-ministres (le « **CSP** »)
- Comité des sous-ministres sur la prospérité économique et la sécurité[8].

[8] Au moment de rédiger ce rapport, le nom officiel de ce comité, et sa traduction, n'étaient pas déterminés. Son nom provisoire en anglais était « Deputy Minister Committee on Economic Prosperity and Security, ou « DMES ».

Le BCP préside tous les comités, le CSNR assumant ce rôle pour trois d'entre eux (le CSCO, le CSMAR et le CSSN). Le gouvernement estime que cette nouvelle structure améliorera la centralisation et l'efficacité des comités. La composition de chaque comité diffère légèrement, mais les principaux organismes et ministères chargés de la sécurité nationale sont généralement représentés. Tous les comités invitent d'autres sous-ministres sur une base ponctuelle.

Le **CSCO** continue de superviser la gestion des incidents et des problèmes de sécurité nationale et coordonne les activités et les opérations de sécurité et de renseignement. Il constitue également un forum pour les mises à jour et les discussions opérationnelles. Alors que le CSMAR est conçu pour utiliser le renseignement de manière proactive, le CSCO se concentre de manière réactive sur les dossiers opérationnels les plus urgents et les plus sensibles au facteur temps. Les réunions se déroulent généralement au niveau « Très secret »[9].

Le **CSMAR** remplace le CSMGIR et c'est là que sont discutés les informations particulièrement sensibles et les rapports de renseignement. Le CSMAR oriente ensuite les réponses et conseille le gouvernement. Le Comité a pour but de permettre l'utilisation de renseignement contextualisé, d'éviter les surprises sur le plan stratégique et d'améliorer la coordination et l'efficacité de la communauté du renseignement. Le CSMAR a pour but de prendre des mesures sur la base du renseignement. Tant les producteurs que les principaux consommateurs de renseignement y participent[10]. Les réunions se déroulent généralement au niveau « Très secret ».

Le **CSSN** supervise et coordonne l'élaboration et la mise en œuvre des politiques de sécurité nationale et de renseignement. Il fournit également des conseils et des orientations stratégiques sur les questions de sécurité nationale et de renseignement à moyen et à long terme. Lorsque cela est pertinent, il examine les recommandations ou les produits en lien avec ces questions qui sont destinés au Cabinet. Le CSSN est responsable de l'orientation générale de la communauté de la sécurité et du renseignement sur le plan des politiques et de la stratégie. Les réunions se déroulent généralement au niveau « Secret »[11] .

Le **CSP** supervise la protection et la sécurité des ministres, des autres fonctionnaires et des dignitaires étrangers en visite. Alors que la sécurité générale des événements relève du ministère ou de l'organisme responsable de chaque événement, le CSP est chargé de la protection des personnes dans

---

9 Les membres du CSCO sont : le conseiller en matière de politique étrangère et de défense du BCP, Sécurité publique Canada, le sous-secrétaire du Cabinet (Enquête publique sur l'ingérence étrangère) du BCP, le CST, le SCRS, Transports Canada, la GRC, le ministère de la Défense nationale et les Forces armées canadiennes, AMC, Immigration, Réfugiés et Citoyenneté Canada et l'Agence des services frontaliers du Canada.

10 Les membres du CSMAR sont : Sécurité publique Canada, AMC, le ministère de la Défense nationale et les Forces armées canadiennes, le CST, le SCRS, la GRC et le sous-secrétaire du Cabinet (Gouvernance) du BCP.

11 Les membres du CSSN sont : Sécurité publique Canada, AMC, le ministère de la Défense nationale et les Forces armées canadiennes, le ministère de la Justice, le CST, le SCRS, la GRC et l'Agence des services frontaliers du Canada.

le cadre de son mandat. Par exemple, le CSP est chargé de faire des recommandations au ministre de la Sécurité publique sur les personnes qui devraient bénéficier d'une protection sur la base de l'analyse des menaces, et il conseille la GRC sur le niveau de protection qui devrait être offert. Les réunions se déroulent généralement au niveau « Secret »[12] .

Au moment d'écrire ce rapport, le mandat du Comité des sous-ministres sur la prospérité économique et la sécurité était en cours d'élaboration. Ma compréhension est que son mandat vise à soutenir la coordination des approches qui protègent l'économie et les secteurs critiques du Canada. Il ne s'agit pas d'un comité décisionnel. Le gouvernement s'attend à ce que ce comité soit coprésidé par AMC et le CSNR[13].

L'évolution du rôle de conseiller à la sécurité nationale et au renseignement (CSNR)

Le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (CSNR) réunit la communauté de la sécurité nationale et du renseignement et travaille avec d'autres ministères. Le CSNR a la capacité et l'autorité de convoquer les ministères et les sous-ministres pour examiner des questions particulières, répondre aux événements courants et gérer les crises. D'autres ministères peuvent réunir des sous-ministres ou des sous-ministres adjoints à différents moments, mais le pouvoir de convocation du BCP, dont fait partie le CSNR, est plus étendu et plus marqué.

Au cours de la dernière année, d'autres mesures ont été mises en place pour renforcer le rôle de CSNR dans la coordination de la communauté de la sécurité nationale et du renseignement.

Tout d'abord, le premier ministre a ajouté au titre de CSNR celui, plus élevé, de sous-greffier. L'actuel greffier, John Hannaford, a expliqué que cette mesure souligne l'importance de la fonction et renforce l'influence du CSNR au sein de la communauté des sous-ministres.

Deuxièmement, le CSNR est désormais secrétaire du Conseil de la sécurité nationale, un comité du Cabinet créé en septembre 2023 que j'aborde plus en détail ci-dessous. Cela renforce le rôle du CSNR en tant que point d'intégration du gouvernement sur les questions de sécurité nationale et lui donne un levier pour convoquer des personnes et contrôler les travaux du Conseil.

---

[12] Les membres principaux du CSP sont : Sécurité publique Canada, le Secrétariat du Conseil du Trésor du Canada, Patrimoine canadien et le BCP. Les membres auxiliaires sont : la GRC, le SCRS, le CST, le sergent d'armes, le Service des poursuites pénales du Canada et le Centre intégré d'évaluation du terrorisme.

[13] Les membres du Comité des sous-ministres sur la prospérité économique et la sécurité sont : le ministère des Finances, Innovation, Sciences et Développement économique Canada, AMC, Sécurité publique Canada, Ressources naturelles Canada, le SCRS, le CST, Transports Canada, l'Agence des services frontaliers du Canada, le chef de mission à Washington, DC et la GRC. D'autres sous-ministres, dont ceux de Patrimoine canadien, du Secrétariat du Conseil du Trésor du Canada et de RCAANC, sont invités aux réunions du CSMPES.

Troisièmement, le premier ministre a envoyé pour la première fois une lettre de mandat au CSNR, laquelle a été publiée par le BCP le 25 novembre 2024. Cette lettre reflète les responsabilités actuelles du CSNR, notamment pour la transmission du renseignement et des analyses au premier ministre, son rôle de coordination des décisions de sécurité nationale – y compris le renforcement de la sensibilisation des ministres, ainsi que son rôle dans la coordination des réponses opérationnelles aux incidents majeurs. Enfin, le CSNR soutient également le Conseil de la sécurité nationale et la mise en œuvre de ses décisions. La publication d'une lettre de mandat au CSNR me semble être une bonne initiative. Cela devrait devenir une pratique courante.

La lettre de mandat définit également plusieurs priorités précises pour le CSNR, qui s'inspirent des rapports du rapporteur spécial indépendant sur l'ingérence étrangère, de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et du Comité des parlementaires sur la sécurité nationale et le renseignement, ainsi que des travaux de cette commission. La lettre de mandat aborde :

- **La Stratégie de sécurité nationale**. Le CSNR doit produire une stratégie de sécurité nationale renouvelée en 2025, avec un cadre intégré pour la position du Canada sur le plan de la sécurité nationale, de la défense et de la diplomatie. Cette stratégie sera élaborée avec le Conseil de la sécurité nationale.
- **Collaboration internationale**. Le CSNR doit travailler avec des partenaires internationaux sur la sécurité nationale, la politique étrangère et la politique de défense et explorer le potentiel de nouveaux partenariats bilatéraux et multilatéraux pour promouvoir les intérêts et la sécurité du Canada.
- **Les priorités en matière de renseignement**. Conformément à une vision renouvelée de la sécurité nationale, le CSNR doit actualiser sur une base annuelle les priorités du Canada en matière de renseignement, en veillant à ce qu'elles soient conformes à l'orientation stratégique définie par le Conseil de la sécurité nationale et à ce qu'elles soient communiquées au public.
- **L'évaluation du renseignement**. Le CSNR doit moderniser le processus d'évaluation du renseignement et systématiser la circulation de l'information dans l'ensemble du gouvernement.
- **La communication et le dialogue**. Le CSNR doit améliorer le dialogue avec les parties prenantes, notamment les parlementaires, les communautés issues des diasporas et les autres ordres de gouvernement en matière de sécurité nationale afin de les sensibiliser, de détecter et de contrer les menaces, tout en éclairant la définition des priorités.
- **La préparation aux situations d'urgence**. Le CSNR doit soutenir les efforts du gouvernement pour coordonner les capacités fédérales de préparation et de réponse aux situations d'urgence au Canada.

Il a également été demandé au CSNR d'examiner si d'autres ressources sont nécessaires pour accomplir ce mandat.

Les preuves et l'examen des processus en place pour contrer l'ingérence étrangère me convainquent que la fonction de CSNR est très importante, voire critique. Ayant eu l'occasion d'entendre de nombreuses personnes qui ont occupé ce poste dans le passé, ainsi que celles qui l'occupent actuellement, j'ai pu constater que ce poste est toujours confié à des fonctionnaires de haut rang très expérimentés. Cependant, je note également que de nombreuses personnes ont occupé ce poste. À mon avis, le taux de roulement élevé a probablement joué un rôle dans certains des problèmes de circulation de l'information au sein du gouvernement qui ont été relevés par les organismes de surveillance.

Le rôle de coordonnateur national de la lutte contre l'ingérence étrangère (CNLIE)

Comme je l'expliquerai au **chapitre 12**, la création du rôle de coordinateur de la lutte contre l'ingérence étrangère et sa place dans l'appareil gouvernemental avaient fait l'objet de débats et discussions au sein du gouvernement depuis au moins 2020. Le poste de CNLIE a éventuellement été créé en mars 2023.

Les témoins du BCP m'ont dit qu'il a été décidé que le rôle serait hébergé par Sécurité publique Canada, et non par le BCP, car Sécurité publique est le responsable de l'élaboration des politiques régissant la sécurité nationale et l'ingérence étrangère. La décision de loger le CNLIE à Sécurité publique Canada reconnaît que la reddition de comptes en la matière revient aux ministres et aux sous-ministres plutôt qu'au BCP. Des témoins ont expliqué que l'implication directe du BCP dans certains enjeux pouvait affecter son rôle d'analyse critique. Le BCP est censé être le ministère qui remet en question, convoque et coordonne, le tout de manière objective, et non le ministère qui effectue le travail.

La création du poste de CNLIE a donné lieu à plusieurs discussions à propos de ce que devraient être la nature de son rôle, sa place dans la structure de gouvernance et sa relation avec les tables de gouvernance et les comités. Par exemple, le CNLIE devrait-il travailler seul dans une certaine mesure, puis présenter ses travaux à un comité? Les comités doivent-ils travailler indépendamment du CNLIE? Les comités doivent-ils même participer aux travaux du CNLIE?

L'actuel CNLIE, Sébastien Aubertin-Giguère, m'a dit qu'étant donné qu'il existait déjà de nombreux comités et qu'il se passe beaucoup de choses dans ce domaine, il était préférable de tirer parti des mécanismes déjà en place, plutôt que de créer une filière distincte de gouvernance pour l'ingérence étrangère. Le CNLIE participe régulièrement aux réunions du Comité des sous-ministres adjoints sur les opérations de sécurité nationale (le CSMAOSN), du Comité tactique des sous-ministres adjoints sur les opérations de sécurité nationale (le CTSMAOSN, qui traite fréquemment de

l'ingérence étrangère), du Comité des sous-ministre adjoints sur les politiques de la sécurité nationale (le CSMAPSN) et d'autres réunions de sous-ministres adjoints chaque fois que le sujet est lié à l'ingérence étrangère.

À la mi-octobre 2023, à peu près au moment où les travaux de révision des comités interministériels commençaient, le rôle et la place du CNLIE sont devenus les sujets de discussion d'une séance du Comité des sous-ministres sur la gestion de l'intervention du renseignement (CSMGIR).

Les hauts fonctionnaires se sont rendu compte qu'ils n'avaient pas tous les mêmes attentes à l'égard du CNLIE. Ils sont donc revenus aux sources et ont discuté du CNLIE, du type de coordination (du point de vue des politiques ou des opérations) qu'il devait assurer et du ministère qui devrait l'héberger (Sécurité publique Canada ou le BCP). Au terme de la séance, les membres du CSMGIR ont convenu qu'il fallait réexaminer le cadre et la raison d'être du rôle .

Finalement, le rôle du CNLIE est demeuré axé sur la coordination des politiques plutôt que celle de nature opérationnelle. Des témoins du BCP ont expliqué que la coordination opérationnelle était déjà assurée par le BCP et qu'elle lui convenait mieux en raison de sa fonction de convocation. De nombreux témoins ont mentionné que le rôle du CNLIE était encore très nouveau et qu'il demeurait en développement. Je suis d'accord avec eux et j'ajoute que, si son rôle est bien défini, le CNLIE pourrait être en mesure de résoudre bon nombre des problèmes de coordination et de communication révélés par la preuve.

Comités du Cabinet

Le Cabinet a des comités qui se concentrent sur des domaines particuliers en matière de politiques. Chaque comité du Cabinet est soutenu par un secrétariat du BCP. Le nouveau Conseil de la sécurité nationale est particulièrement pertinent en ce qui concerne l'ingérence étrangère.

Les initiatives politiques ou législatives sont généralement examinées par les comités du Cabinet avant d'être soumises à l'ensemble du Cabinet. Les initiatives sont présentées aux comités sous la forme de documents nommés « mémoires au Cabinet ». Les mémoires au Cabinet passent par un processus de consultation interministérielle et de discussion par les ministres avant d'être examinés par un comité du Cabinet. Les comités font ensuite des recommandations au Cabinet pour décision. Les décisions du Cabinet sont renvoyées aux ministères pour être mises en œuvre.

Les comités du Cabinet susceptibles d'aborder les questions d'ingérence étrangère comprennent le Comité chargé des affaires internationales et de la sécurité publique (le « **CCAISP** »), le Groupe d'intervention en cas d'incident (le « **GII** ») et le Conseil de la sécurité nationale récemment créé.

Le CCAISP examine les questions relatives à l'engagement et à la participation du Canada au sein de la communauté internationale, y compris la promotion et la diversification du commerce. Il est responsable des questions liées à la sécurité nationale et mondiale et fixe les priorités en matière de renseignement. Le CCAISP fait progresser le travail sur les politiques dans le domaine de la sécurité nationale.

Le GII est un comité *ad hoc* du Cabinet qui peut être activé en réponse à une situation particulière. Il constitue un forum tactique et opérationnel permettant aux ministres et aux sous-ministres de coordonner les réponses à des incidents précis. Il est présidé par le premier ministre et sa composition dépend de la situation à laquelle il est confronté.

Comme je le mentionne ci-dessus, le Conseil de la sécurité nationale a été établi en 2023. Présidé par le premier ministre, et dont le secrétariat est assuré par la CSNR, le Conseil de la sécurité nationale crée un processus formel pour transmettre du renseignement au Cabinet et concentre ses travaux sur la planification stratégique à long terme. Il ne prend pas de décisions opérationnelles, mais guide et oriente les actions du gouvernement. Les autres membres permanents sont, entre autres, le ministre de la Sécurité publique, le ministre de la Défense nationale et le ministre des Affaires étrangères. Le Comité invite également d'autres ministres sur une base ponctuelle, selon l'ordre du jour.

Le premier ministre a déclaré que l'élan ayant mené à la création du Conseil de sécurité nationale provenait en partie de la convocation régulière des GII ces dernières années, en réponse à divers événements. Dans ce cadre, des questions se posaient parfois sur la planification future et la nécessité d'une réflexion stratégique. Le Conseil de la sécurité nationale est un forum dédié au niveau du Cabinet, destiné à permettre une approche stratégique des questions de sécurité nationale à travers l'ensemble du gouvernement.

Comme pour les GII, l'une des principales caractéristiques du Conseil de la sécurité nationale est que de hauts fonctionnaires (généralement des sous-ministres et directeurs d'organismes) sont présents et participent aux discussions avec les ministres. Cela permet des délibérations approfondies et une orientation stratégique cohérente.

Des témoins ont déclaré que le Conseil de la sécurité nationale est une innovation importante qui a déjà prouvé son utilité. Le greffier actuel, M. Hannaford, l'a qualifié d'« extraordinairement important ».

Il appert de la preuve ci-dessus que le gouvernement s'efforce depuis un certain temps de renforcer et de simplifier la structure de gouvernance relative à la lutte contre l'ingérence étrangère. Il est trop tôt pour évaluer les changements effectués ou en discussion, mais il me semble que cette réflexion était nécessaire. J'ai pu constater la complexité de la structure mise en place jusqu'à tout récemment et à quel point elle pouvait compliquer et retarder la prise de décision.

11.5 Conclusion

Le Canada dispose d’un large éventail de ministères, d’agences et de structures de gouvernance qui répondent à l’ingérence étrangère. Comme le montre clairement ma discussion sur les comités interministériels du gouvernement canadien, il s’agit d’un domaine dynamique où les choses changent fréquemment. Dans le chapitre suivant, j’aborde ces changements en examinant les initiatives politiques et législatives qui se sont matérialisées dans les dernières années en réponse à l’ingérence étrangère.

CHAPITRE 12

Initiatives en matière de politiques et de législation

Les informations peuvent être incomplètes : *des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

12.1 Introduction

Dans ce chapitre, j'aborde deux éléments centraux de l'action du gouvernement pour détecter, dissuader et contrer l'ingérence étrangère : le Plan pour protéger la démocratie canadienne (le « **Plan** ») et la Stratégie de lutte contre les activités hostiles parrainées par des États. J'évoque aussi brièvement des développements plus récents.

En 2016 et 2017, la Russie a utilisé des cyberoutils et des campagnes de désinformation pour tenter de s'ingérer dans une série d'événements démocratiques : les élections présidentielles américaines et françaises, les élections législatives allemandes et le vote du Royaume-Uni sur son appartenance à l'Union européenne (le Brexit).

Ces événements ont révélé des vulnérabilités dans les processus électoraux. Ils ont également soulevé des questions sur la manière dont les gouvernements devraient réagir dans de telles situations. L'élection américaine a donné lieu à ce que l'on a appelé le « dilemme Obama ». Il s'agit du dilemme auquel a fait face le président américain alors qu'il était au courant de l'ingérence russe, mais estimait ne pas pouvoir intervenir publiquement parce qu'il craignait d'être perçu comme interférant dans l'élection à des fins partisanes.

Le gouvernement a suivi ces événements de près et, en 2019, a annoncé une série d'initiatives collectivement appelées le Plan pour protéger la démocratie canadienne. Lee Plan visait à aider à protéger les processus électoraux du Canada contre les menaces observées dans d'autres pays. Le Plan est toujours en place et des discussions sont en cours au sujet de la manière dont il devrait évoluer.

Parallèlement à l'élaboration du Plan en 2018, le gouvernement a commencé à travailler sur la Stratégie de lutte contre les activités hostiles parrainées par des États (la « **Stratégie AHPE** »). Les activités hostiles parrainées par des États (les « **AHPE** ») réfèrent aux actions menées par des États hostiles, ou par leurs mandataires, qui sont trompeuses, coercitives, corruptrices, secrètes, menaçantes ou illégales, mais qui se situent en deçà du seuil d'un conflit armé, et qui compromettent les intérêts nationaux du Canada. Alors que le Plan concentrait sur la protection des élections et des institutions démocratiques, la Stratégie AHPE portait sur des initiatives beaucoup plus larges en matière de politiques et de législation visant à répondre à l'ensemble des menaces d'ingérence étrangère auxquelles le Canada peut être confronté. L'intention était

de faire face aux AHPE en adoptant une approche impliquant l'ensemble du gouvernement et de la société. En 2022, un mémorandum concernant les AHPE a été soumis au Cabinet. Il proposait notamment de mener une consultation sur les modifications législatives qui sont devenues le projet de loi C-70 (la *Loi concernant la lutte contre l'ingérence étrangère*) ainsi que des propositions relatives aux politiques et au financement.

12.2 Le Plan pour protéger la démocratie canadienne

L'origine du Plan

Le 1er février 2017, le premier ministre a adressé une lettre de mandat à Karina Gould, alors ministre des Institutions démocratiques, la chargeant de diriger, avec les ministres de la Défense nationale et de la Sécurité publique, les efforts du gouvernement pour défendre les processus électoraux canadiens contre les cybermenaces.

Dans les mois qui ont suivi, la ministre Gould a collaboré avec plusieurs ministres, a rencontré les responsables d'organismes gouvernementaux et a consulté les partis politiques en vue d'élaborer la réponse du Canada.

Alors que la Russie était considérée comme la plus grande menace d'ingérence étrangère au début de ces travaux, la République populaire de Chine (la « **RPC** ») est apparue comme l'acteur menaçant clé dans les années qui ont suivi. Les travaux ont donc dépassé le cadre des cybermenaces générales utilisées par la Russie pour répondre à un éventail plus large de menaces d'ingérence étrangère contre la démocratie canadienne.

Le résultat de ces efforts a été le Plan, lequel a été annoncé publiquement le 30 janvier 2019.

Contenu du Plan

Le Plan reposait sur quatre piliers :

- lutter contre l'ingérence étrangère
- promouvoir la résilience institutionnelle
- renforcer la résilience des citoyens
- établir des règles de conduite pour les plateformes numériques (ce pilier a été renommé depuis « Bâtir un écosystème d'information sain »).

Une bonne partie de la preuve que j'ai entendue au sujet du Plan était centrée sur deux entités clés qui ont été établies pour répondre aux menaces d'ingérence étrangère pendant les élections : le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (le « **Groupe de travail** ») et le Protocole public en cas d'incident électoral majeur (le « **PPIEM** »). Le Plan comprenait également un ensemble d'autres initiatives destinées à renforcer la résilience de la société face à la désinformation et à la mésinformation.

Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections

Le Groupe de travail a été mis sur pied en août 2018, alors que le Plan était encore en cours d'élaboration, afin de coordonner les efforts visant à empêcher les activités secrètes, clandestines ou criminelles d'interférer dans le processus électoral canadien. Il est composé de représentants du Centre de la sécurité des télécommunications (le « **CST** »), du Service canadien du renseignement de sécurité (le « **SCRS** »), de la Gendarmerie royale du Canada (la « **GRC** ») et d'Affaires mondiales Canada (« **AMC** »). Les outils et les capacités de chacun des membres du Groupe de travail sont abordés au **chapitre 11**.

Le Groupe de travail est un forum de coordination et d'échange d'informations, et non un organe décisionnel de haut niveau. Ses membres coordonnent l'examen du renseignement relatif aux élections, offrent un portrait de la situation et échangent des informations afin que des réponses puissent être apportées si nécessaire. Chaque membre conserve son pouvoir d'action indépendant.

Le Protocole public en cas d'incident électoral majeur (PPIEM) et le Panel des cinq

Le PPIEM est une directive du Cabinet rendue publique le 9 juillet 2019. Il exige que cinq hauts fonctionnaires, appelés le « Panel des cinq » (ou le « **Panel** »), communiquent avec les Canadiennes et les Canadiens si la capacité du Canada à tenir des élections libres et justes est menacée. Ses membres sont :

- le greffier du Conseil privé
- le conseiller à la sécurité nationale et au renseignement auprès du premier ministre (le « **CSNR** »)
- le sous-ministre de la Justice et sous-procureur général
- le sous-ministre de la Sécurité publique
- le sous-ministre des Affaires étrangères.

Pendant les élections, le Panel reçoit des informations du Groupe de travail et d'autres sources. S'il conclut qu'un incident, ou une accumulation

d'incidents, menacent la capacité du Canada à tenir des élections libres et équitables, le gouvernement fait alors une déclaration publique pour informer les Canadiennes et les Canadiens de l'incident. Au cours des travaux de la Commission, le critère de l'incident ou de la série d'incidents menaçant la capacité du Canada à organiser des élections libres et équitables utilisé pour déterminer quand le Panel devrait conclure qu'il y a lieu de faire une déclaration publique a été appelé « le seuil ». L'évaluation visant à déterminer si le seuil est atteint prend en compte les impacts à l'échelle des circonscriptions et à l'échelle nationale. Les décisions du Panel sont prises par consensus.

Le Panel a été créé pour écarter les intérêts politiques de l'évaluation et de l'annonce des menaces pesant sur le processus électoral. En s'appuyant sur de hauts fonctionnaires non partisans, le gouvernement a cherché à éviter les problèmes de conflit d'intérêts qui pourraient survenir si des élus faisant campagne pour obtenir un mandat politique étaient chargés de soulever publiquement des préoccupations au sujet de l'ingérence étrangère.

La ministre Gould a expliqué les raisons pour lesquelles le gouvernement a désigné ces cinq postes au sein de la fonction publique. Elle a affirmé qu'ils ont une connaissance approfondie de la nature du renseignement et de ses limites. Ils apportent également des perspectives différentes, ce qui permet au Panel d'évaluer les situations factuelles avec les nuances nécessaires.

Si le seuil est atteint, le Panel informe le premier ministre, les autres chefs des principaux partis ou d'autres représentants désignés des partis et Élections Canada qu'une annonce publique sera faite. Immédiatement après, le greffier du Conseil privé, au nom du Panel, publie une déclaration publique ou demande au(x) dirigeants(s) des agences concernées de le faire.

Le seuil pour faire une annonce publique est élevé. Il doit y avoir plus qu'une simple possibilité de menace pour une élection. François Daigle, ancien sous-ministre de la Justice, sous-procureur général et membre du Panel en 2021, m'a indiqué que les membres du Panel recherchaient des informations qui leur permettraient de déterminer si un incident était probable et aurait une incidence probable sur l'élection.

Pour déterminer si un incident est probable, le Panel prend en compte la crédibilité et la fiabilité du renseignement qu'il reçoit. Pour évaluer son incidence, le Panel tient compte de facteurs liés à l'incident comme sa portée, son ampleur, sa source, sa pertinence, sa durée de vie, sa capacité d'autocorrection et l'existence d'autres options permettant d'atténuer les risques en vue d'assurer des élections libres et équitables.

La raison justifiant un seuil élevé est la crainte que l'intervention du Panel ne fasse plus de mal que de bien, car dès qu'une annonce publique concernant l'ingérence étrangère est faite, la confiance envers l'élection peut être ébranlée. Cela peut également avoir un effet négatif sur la confiance du public envers la démocratie canadienne dans son ensemble. Il est également possible que le Panel lui-même soit perçu comme partisan et s'ingérant dans l'élection. En outre, il se peut que des pays étrangers tentent de faire en sorte

qu'une annonce soit faite afin de saper la confiance envers les élections ou d'amplifier la désinformation.

Même si le Plan était une excellente initiative, je crois comprendre que la population connaît peu ou pas le Panel des cinq, sa composition et son mandat. Il me semble essentiel que la population canadienne soit au fait du rôle du Panel si l'on veut que le public accepte une éventuelle intervention de sa part. J'espère que les travaux de la Commission contribueront à mieux faire connaître le Panel, mais je sais que cela est loin d'être suffisant. Le gouvernement doit se consacrer, dès à présent, à faire en sorte que le Panel, et son rôle, soient connus de la population.

La Déclaration du Canada sur l'intégrité électorale en ligne

La désinformation en ligne peut créer de la confusion et exploiter des tensions sociétales existantes. Dans le cadre du Plan, le gouvernement a travaillé avec les plateformes de médias sociaux pour qu'elles accroissent leur transparence, leur authenticité et leur intégrité et ainsi contribuent à la protection des élections. L'un des éléments de cette approche est la Déclaration du Canada sur l'intégrité électorale en ligne (la « **Déclaration** »).

La Déclaration est un accord volontaire qui établit un ensemble d'engagements entre le gouvernement et les plateformes en ligne afin de préserver les élections fédérales de l'ingérence malveillante et de bâtir un écosystème en ligne plus sain. La Déclaration n'a pas force de loi et ce ne sont pas toutes les plateformes de médias sociaux qui en sont signataires.

L'Initiative de citoyenneté numérique

L'un des objectifs généraux du Plan est de renforcer la résilience des citoyens. Le ministère du Patrimoine canadien est le chef de file de ce travail. L'Initiative de citoyenneté numérique (l'« **ICN** ») du ministère du Patrimoine canadien est une stratégie qui vise à soutenir la démocratie et la cohésion sociale en renforçant la résilience contre la désinformation en ligne. Elle établit également des partenariats pour soutenir un écosystème d'information sain. La Direction générale des Cadres de politiques pour les marchés numériques et créatifs du ministère élabore des politiques relatives aux cyberpréjudices et à la désinformation en ligne.

La preuve que j'ai entendue me convainc que le rôle du ministère du Patrimoine canadien deviendra bientôt extrêmement important en lien avec l'ingérence étrangère. Tout indique que les États étrangers qui tentent de s'ingérer dans nos élections ou d'autres institutions démocratiques le feront de plus en plus par le biais de la désinformation sur les médias sociaux. Permettre au public de comprendre et de détecter la désinformation est déjà un travail important, mais, compte tenu du rythme rapide auquel la technologie évolue, ces efforts doivent redoubler d'ardeur.

Le Plan en action : 2019

La Déclaration du Canada sur l'intégrité électorale en ligne de 2019

Avant les élections générales de 2019, quatre grandes entreprises américaines de médias sociaux – Microsoft, Twitter, Facebook et Google – ont signé la Déclaration. Le gouvernement souhaitait ainsi indiquer qu'il attendait des plateformes de médias sociaux qu'elles contribuent à garantir l'intégrité des élections de 2019 en appliquant leurs propres normes et politiques.

Le Groupe de travail et le Panel des cinq

Les travaux du Groupe de travail ont commencé bien avant les élections de 2019. En novembre 2018, le Groupe de travail a créé l'« équipe technique » (un groupe d'experts du CST, d'AMC et du SCRS) pour coordonner les efforts de lutte contre l'ingérence étrangère en ligne. Le Groupe de travail a également commencé à mettre au point une gamme de produits analytiques pour aider à définir les menaces pour l'élection et à clarifier les processus d'intervention internes et externes. Il s'agissait notamment d'évaluations des menaces de base concernant les capacités et les intentions des États hostiles, de scénarios et d'analyses des réponses potentielles, ainsi que de documents préparés aux niveaux « Secret » et non classifié destinés à un public plus large.

Le Panel des cinq a commencé à se réunir juste avant la période électorale. Il a régulièrement reçu des breffages de base de la part du Groupe de travail. Il a revu les termes de son mandat et a rencontré les responsables des élections pour mieux comprendre leurs rôles. Le Panel a tenté de mieux comprendre le seuil d'intervention prévu au Protocole public en cas d'incident électoral majeur (PPIEM) en travaillant sur des scénarios conçus pour explorer des enjeux, notamment ceux ayant trait au moment où il serait approprié d'agir, à la manière dont se déroulerait une annonce et à qui la ferait. Une fois la période électorale commencée, le Panel s'est réuni chaque semaine et était toujours disponible sur appel.

Les membres du Panel ont également reçu des informations par l'intermédiaire de leurs ministères et figuraient sur la liste de distribution du SCRS pour les produits de renseignement pertinents. Lors de ses réunions hebdomadaires, le Panel était breffé par le Groupe de travail. Entre les réunions, il recevait également des rapports de situation (des « **RAPSIT** ») quotidiens du Groupe de travail. Les RAPSIT étaient basés sur des informations fournies par les membres du Groupe de travail. Le Panel pouvait demander plus d'informations au Groupe de travail ou à d'autres en cas de besoin.

Tous les membres du Groupe de travail ont adopté une conception large des informations qu'ils devaient s'échanger entre eux. Le Mécanisme de réponse rapide du Canada (le « **MRR du Canada** ») d'AMC fournissait des rapports en temps réel sur sa surveillance de l'environnement numérique national en ce

qui a trait à la désinformation et la mésinformation. Le CST transmettait des rapports jugés suffisamment importants sur les capacités des États d'intérêt. Le SCRS fournissait des produits potentiellement pertinents pour l'ingérence étrangère ou les institutions démocratiques, ainsi que des informations sur les motivations et les capacités des acteurs menaçants. La GRC, vu sa mission, avait moins d'informations à communiquer, mais elle relayait tout ce qu'elle pensait être important.

Bien que le Panel des cinq ait été le principal bénéficiaire des informations fournies par le Groupe de travail, celui-ci partageait également des informations avec un ensemble de partenaires externes, notamment par l'intermédiaire des comités de coordination sur la sécurité des élections, qui sont des groupes de fonctionnaires chargés des questions ayant trait à l'intégrité des élections. Le Groupe de travail organisait également des breffages de niveau « Secret » à l'intention des représentants des partis politiques bénéficiant d'une autorisation de sécurité. Ces breffages comprenaient des informations provenant de sources ouvertes ainsi que certaines informations classifiées sur les tactiques d'ingérence étrangère utilisées.

Comme je l'ai dit au chapitre 7 (volume 2), le Panel a conclu, en 2019, que le seuil requis pour procéder à une annonce publique n'avait pas été atteint. Il a constaté qu'il y avait eu un certain niveau d'ingérence étrangère, mais rien qui avait menacé la capacité du Canada à tenir une élection libre et équitable.

Le rapport après-action du Groupe de travail de 2019

À la suite de l'élection, le Groupe de travail a produit un rapport après-action (un « **RAA** ») classifié. Les RAA du Groupe de travail ne sont pas censés être des produits d'évaluation ou d'analyse. Selon un représentant du SCRS, un RAA est plutôt considéré comme un rapport tactique sur ce que le Groupe de travail a observé ou n'a pas observé. Le RAA 2019 a recensé les succès, les défis et les éléments à améliorer.

Le RAA 2019 indiquait que le Groupe de travail a constaté des activités d'ingérence étrangère ciblant certaines circonscriptions et certains candidats. Selon ce rapport, ces activités ne faisaient pas partie d'une vaste campagne d'ingérence électorale et n'ont pas eu d'impact sur le résultat global des élections. La représentante d'AMC au sein du Groupe de travail en 2019 a expliqué que la conclusion quant à l'impact était celle du Panel des cinq et que le Groupe de travail s'était contenté de la rapporter. Ce n'est pas le rôle du Groupe de travail d'évaluer l'impact de ce qu'il observe.

Le rapport Judd et les modifications apportées au PPIEM

Le PPIEM exige un examen indépendant après une élection afin d'évaluer sa mise en œuvre et son efficacité. L'examen pour 2019 a été effectué par l'ancien directeur du SCRS, James Judd (le « **Rapport Judd** »). M. Judd a constaté que le PPIEM avait été mis en œuvre avec succès et a recommandé qu'il soit utilisé lors des prochaines élections générales.

M. Judd a formulé un certain nombre de recommandations visant à l'améliorer ainsi que d'autres réponses du gouvernement à l'ingérence étrangère. En conséquence, le Cabinet a publié une Directive du Cabinet modifiée en mai 2021. Les changements apportés sont les suivants :

- Le PPIEM a été rendu applicable à toutes les élections futures.
- Le mandat du Panel des cinq a été élargi pour prendre en compte les menaces intérieures ainsi que celles provenant de l'étranger.
- Le PPIEM a été étendu à toute la période de transition, qui peut être plus longue que la période électorale dans certaines circonstances.
- Le Panel des cinq a été expressément autorisé à communiquer des informations à d'autres entités.

Les partis politiques ont été expressément autorisés à fournir des informations au Panel.

Le gouvernement n'a pas accepté la recommandation du Rapport Judd d'étendre le PPIEM à la période préélectorale, c'est-à-dire la période qui précède le début d'une campagne électorale. En effet, pendant cette période, les ministres disposent des pouvoirs et ont la responsabilité de répondre à l'ingérence étrangère. Le PPIEM est en partie le reflet de la convention de transition selon laquelle, à partir de la période électorale et jusqu'à la formation d'un nouveau gouvernement, le gouvernement (les ministres en particulier) ne doit traiter que des affaires courantes, non controversées ou urgentes, qui sont dans l'intérêt du public.

Le Plan en action : 2021

La Déclaration du Canada sur l'intégrité électorale en ligne de 2021

La Déclaration a été mise à jour en 2021 en prévision des élections générales et davantage de plateformes l'ont signée. Aux quatre membres initiaux (Facebook/Meta, Google, Microsoft et Twitter) se sont ajoutés TikTok, LinkedIn et YouTube.

Le Groupe de travail et le Panel des cinq

En 2021, le Groupe de travail a fonctionné de la même manière qu'en 2019. La fréquence des réunions et des rapports est restée la même, et le Groupe de travail a produit en grande partie les mêmes types de documents. Cependant, il a tiré une leçon des élections de 2019 et a reconnu l'importance de partager des informations au niveau de classification le plus bas possible.

À la fin de 2020, le Groupe de travail a également commencé à produire des « résumés des menaces » pour permettre à tous ses partenaires de saisir le contexte global de la menace. Les premiers résumés, publiés à la fin de 2020 et en janvier 2021, ont été suivis de rapports mensuels de mai à août 2021. Les rapports mensuels ont commencé lorsque le Panel des cinq est devenu actif, de sorte que ses membres avaient une vision plus cohérente de ce que le Groupe de travail constatait.

En 2021, la pandémie de COVID-19 a constitué une différence majeure qui a eu une incidence sur les activités du Groupe de travail. Le Groupe de travail a dû œuvrer dans un environnement de classification mixte, car ses membres ne pouvaient pas toujours se réunir dans un espace classifié. Cela signifie que, parfois, ils ne pouvaient discuter de sujets qu'à un niveau très général. La pandémie a également eu pour conséquence que la présidence du Groupe de travail disposait de moins de ressources pour assurer les fonctions administratives et de secrétariat.

Le Groupe de travail disposait cependant de plus de capacités qu'en 2019. Le CST bénéficiait de plus de ressources, et le MRR du Canada avait plus d'expérience et de capacités linguistiques. Comme le mandat du Groupe de travail s'était élargi pour inclure les menaces intérieures, dont les menaces liées à la sécurité des élections, la GRC y a joué un rôle plus important qu'auparavant.

Le Panel des cinq s'est réuni avant, pendant et après la période électorale. À partir de janvier 2021, il s'est attelé à la tâche de comprendre des menaces pertinentes, a discuté des enseignements tirés de 2019 et a travaillé sur des scénarios hypothétiques.

Dès l'annonce de l'élection, le Groupe de travail a envoyé des RAPSIT quotidiens au Panel. Cependant, en raison de la pandémie, les membres du Panel ne pouvaient les consulter que lorsqu'ils se rendaient à leur bureau. Le Groupe de travail organisait également des breffages hebdomadaires à l'issue desquels le Panel délibérait en privé.

Le Groupe de travail a continué à fournir des breffages aux représentants des partis politiques.

Comme en 2019, le Panel des cinq de 2021 a conclu que le seuil justifiant d'effectuer une annonce n'avait pas été atteint.

Le rapport après-action du Groupe de travail de 2021

Le Groupe de travail a produit un rapport après-action (RAA) classifié à la suite des élections générales de 2021. Selon ce rapport, la République populaire de Chine (la RPC) a cherché à s'ingérer dans les élections en soutenant des individus considérés comme pro-RPC ou neutres, et l'Inde a pu se livrer à des activités d'ingérence destinées à influencer les résultats électoraux. D'autres États comme la Russie, l'Iran et le Pakistan n'ont pas été observés comme ayant tenté de s'ingérer dans les élections.

Le RAA 2021 formulait un certain nombre de recommandations à l'intention du gouvernement, notamment qu'il :

- Revoie son plan de communication afin d'être plus stratégique en matière de communication sur la sécurité des élections
- Continue à financer le MRR du Canada et à conclure des contrats avec des partenaires externes pour compléter les activités de surveillance du MRR du Canada
- Assure le financement d'une surveillance indépendante menée par des groupes universitaires et de la société civile.
- Examine comment la communauté de la sécurité et du renseignement pourrait mieux travailler avec les partis politiques en dehors du cycle électoral.

Évolution du Plan après 2021

Le Rapport Rosenberg

L'examen du PPIEM de 2021 a été réalisé par l'ancien sous-ministre Morris Rosenberg. Son rapport (le « **Rapport Rosenberg** ») a été publié en 2023. Comme le Rapport Judd, le Rapport Rosenberg a conclu que plusieurs éléments fonctionnaient bien et devaient être maintenus, mais il a également recommandé certaines améliorations.

Plusieurs des recommandations de M. Rosenberg avaient trait à une meilleure communication avec le public canadien sur le risque d'ingérence étrangère et les mesures prises par le gouvernement pour protéger l'intégrité des élections. D'autres recommandations visaient à assurer un meilleur fonctionnement du Panel des cinq. Cela comprenait notamment une meilleure préparation, d'assurer une continuité quant aux individus qui le composent, et la tenue de breffages plus tôt, avec des informations provenant d'un plus grand nombre de sources.

M. Rosenberg a également recommandé de poursuivre l'étude de plusieurs enjeux, y compris le rôle des différents membres du Groupe de travail et l'enjeu de savoir si le Panel des cinq devrait être en mesure de faire des

annonces dans des circonstances où il existe de l'ingérence étrangère, sans toutefois que le seuil fixé par le PPIEM ne soit atteint.

Davantage de breffages pour les membres du Panel

En 2023, en réponse au Rapport Rosenberg, le gouvernement s'est engagé à breffer les nouveaux membres du Panel dans les trois mois suivant leur nomination et à tenir des réunions régulières du Panel à partir du printemps 2023. Depuis lors, les nouveaux membres du Panel ont reçu des breffages individuels, et, depuis janvier 2024, le Groupe de travail a breffé le Panel environ toutes les six semaines. Les membres du Groupe de travail et du Panel des cinq m'ont dit à quel point ils appréciaient ces breffages réguliers.

L'utilisation du Groupe de travail pour les élections partielles et le rôle du Comité des sous-ministres sur la gestion de l'intervention du renseignement

Même si le Groupe de travail fonctionnait dans les faits toute l'année, il se concentrait jusqu'en 2023 sur les élections générales. Il n'était pas responsable des élections partielles.

Le 16 mai 2023, le gouvernement a annoncé qu'en raison du nombre important de discussions publiques sur l'ingérence étrangère à l'époque et de l'importance d'assurer la confiance du public envers les élections, le Groupe de travail fournirait une surveillance renforcée pour les quatre élections partielles qui se tiendraient en juin 2023. Il s'agissait d'un changement d'approche important, qui a surpris le Groupe de travail. Le Groupe de travail a été mobilisé pour chaque élection partielle fédérale depuis lors.

Il existe des différences entre le fonctionnement du Groupe de travail lors d'élections partielles et lors d'élections générales.

La plus importante concerne la manière dont le Groupe de travail fait rapport à l'appareil gouvernemental. Étant donné que le PPIEM ne s'applique pas aux élections partielles (puisque la convention de transition n'est pas alors en vigueur), et que les ministres conservent leurs pouvoirs et leurs responsabilités, le Panel des cinq n'a pas d'autorité. Au lieu de cela, le Groupe de travail fait rapport au Comité des sous-ministres sur la gestion de l'intervention du renseignement (le « **CSMGIR** », voir au **chapitre 11**), et les sous-ministres se tourneraient vers leur ministre s'ils estimaient qu'une mesure devait être prise. La composition du CSMGIR est semblable à celle du Panel des cinq, sans être identique. Le sous-ministre de la Justice et le sous-procureur général ne siégeaient pas au CSMGIR, et il y avait de hauts fonctionnaires au CSMGIR qui n'étaient pas membres du Panel.

Le rôle du CSMGIR était également différent de celui du Panel des cinq. Alors que le Panel est un organe décisionnel, le CSMGIR était un comité de fonctionnaires responsables devant leurs ministres respectifs. Si des

informations relatives à un incident électoral avaient été signalées au CSMGIR et avaient nécessité une communication publique, ces informations auraient été relayées par le CSMGIR aux ministres responsables.

Avant chaque élection partielle, le Groupe de travail produit désormais une évaluation de la menace de base qui examine s'il existe ou non du renseignement indiquant qu'un État étranger a l'intention de s'ingérer dans l'élection partielle. Cette évaluation prend également en compte les données démographiques de la circonscription et les candidats précis qui s'y présentent.

Les rapports du Groupe de travail sont moins fréquents pendant les élections partielles, comparativement aux élections générales. S'il n'a pas de nouvelles informations à communiquer, le Groupe de travail ne publie que des RAPSIT hebdomadaires. Les cabinets des ministres figuraient auparavant sur la liste de distribution des RAPSIT. Cependant, en juin 2023, le CSMGIR a décidé de les retirer. Le représentant du SCRS au sein du Groupe de travail a expliqué que, si le CSMGIR avait connaissance d'une information qu'il estimait devoir être transmise à un ministre, il l'en informait. Il a également expliqué que les rapports continuaient de circuler, de telle sorte que, si une information devait faire l'objet d'une discussion, elle pouvait être diffusée par les mécanismes normalement utilisés.

À la suite des reportages médiatiques de 2023, le Bureau du Conseil privé (le « **BCP** ») a demandé au Groupe de travail de vérifier qui lisait ses RAPSIT. Cela s'est avéré difficile à faire. Par conséquent, en 2024, le Groupe de travail a décidé d'utiliser la base de données centralisée du CST, qui permet de suivre les produits distribués (voir le chapitre 14, volume 4). Tous les produits liés au Groupe de travail sont désormais distribués de cette manière.

J'ai entendu des témoignages de la part des membres du Groupe de travail voulant que le maintien du Groupe de travail pendant les élections partielles ait à la fois entraîné des coûts et des opportunités. Le MRR du Canada avait le coût le plus important. Pendant les élections partielles de 2023 et 2024, la moitié des analystes du MRR du Canada ont en effet consacré les deux tiers de leur temps au Groupe de travail. Cela signifie que le MRR du Canada a dû arrêter, réduire ou reporter le travail qu'il exécute dans d'autres domaines. Par exemple, pour les élections partielles de juin 2023, le MRR du Canada a interrompu sa surveillance des postes de police étrangers de la RPC (voir le chapitre 17, volume 4). Un fardeau opérationnel pèse également sur l'Équipe de renseignement sur la criminalité à caractère idéologique de la GRC. Environ la moitié de son temps a été consacrée aux élections partielles.

L'incidence sur le CST et le SCRS a été moindre, puisque la collecte et la diffusion du renseignement sur l'ingérence étrangère font partie de leur mandat habituel. Toutefois, ces agences ont dû composer avec des charges administratives supplémentaires, en particulier pour le président du Groupe de travail.

L'adoption d'un rôle de surveillance des élections partielles a eu des répercussions sur les autres activités propres au Groupe de travail lui-même, qui a dû interrompre ses exercices de simulation et l'examen des recommandations visant à le perfectionner.

Néanmoins, les membres du Groupe de travail m'ont dit que la surveillance des élections partielles les avait aidés à éviter le problème du « démarrage à froid » qui se produit si le Groupe de travail est utilisé à quelques années d'intervalle. Des périodes plus fréquentes de surveillance ont permis d'exécuter leurs activités plus efficacement, ont encouragé les discussions et ont aidé à planifier les activités pour les prochaines élections générales. Elles ont également augmenté la cohésion et la coordination au sein du groupe.

Rapports après-action non classifiés du Groupe de travail

À partir des élections partielles de 2023, le Groupe de travail a commencé à produire des rapports après-action (RAA) non classifiés. Il en a publié pour toutes les élections partielles depuis juin 2023. Dans chaque cas, il a indiqué n'avoir observé aucun indice d'ingérence étrangère.

Les membres du Groupe de travail ont déclaré qu'il était difficile de produire des rapports non classifiés. S'ils détiennent du renseignement sur des activités menaçantes, il peut être difficile de déterminer ce qui peut être dévoilé dans le RAA. Même le fait de signaler qu'aucun incident d'ingérence étrangère n'a été observé pourrait révéler à des acteurs étatiques hostiles des lacunes en matière de renseignement. Cependant, les témoins du Groupe de travail ont convenu que la divulgation d'informations au public était un moyen de renforcer la résilience du Canada face à l'ingérence étrangère dans les élections. Je suis tout à fait d'accord avec eux.

L'Initiative de citoyenneté numérique et le Programme de contributions en matière de citoyenneté numérique

L'Initiative de citoyenneté numérique (l'ICN) est une composante du Plan qui n'est pas directement liée au cycle électoral, mais qui se poursuit plutôt tout au long de l'année. Elle s'inscrit dans le pilier « renforcer la résilience des citoyens » du Plan. L'objectif est de soutenir la démocratie et l'inclusion sociale au Canada en renforçant la résilience des citoyens contre la désinformation en ligne et en appuyant un écosystème d'information sain.

Lorsque le gouvernement a dévoilé le Plan en 2019, il a également annoncé 7 millions de dollars pour financer la première phase de l'ICN. En raison de l'urgence de mettre en place des mesures pour les élections de 2019, le financement a été fourni par le biais de programmes préexistants administrés par le ministère du Patrimoine canadien. Ce financement a donné lieu à plus de 20 accords de contribution avec la société civile, le monde universitaire et le secteur privé.

Le ministère du Patrimoine canadien a ensuite créé le Programme de contributions en matière de citoyenneté numérique (le « **PCCN** ») pour administrer le financement de la recherche appliquée et des activités axées sur les citoyens.

Chaque année, le PCCN lance un appel de propositions dont les priorités sont élaborées par les fonctionnaires du ministère du Patrimoine canadien en consultation avec d'autres ministères et partenaires externes. L'appel de propositions 2023-2024 du PCCN comprenait sept priorités, dont l'une concernait des projets visant à élaborer et à publier des outils pour renforcer la résilience face à la mésinformation et à la désinformation d'États étrangers ciblant les Canadiennes et les Canadiens, y compris les membres des communautés issues des diasporas.

Depuis 2022, le PCCN finance également le Réseau canadien de recherche sur les médias numériques (le « **RCRMN**[14] »), un réseau de groupes universitaires et de la société civile qui surveillent et analysent l'écosystème de l'information au Canada. Le RCRMN produit des évaluations de base de l'écosystème de l'information et utilise un protocole de réponse pour réagir aux incidents majeurs liés à l'information, y compris ceux entourant les élections. J'aborde le RCRMN au **chapitre 13**.

Des représentants du RCRMN ont assisté à une retraite du Panel des cinq tenue le 25 mars 2024 pour discuter de l'écosystème canadien de l'information et du protocole d'alerte en cas d'incident du RCRMN. Une discussion a suivi sur la manière dont le RCRMN pourrait soutenir et compléter les travaux du Panel. C'était la première fois depuis la création du PPIEM que des personnes extérieures au gouvernement étaient invitées à breffer le Panel.

Le RCRMN devrait jouer un rôle important dans la surveillance de l'écosystème en ligne lors des prochaines élections générales fédérales.

L'Unité de protection de la démocratie

En 2022, le gouvernement a créé l'Unité de protection de la démocratie (l'« **UPD** ») au sein du Secrétariat des institutions démocratiques du BCP (le « **SID du BCP** »). Le mandat de l'UPD est de coordonner, d'élaborer et de mettre en œuvre des mesures à l'échelle du gouvernement pour protéger les institutions démocratiques du Canada.

Les exemples de travaux de l'UPD comprennent les trousses d'outils de lutte contre la mésinformation et la désinformation destinés aux parlementaires, aux fonctionnaires et aux leaders communautaires, ainsi que des formations sur la désinformation destinées au grand public.

[14] Le PCCN a accordé au RCRMN un financement de 5,5 millions de dollars sur trois ans.

Un regard sur l'avenir

Le Plan a fait l'objet de divers examens, rapports et évaluations depuis sa mise en œuvre initiale.

Il y a d'abord eu les évaluations effectuées par M. Judd et M. Rosenberg dont il a été question plus haut. Puis, en 2023, le gouvernement a commandé un rapport – le rapport LeBlanc-Charette – pour expliquer les mesures qu'il prenait pour contrer l'ingérence étrangère et pour traiter des recommandations sur le Plan qui étaient toujours à l'étude[15].

En 2024, trois autres rapports pertinents traitant du Plan ont été publiés : les rapports de 2024 du Comité des parlementaires sur la sécurité nationale et le renseignement (le « **CPSNR** ») et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, ainsi que le Rapport initial de cette Commission. J'ai entendu des témoignages indiquant que tous ces rapports sont également considérés par le gouvernement dans le cadre de ses travaux en vue d'élaborer une troisième version du Plan. Les options de politiques font régulièrement l'objet de discussions au sein de la fonction publique et au niveau des ministères.

Ci-dessous, j'aborde certaines questions qui ont été soulevées au sujet du Plan et qui pourraient avoir une incidence sur l'élaboration de sa prochaine version.

Composition du Panel des cinq

La composition du Panel des cinq a fait l'objet de beaucoup d'attention lors des audiences de la Commission.

Certains participants ont suggéré que les sous-ministres ne sont pas suffisamment indépendants du Cabinet pour remplir leurs obligations liées au PPIEM, ou qu'ils ne comprennent pas assez la politique électorale pour évaluer correctement l'incidence d'événements particuliers. Des juges, des personnalités respectées et le directeur général des élections ont été proposés comme membres du Panel, soit en plus des membres existants, soit en remplacement de ceux-ci.

La question de la composition du Panel a suscité un vif intérêt au sein du gouvernement lors de la création du PPIEM. Le SID du BCP a envisagé différentes compositions possibles, mais estime que les membres actuels forment un groupe unique et efficace. Ils ont accès au renseignement et savent comment l'utiliser, ce qui leur permet de mieux comprendre le contexte de la menace. Les membres du Panel conservent aussi leurs propres pouvoirs et agissent, de fait, en tant qu'organe de coordination

[15] Le rapport LeBlanc-Charette a été commandé en réponse aux fuites médiatiques de 2022-2023 et aux préoccupations croissantes au sein du Parlement et du public concernant l'ingérence étrangère.

opérationnelle destiné à répondre aux incidents potentiels d'ingérence étrangère.

Le directeur général des élections n'est pas membre du Panel. Stéphane Perrault, qui occupe actuellement ce rôle, m'a dit que cela préservait l'indépendance d'Élections Canada et reflétait ses propres obligations de reddition de comptes, qui diffèrent de celles du gouvernement.

La communication publique par le Panel

Les membres du Panel ont indiqué qu'une meilleure connaissance du Panel par le public était importante pour renforcer la confiance envers les institutions publiques. Cela pourrait rassurer le public de savoir qu'une structure de gouvernance est en place pour lutter contre l'ingérence étrangère pendant les élections. En outre, si le public comprenait mieux le Panel, il serait davantage en mesure de saisir la signification d'une annonce du Panel si jamais une telle annonce s'avérait nécessaire lors d'élections. Le Panel s'interroge actuellement sur les différentes manières d'expliquer son rôle au public et sur l'adoption d'une approche de communication plus proactive liée à son travail avant, pendant et après une élection.

Toutefois, le Panel m'a aussi fait part des risques liés à la communication publique. Par exemple, une tentative du Panel de répondre aux préoccupations concernant la désinformation pourrait être perçue comme décelant un parti pris. Les témoins du BCP estiment qu'il est essentiel que les fonctionnaires n'entreprennent pas de débats sur la véracité ou l'authenticité des informations qui circulent dans le cadre d'un processus électoral si la fonction publique veut conserver son rôle non partisan.

Pour tirer profit de la communication publique tout en évitant les risques, le Panel envisage une série d'options, notamment la tenue d'un breffage technique destiné aux médias, l'organisation d'un événement de presse plus formel, la possibilité pour les représentants des médias d'observer le Panel lors d'un exercice de simulation, ou une combinaison de ces approches.

Un autre seuil pour le PPIEM

On m'a indiqué que le gouvernement étudiait la possibilité de modifier le PPIEM pour l'autoriser à faire des annonces au nom du gouvernement même si le seuil actuel n'est pas rencontré. Bien que le gouvernement ne veuille pas s'immiscer dans le discours démocratique légitime, il peut arriver que les Canadiennes et les Canadiens aient intérêt à savoir s'il y a de l'ingérence étrangère dans une élection générale, même si elle n'atteint pas le seuil élevé prévu au PPIEM. On peut supposer que cela exigerait du gouvernement qu'il définisse des critères devant être satisfaits pour justifier des annonces publiques correspondant à un seuil plus bas. Il reste cependant à déterminer qui devrait faire une annonce pour un événement qui n'atteint pas le seuil (on peut penser, par exemple, au Groupe de travail), et la manière dont elle serait communiquée (un exemple serait un breffage technique à des journalistes).

Les témoins du BCP ont souligné qu'il existe une distinction importante entre une annonce du Panel en vertu du PPIEM et les communications générales du gouvernement. Ils ont affirmé que l'intention est que, lors des périodes d'élections, le Panel continue de garder le même seuil élevé pour justifier une annonce publique.

Rendre le Groupe de travail permanent

L'idée initiale était que le Groupe de travail ne soit actif que pendant les élections générales. Toutefois, cela ne tenait pas compte du fait que les menaces d'ingérence étrangère existent aussi en dehors des périodes électorales. En réalité, le Groupe de travail est actif en permanence, même si cela n'apparaît pas dans son mandat.

Par exemple, le Groupe de travail reçoit du renseignement sur l'ingérence étrangère observée dans des élections non fédérales ou dans des processus de partis politiques, comme les courses à l'investiture et à la direction, même si cela ne fait pas partie de son mandat. Cette approche permet au Groupe de travail de mieux évaluer et comprendre les menaces éventuelles pesant sur les élections fédérales. Il est utile de disposer d'une base de référence sur l'environnement de la menace en dehors des périodes électorales.

Certains témoins du Groupe de travail ont souligné qu'un Groupe de travail permanent pourrait effectuer des évaluations plus solides de la menace sur le plan national, qu'il serait mieux placé pour échanger l'information avec les parties prenantes et le grand public, ou qu'il pourrait bénéficier d'une interaction plus importante avec les partenaires internationaux. Cependant, ils ont reconnu, et d'autres témoins se sont dit d'accord, que le fait de rendre le Groupe de travail permanent, avec des capacités renforcées, exigerait des ressources supplémentaires pour réaliser un mandat qui, à certains égards, chevaucherait celui des agences de sécurité. Daniel Rogers, ancien conseiller adjoint à la sécurité nationale et au renseignement auprès du premier ministre et directeur actuel du SCRS, m'a dit que le gouvernement était soucieux d'utiliser judicieusement ses ressources pour contrer l'ingérence étrangère.

John Hannaford, actuel greffier du Conseil privé et président du Panel des cinq, a déclaré que les conseils du Groupe de travail destinés aux fonctionnaires lors d'élections partielles étaient utiles. Selon lui, la question de savoir si le Groupe de travail doit être permanent dépendra des exigences imposées par le calendrier électoral.

David Vigneault, ancien directeur du SCRS, a déclaré qu'il était important d'adopter une approche plus large de l'ingérence étrangère, plutôt que d'avoir différents groupes qui ne l'examinent que dans certaines circonstances, comme une élection. Cependant, il n'est pas certain que le Groupe de travail constitue le moyen approprié pour traiter des questions plus larges d'ingérence étrangère, y compris la mésinformation, la désinformation ou les menaces contre les communautés issues des diasporas.

Par ailleurs, le Groupe de travail n'ayant pas été conçu à l'origine pour être un organe permanent, les témoins ont indiqué que le rendre permanent posait certains défis. Ceux-ci comprennent la structure actuelle de la présidence tournante et le roulement des membres, qui rend difficile l'établissement d'une mémoire institutionnelle. Le roulement des membres peut aussi complexifier l'établissement et le maintien de la confiance avec des partenaires extérieurs, comme les partis politiques.

Le gouvernement envisage de rendre le Groupe de travail permanent en établissant une présidence et un secrétariat administratif permanents. On m'a dit qu'il est probable qu'aucune décision définitive ne soit prise avant la publication de ce rapport.

Où situer le Groupe de travail permanent?

Si le Groupe de travail devait disposer d'un secrétariat permanent, une question serait de savoir où l'installer au sein du gouvernement. Le gouvernement y réfléchit encore. L'une des options est le Bureau du Conseil privé (BCP). Une autre est Sécurité publique Canada, auprès du coordonnateur national de la lutte contre l'ingérence étrangère (le « **CNLIE** »).

Plusieurs représentants du gouvernement ont fait remarquer qu'installer le Groupe de travail permanent au sein du BCP présentait des avantages et des inconvénients. Par exemple, le fait d'avoir le Groupe de travail au sein du BCP pourrait lui donner un certain degré d'influence. Toutefois, cela soulève des questions de dédoublement des fonctions et d'efficacité. De plus, M. Rogers a noté que le BCP n'est pas un ministère opérationnel alors que le Groupe de travail est une entité opérationnelle. En outre, la proximité avec l'échelon politique n'est peut-être pas idéale. Cependant, la proximité avec le cœur du gouvernement pourrait être bénéfique pour la gouvernance et la coordination du Groupe de travail.

Nathalie Drouin, actuelle conseillère à la sécurité nationale et au renseignement auprès du premier ministre (« CSNR »), et M. Rogers ont indiqué ne pas avoir de préférences quant à l'emplacement du Groupe de travail. M. Rogers a déclaré que la question la plus importante est de savoir s'il peut s'intégrer efficacement dans d'autres organes de décision.

Au moment de rédiger ce rapport, des discussions étaient en cours sur la question de la permanence du Groupe de travail, et le cas échéant, sur la manière de le structurer, et sur ce qu'il accomplirait. À la lumière des différents points de vue que j'ai entendus, je note qu'une attention particulière devrait être consacrée à la question de savoir si le Groupe de travail devrait surveiller chaque élection partielle ou plutôt ne surveiller que celles qu'il pense être susceptibles d'intéresser les acteurs de l'ingérence étrangère. Les ressources nécessaires pour surveiller une élection partielle sont importantes. Au vu de ce que j'ai appris tout au long des travaux de la Commission, je ne crois pas que le risque d'ingérence étrangère soit présent dans toutes les circonscriptions.

La surveillance de l'environnement numérique du Canada pour détecter la désinformation

À l'heure actuelle, aucune entité fédérale ne dispose d'un mandat particulier pour surveiller l'environnement numérique du Canada afin d'y détecter la désinformation en dehors des élections.

De nombreux témoins, y compris des représentants de Sécurité publique Canada, la CSNR, le greffier du Conseil privé et le sous-ministre des affaires étrangères, ont déclaré qu'il était nécessaire que le gouvernement soit en mesure d'effectuer cette surveillance et d'agir en fonction de ce qu'il apprend. Des témoins ont également relevé que la manière dont le gouvernement utilise cette information doit être étudiée avec soin, en tenant compte des obligations et risques juridiques applicables.

La question de la surveillance de l'environnement national de l'information recoupe, dans une certaine mesure, la question liée à la relation du gouvernement avec les organisations de la société civile, comme le Réseau canadien de recherche sur les médias numériques (RCRMN). Le greffier du Conseil privé, M. Hannaford, a déclaré que le gouvernement réfléchissait à la manière dont le Panel et le RCRMN interagiraient en période électorale. M^{me} Drouin a déclaré qu'il y avait une convergence d'intérêts et que le RCRMN pouvait apporter une valeur ajoutée en faisant la lumière sur une question tout en restant indépendant du gouvernement.

Qui surveillerait l'environnement numérique du Canada pour y détecter la désinformation?

Si le gouvernement devait surveiller l'environnement numérique national pour y détecter la désinformation pendant les élections ou tout au long de l'année, la question consisterait à savoir quelle entité gouvernementale pourrait s'en charger.

Le Mécanisme de réponse rapide du Canada (le MRR du Canada) fait partie du Groupe de travail en raison de sa capacité de surveillance numérique et de son expertise. Pendant les élections de 2019 et de 2021, le MRR du Canada a surveillé l'environnement numérique du Canada pour détecter la mésinformation et la désinformation en lien avec les élections. Il a soutenu le Groupe de travail avec des recherches et des analyses de source ouverte, et avec des informations provenant des partenaires du G7 sur l'évolution des tactiques d'ingérence étrangère. Comme je l'explique ci-dessus, il a fait le même travail pour les élections partielles à compter de juin 2023.

Bien que l'expertise du MRR du Canada soit considérée comme très utile pour le Groupe de travail, ce n'était pas la fonction que cette entité était censée remplir à l'origine. Comme je l'explique au **chapitre 11**, le MRR du Canada a été créé dans le cadre d'une initiative canadienne au sein du G7 visant à contrer les menaces à la démocratie. Son champ d'action est essentiellement international, et c'est pourquoi il fait partie d'AMC.

Plusieurs témoins se sont demandé pourquoi AMC, qui après tout est le ministère des Affaires « étrangères », devait être responsable de la surveillance de l'environnement domestique de l'information en ligne. Et comme je l'ai indiqué plus tôt dans ce chapitre, le travail du MRR du Canada en période électorale se fait au prix d'une réduction de sa capacité à se concentrer sur son mandat habituel. Des préoccupations ont été exprimées aux échelons supérieurs du gouvernement quant au fait que son rôle au sein du Groupe de travail n'est pas conforme à son mandat.

Plusieurs des témoins d'AMC ont fait remarquer que, même si on retirait la responsabilité de la surveillance de l'environnement domestique de l'information du MRR du Canada, celui-ci pourrait continuer à faire partie du Groupe de travail. Cela permettrait au Groupe de travail de savoir ce que le MRR du Canada et ses partenaires du G7 constatent sur la scène internationale, sans que ses ressources soient détournées de la surveillance de l'environnement international de l'information.

Je comprends que des discussions sont en cours sur le renforcement des capacités de surveillance domestique au sein d'autres ministères, comme Sécurité publique Canada ou le BCP, mais la question demeure à l'étude.

Le sous-ministre de la Sécurité publique, Shawn Tupper (maintenant retraité), a suggéré qu'une possibilité serait d'élargir le champ d'action du Centre des opérations du gouvernement de Sécurité publique Canada, une direction générale du ministère qui assure la coordination de l'ensemble du gouvernement pour la gestion des situations d'urgence. Le Centre des opérations du gouvernement contribue à répondre aux événements liés à la sécurité nationale, notamment en faisant appel à d'autres ministères et à d'autres compétences. Il est informé grâce à des liens étroits avec les secteurs d'intervention d'urgence provinciaux, territoriaux et municipaux.

Une meilleure communication publique de la part du gouvernement

L'un des principaux enseignements tirés du rapport après-action (RAA) de 2021 du Groupe de travail est que la communication est un outil essentiel pour répondre à l'ingérence étrangère. Le Groupe de travail a noté que la communication a représenté un défi avant et pendant les élections de 2021. Par exemple, le fait que le gouvernement n'ait pas fait connaître de manière proactive ses efforts pour protéger les élections a suscité des critiques sur ce que certains ont perçu comme un manque d'action.

Le Groupe de travail a recommandé au gouvernement de revoir son plan de communication. La sous-secrétaire du cabinet (Gouvernance) du BCP a reconnu la valeur de communications plus fréquentes avec les Canadiennes et les Canadiens pour « normaliser les communications » dans la sphère électorale et accroître la confiance envers les processus électoraux fédéraux.

L’interaction avec les partis politiques

Interagir efficacement avec les partis politiques au sujet de l’ingérence étrangère est un enjeu épineux que j’aborde plus en détail au chapitre 15 (volume 4). Dans cette section-ci, j’aborde la relation précise qui existe entre le Groupe de travail et les partis politiques.

Avec l’aide du Secrétariat des institutions démocratiques du BCP (le SID du BCP), le Groupe de travail a proposé des breffages non classifiés aux représentants des partis politiques pour presque toutes les élections partielles depuis juin 2023. Peu de personnes y ont assisté. Seuls le Nouveau Parti démocratique du Canada (le « **NPD** ») et le Bloc Québécois ont assisté aux breffages pour les élections partielles de juin 2023. Quant aux breffages précédant les élections partielles de mars et de juin 2024, seul le NPD y a assisté.

Le directeur exécutif du Parti conservateur du Canada a déclaré qu’il n’était pas au courant que son parti avait été invité à ces breffages. Des représentants du Parti vert du Canada ont affirmé qu’ils ignoraient l’existence des breffages. Des témoins gouvernementaux ont indiqué que, de manière générale, tous les principaux partis politiques qui participaient aux élections partielles ont été invités. Le directeur national du Parti libéral du Canada a déclaré qu’il était au courant des breffages, mais supposait qu’ils n’offriraient rien de nouveau parce qu’ils n’étaient pas classifiés. Il s’est dit que, s’il y avait des informations que son parti devait savoir, ces informations seraient classifiées, ou alors le gouvernement ferait plus d’efforts pour attirer son attention.

À la suite du breffage des partis politiques en juin 2023, le BCP a conclu qu’il n’y avait pas suffisamment d’exemples concrets d’ingérence étrangère et que le breffage n’avait « pas atteint sa cible ». Ce breffage, selon lui, n’a pas répondu aux attentes des partis. Le Groupe de travail a alors discuté de la nécessité de trouver et d’incorporer des exemples concrets d’ingérence étrangère dans les breffages.

On m’a dit que des efforts avaient été faits pour réviser ces breffages, notamment avec des exemples concrets d’ingérence étrangère possible au Canada provenant de sources ouvertes, dont certains sont même tirés du Rapport initial de la Commission. Toutefois, compte tenu du faible niveau de participation des partis politiques, il n’est pas encore certain que ce contenu révisé soit utile.

Le Groupe de travail a aussi organisé des breffages classifiés à l’intention des représentants des partis politiques bénéficiant d’une autorisation de sécurité pendant les élections générales. Les breffages de niveau « Secret » permettent de partager un plus grand nombre d’informations, bien que, comme je l’explique au chapitre 15 (volume 4), les partis politiques puissent être limités dans ce qu’ils peuvent faire avec ce qu’ils apprennent.

Les plateformes en ligne

Plus tôt dans ce chapitre, j'ai mentionné la Déclaration du Canada sur l'intégrité électorale en ligne (Déclaration). Après les élections de 2019, le ministre des Institutions démocratiques de l'époque, Dominic LeBlanc, a conclu que la Déclaration avait été efficace. Elle a ainsi été renouvelée pour les élections de 2021. Actuellement, le Secrétariat des institutions démocratiques du BCP (SID du BCP) conseille le ministre des Institutions démocratiques pour déterminer si le Canada devrait renouveler la Déclaration pour les prochaines élections générales, et déterminer quels changements devraient y être apportés pour la mettre à jour ou ajouter de nouveaux signataires.

Au sujet de l'élargissement de l'éventail des signataires, le secrétaire adjoint du cabinet, Allen Sutherland, a indiqué que le SID du BCP avait approché Tencent, la société mère de WeChat, et qu'une discussion générale avait eu lieu au sujet de la plateforme, de même que sur son intérêt à devenir signataire. À ce jour, WeChat n'a pas signé la Déclaration.

En raison de l'évolution rapide de l'environnement des plateformes de médias sociaux, le SID du BCP étudie la possibilité que le Canada interagisse avec les entreprises de médias sociaux à titre de membre d'un groupe de démocraties plutôt que de manière isolée. La Commission a entendu dire que les entreprises de médias sociaux, en particulier les plus grandes, sont parfois peu disposées à coopérer avec des pays relativement petits qui tentent de les réglementer.

La Déclaration est un accord volontaire. Une autre option pour traiter avec les plateformes de médias sociaux serait la réglementation. Le gouvernement a envisagé cette avenue, mais a également noté qu'une telle approche soulève des questions quant à la possibilité de réglementer la censure et la liberté d'expression.

Néanmoins, le gouvernement a commencé à réglementer les médias sociaux et certains contenus en ligne. En 2023, il a modifié la *Loi sur la radiodiffusion* pour réglementer les services de diffusion en continu étrangers. Le Conseil de la radiodiffusion et des télécommunications canadiennes (le « **CRTC** ») utilise les contributions provenant de ces services pour un fonds d'information destiné à soutenir les médias indépendants.

Par ailleurs, en vertu de la *Loi sur les nouvelles en ligne*, si une plateforme de médias sociaux répond à certains critères, elle doit en informer le gouvernement et négocier avec les entreprises de presse dont elle affiche le contenu. Pour ceux qui ne veulent pas négocier avec les médias, le CRTC peut accorder une exemption en échange d'une contribution financière[16].

La *Loi sur les préjudices en ligne* (projet de loi C-63), telle que proposée, aurait imposé aux plateformes de médias sociaux l'obligation de réduire les

[16] Par exemple, Google fournit 100 millions de dollars que le CRTC utilisera pour renforcer les organisations journalistiques canadiennes.

risques de préjudice liés à sept catégories de contenu, qui pourraient inclure certaines formes de mésinformation et de désinformation. La raison d'être du projet de loi C-63 était la diminution des efforts des plateformes pour modérer leurs contenus. Les laisser en charge de la modération peut donc causer des dommages. La loi proposée aurait exigé que les plateformes soient responsables de certains préjudices identifiés par la loi et qu'elles aient l'obligation de les atténuer. Le projet de loi C-63 aurait aussi autorisé le gouvernement à ordonner aux plateformes de médias sociaux de donner accès aux chercheurs à leurs ensembles de données et à leurs informations. Avec la prorogation du Parlement le 6 janvier 2025, le projet de loi C-63 est mort au feuilleton.

12.3 La Stratégie de lutte contre les activités hostiles parrainées par des États

Le Plan n'était pas le seul ensemble d'initiatives politiques que le Canada a poursuivi pour répondre aux menaces d'ingérence étrangère. À partir de 2018, le gouvernement a entamé des efforts parallèles pour élaborer une Stratégie de lutte contre les activités hostiles parrainées par les États (la Stratégie AHPE).

L'origine de la Stratégie AHPE

En juillet 2018, Sécurité publique Canada a été chargée de diriger les travaux sur une Stratégie interministérielle de lutte contre les AHPE[17]. L'objectif global était d'établir les bases d'une approche des AHPE impliquant l'ensemble de la société et du gouvernement en s'appuyant sur la communauté de la sécurité et du renseignement et sur d'autres partenaires, y compris des entités privées et d'autres autorités gouvernementales. Dans le cadre de ces travaux, Sécurité publique Canada a noté que la version publique de la Stratégie AHPE pourrait faire partie d'une approche plus large des communications destinées à renforcer la connaissance de la menace au sein de la population canadienne.

Une brève esquisse d'une stratégie AHPE a vu le jour quelques mois plus tard. À partir d'une évaluation de l'intérêt national et de la vulnérabilité globale à

[17] Les AHPE englobent toute tentative d'un État étranger, ou de ses mandataires, de compromettre les intérêts nationaux du Canada et ceux de ses alliés proches, dans le but de promouvoir ses propres intérêts. Ces tentatives peuvent aller au-delà de la conduite habituelle des affaires d'État, remettre en cause l'ordre fondé sur les règles ou chercher délibérément à demeurer ambiguës. Les AHPE englobent les actions qui sont trompeuses, coercitives, corruptrices, secrètes ou illégales, mais qui se situent en deçà du seuil d'un conflit armé.

l'égard des AHPE, elle définissait cinq secteurs prioritaires, à savoir les processus démocratiques et les institutions gouvernementales, la prospérité économique, les affaires internationales et la défense, la cohésion sociale et les infrastructures critiques.

Dans son rapport annuel de 2019, le Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) a recommandé au gouvernement d'élaborer une stratégie globale sur l'ingérence étrangère. Le CPSNR a qualifié les réactions du gouvernement face à l'ingérence étrangère de « ponctuelles et au cas par cas ». Il a noté que les membres de la communauté de la sécurité et du renseignement différaient sur la façon de définir le problème et sur la façon de comprendre sa gravité et sa prévalence.

Le CPSNR a conclu qu'il manquait de coordination et de collaboration interministérielles en matière d'ingérence étrangère et que la capacité du Canada de faire face à cette ingérence était limitée en raison de l'absence d'une approche globale visant à prendre en compte les risques pertinents, les outils appropriés et les répercussions possibles des réponses aux comportements des États. Le CPSNR a également noté l'absence d'une stratégie publique en matière d'ingérence étrangère semblable à celles qui existent pour le terrorisme et la cybersécurité.

Après les élections générales de 2019, Bill Blair, alors ministre de la Sécurité publique, a demandé à son ministère de continuer à travailler à l'élaboration d'une stratégie de lutte contre les AHPE.

Rob Stewart, sous-ministre de la Sécurité publique de décembre 2019 à octobre 2022, a déclaré que l'avancement d'un tel plan implique un processus complexe et non linéaire de consultation et d'approbation au sein du gouvernement, ce qui représente toujours un certain défi.

Dominic Rochon, sous-ministre adjoint du Secteur de la sécurité nationale et de la cybersécurité à Sécurité publique Canada d'octobre 2019 à octobre 2022, a ajouté qu'une partie du défi résidait dans le fait que la Stratégie AHPE englobait non seulement l'ingérence étrangère, mais aussi tout un ensemble d'activités et de domaines dans lesquels les États hostiles agissent, comme la sécurité économique. Le processus impliquait donc un grand nombre de ministères et d'organismes, chacun ayant ses propres besoins et outils législatifs à ajuster.

J'ai ainsi appris que la Stratégie AHPE était une entreprise de vaste envergure qui a fait l'objet de nombreuses discussions, notamment au sein du Comité des sous-ministres sur la sécurité nationale (voir le **chapitre 11**), et qui a été ajustée à maintes reprises. Une question particulièrement épineuse concernait la gouvernance et la coordination, y compris la création d'un poste de coordonnateur chargé de la lutte contre les AHPE. De l'avis général, un coordonnateur était nécessaire, mais il n'y avait pas de consensus sur l'endroit où il devrait être installé – à la Sécurité publique, au BCP ou ailleurs.

La preuve montre qu'un autre défi dans l'avancement de la Stratégie AHPE a été la quantité d'autres priorités auxquelles Sécurité publique Canada était

confrontée à l'époque. De nombreuses questions liées à la pandémie de COVID-19 lui incombaient, et le ministère devait aussi composer avec les retombées de l'événement malheureux ayant entraîné de nombreux décès en Nouvelle-Écosse.

Le mémoire au Cabinet sur les AHPE

Marco Mendicino est devenu ministre de la Sécurité publique après les élections générales de 2021. Il a déclaré que sa priorité absolue en ce qui concerne l'ingérence étrangère était de faire avancer la Stratégie AHPE par un mémoire au Cabinet (le « **mémoire AHPE** »).

En mai 2022, le ministre Mendicino a présenté le mémoire AHPE au Cabinet. Ce mémoire s'intéressait à la question de savoir si le gouvernement devait prendre des mesures initiales pour moderniser l'approche du Canada en matière de lutte contre les AHPE. Les mesures proposées incluaient l'amélioration des approches en matière de politiques, le renforcement de la coordination, l'amélioration des outils législatifs et le développement de nouvelles capacités pour contrer les menaces.

Le mémoire AHPE recommandait d'approuver les secteurs prioritaires définis dans la Stratégie AHPE, que j'ai décrite précédemment.

Diverses mesures ont été recommandées, y compris l'amélioration des outils législatifs, la création de nouvelles capacités et la mise en place d'une approche de communication stratégique :

- L'approbation des principes, des secteurs prioritaires et des piliers énoncés dans la Stratégie AHPE pour guider les mesures fédérales actuelles et futures relativement aux AHPE.
- La mise en œuvre par le ministère de la Sécurité publique d'une approche stratégique de communication à l'échelle du gouvernement, qui inclurait la mobilisation auprès des intervenants nationaux, y compris les membres des communautés issues des diasporas qui sont vulnérables aux effets néfastes des AHPE.
- L'examen des améliorations à apporter aux outils législatifs afin de garantir la capacité du Canada à détecter et à contrer les menaces d'AHPE en menant des consultations sur des modifications potentielles à un certain nombre de lois.
- L'élaboration de nouvelles capacités et la conduite de nouvelles activités par la GRC.
- L'élargissement du rôle de coordination de la Sécurité publique en lien avec les activités gouvernementales de lutte contre les AHPE afin de contribuer à la mise en œuvre de la Stratégie AHPE.

Je note que la Stratégie AHPE et le mémoire AHPE ont une portée beaucoup plus large que le mandat de la Commission. Les aspects du mémoire au

Cabinet qui touchent les processus et les institutions démocratiques font cependant partie de son mandat.

Le Cabinet a ratifié le mémoire AHPE en juin 2022. Cette ratification est intervenue près de quatre ans après le début des travaux d'élaboration d'une stratégie de lutte contre les AHPE.

M. Stewart a affirmé que l'approbation du mémoire AHPE par le Cabinet constituait essentiellement une autorisation à poursuivre le travail en consultant les Canadiennes et les Canadiens sur la boîte à outils et les modifications législatives proposées.

Les développements après la ratification du mémoire AHPE

M. Mendicino a déclaré qu'à partir du moment où le Cabinet a ratifié le mémoire AHPE en juin 2022, Sécurité publique Canada s'est concentrée sur sa mise en œuvre. Il a précisé qu'il était impatient que le mémoire AHPE se concrétise, mais que cela avait pris un certain temps, car Sécurité publique Canada avait besoin d'une réponse de l'ensemble du gouvernement pour faciliter le dialogue avec le public et répondre aux préoccupations selon lesquelles le mémoire AHPE pourrait aller trop loin, aller à l'encontre de la *Charte* ou être discriminatoire à l'égard des communautés issues des diasporas. De plus, la mise en œuvre s'est déroulée sur fond de pandémie de COVID-19, d'invasion de l'Ukraine par la Russie, de « Convoi de la liberté » et, plus tard, de la Commission sur l'état d'urgence.

De plus, comme je l'ai expliqué au **chapitre 11**, le débat s'est poursuivi au sein du gouvernement sur la question de savoir où installer le coordonnateur national de la lutte contre l'ingérence étrangère (le CNLIE) au sein de Sécurité publique Canada ou du BCP.

En mars 2023, le poste de CNLIE a finalement été créé au sein de Sécurité publique Canada. Le financement a suivi dans le budget 2023, mais avant qu'il ne soit accessible, Sécurité publique Canada a dû réaffecter des ressources préexistantes afin de soutenir le travail du CNLIE. Ce travail comprenait la coordination, la gestion des relations avec les alliés et la conduite du travail lié aux politiques et aux consultations qui aboutiraient finalement à la *Loi sur la lutte contre l'ingérence étrangère* (le projet de loi C-70, que j'aborde ci-dessous).

Au printemps 2023, Sécurité publique Canada a lancé une première série de consultations publiques sur d'éventuelles modifications législatives. Cela s'est limité à sonder les réactions au registre des agents étrangers.

Certains craignaient qu'un registre ne stigmatise les Canadiennes et les Canadiens d'origine chinoise, notamment en raison du racisme anti-asiatique résultant de la pandémie. C'est cette crainte qui a motivé la décision de ne

pas lier le registre à un pays particulier, ce qui signifie que les obligations de déclaration liées à la loi n'établissaient pas de distinction entre les différents pays. Les réactions lors des consultations ont été généralement positives à l'endroit d'un registre.

Une deuxième série de consultations a débuté à l'automne 2023, pendant le mandat à titre de ministre de la Sécurité publique de Dominic LeBlanc. Ces consultations portaient sur les autres modifications législatives qui ont finalement été incluses dans le projet de loi C-70.

Les deux séries de consultations ont consisté à recueillir des commentaires écrits et à organiser des tables rondes avec les parties prenantes, notamment des universitaires, des groupes d'intérêts, des gouvernements autochtones et des membres de différentes communautés. Les responsables des consultations ont reçu une rétroaction détaillée. De l'avis général, l'ingérence étrangère était un problème grave et les outils du Canada devaient être adaptés.

Après les consultations, les modifications législatives proposées ont été présentées une nouvelle fois au Cabinet, avant que le projet de loi ne soit présenté au Parlement.

Patrick Travers, conseiller principal, Affaires mondiales, auprès du premier ministre, a affirmé que le temps qui a été nécessaire pour mettre en œuvre ces modifications législatives doit être considéré à la lumière des leçons tirées des initiatives législatives précédentes traitant de questions liées à la sécurité nationale. La tentative du gouvernement précédent de réformer l'architecture de la sécurité nationale s'est heurtée à une opposition importante et, après le changement du parti au pouvoir, cette architecture a été remodelée pour devenir la *Loi de 2017 sur la sécurité nationale*. Toute loi touchant aux pouvoirs principaux des agences de sécurité nationale, à leur supervision et aux droits des Canadiennes et des Canadiens est particulièrement délicate et doit être examinée très attentivement.

Le premier ministre a témoigné que c'est la raison pour laquelle il y a eu plusieurs séries de consultations auprès de différentes communautés issues des diasporas et de différents groupes de parties prenantes, et que la loi a été renvoyée plusieurs fois au Cabinet. Il a déclaré qu'il était important de trouver le bon équilibre. Le premier ministre et ses collaborateurs sont d'avis que le large soutien au projet de loi C-70, non seulement au Parlement, mais aussi au sein de la société civile, montre que le travail effectué avant la présentation du projet de loi a permis de créer le consensus nécessaire.

La *Loi sur la lutte contre l'ingérence étrangère* (projet de loi C-70)

Après les deux séries de consultations, le projet de loi C-70 a été présenté à la Chambre des communes le 6 mai 2024 et a reçu la sanction royale le 20 juin 2024. Il est devenu la *Loi sur la lutte contre l'ingérence étrangère*.

Cette loi a modifié la *Loi sur le Service canadien du renseignement de sécurité* (la « ***Loi sur le SCRS*** ») avec effet immédiat, tandis que les changements apportés au *Code criminel*, à la *Loi sur la preuve au Canada* et à la *Loi sur la protection de l'information* (désormais, la *Loi sur l'ingérence étrangère et la protection de l'information* ou la « ***LIEPI*** ») sont entrés en vigueur le 19 août 2024. Elle a créé également un registre pour la transparence en matière d'influence étrangère, qui prendra environ un an à mettre en place, selon l'estimation des fonctionnaires de Sécurité publique Canada. Les principaux éléments de la *Loi sur la lutte contre l'ingérence étrangère* sont examinés ci-dessous.

Modifications à la *Loi sur le SCRS*

La *Loi sur le SCRS* a fait l'objet de plusieurs modifications importantes.

Mandat élargi en matière de renseignement étranger

Le SCRS peut prêter assistance au ministre des Affaires étrangères ou au ministre de la Défense afin de recueillir des informations ou du renseignement portant sur les capacités, les intentions ou les activités d'États étrangers ou de non-Canadiennes et non-Canadiens au Canada. Cette collecte doit avoir lieu « au Canada ». Cette limite territoriale causait des difficultés opérationnelles au SCRS en raison d'une série de décisions de la Cour fédérale, qui interprétaient cette limite comme signifiant que le SCRS ne pouvait pas recueillir des informations situées hors du Canada, par exemple des informations hébergées sur des serveurs à l'extérieur du pays. La *Loi sur le SCRS* a donc été modifiée afin de faire une distinction entre l'endroit où la collecte a lieu (au Canada) et l'endroit où se trouve l'information qui est recueillie (qui peut être à l'extérieur du Canada). Grâce à cette modification, le SCRS peut maintenant recueillir, au Canada, du renseignement étranger situé hors du Canada ou visant une personne ou une chose qui se trouvait au Canada, mais se situe temporairement hors du Canada.

Échange d'informations

Le SCRS avait un pouvoir limité pour divulguer certains types d'informations à des entités extérieures au gouvernement fédéral. Avec les modifications, le SCRS peut désormais divulguer des informations à toute personne ou entité extérieure au gouvernement fédéral afin de renforcer la résilience face aux menaces à la sécurité du Canada. Cela lui permet de divulguer de

l'information qu'il juge importante pour aider à contrer des menaces comme l'ingérence étrangère. Avant de pouvoir partager ces informations, le SCRS doit d'abord les avoir transmises à un ministère ou à un organisme fédéral dont les tâches et les fonctions sont liées à ces informations. Les informations ne peuvent pas inclure des renseignements personnels sur des citoyens canadiens, des résidents permanents ou des personnes au Canada (autres que le destinataire de l'information) ni le nom d'entités canadiennes, comme le nom d'une société canadienne (à moins que la société ne soit le destinataire).

Nouveaux pouvoirs de perquisition et de saisie

La *Loi sur le SCRS* contenait une disposition relative aux mandats, de portée générale, inspirée de la législation en matière d'écoute électronique. Le SCRS dispose maintenant d'un certain nombre de nouveaux outils qu'il peut utiliser avec l'autorisation de la Cour fédérale. Ceux-ci incluent une ordonnance obligeant une personne ou une entité à conserver des objets en sa possession ou sous son contrôle, une ordonnance obligeant une personne ou une entité à remettre au SCRS des objets en sa possession ou sous son contrôle, et un mandat à usage unique autorisant le SCRS à prendre certaines mesures, une seule fois, pour obtenir des informations, des dossiers, des documents ou d'autres choses.

Des témoins ont aussi déclaré qu'il était nécessaire de moderniser la *Loi sur le SCRS* en raison des changements technologiques et sociétaux importants survenus depuis son adoption en 1984. Les dispositions modifiées sur les ensembles de données, un grand nombre des nouveaux pouvoirs relatifs aux mandats et la portée élargie des enquêtes sur le renseignement étranger sont tous liés à l'environnement numérique moderne.

Un autre élément important était le fait que les acteurs menaçants se livrent à un éventail beaucoup plus large d'activités et ciblent une gamme beaucoup plus large d'institutions canadiennes. L'élargissement des pouvoirs du SCRS en matière de divulgation d'informations est particulièrement significatif, car le gouvernement fédéral n'est pas la seule cible des acteurs hostiles. Les provinces et les territoires, les gouvernements autochtones, les municipalités, les établissements de recherche et le secteur privé sont également tous des cibles.

La *Loi sur le SCRS* telle qu'adoptée en 1984 n'anticipait pas cela, et restreignait le pouvoir du SCRS de divulguer des informations à l'extérieur du gouvernement fédéral. Les dispositions introduites en 2015 et permettant au SCRS de prendre des mesures pour réduire les menaces à la sécurité du Canada – que j'aborde au **chapitre 11** – ont été utilisées par le SCRS pour partager des informations sensibles. Les modifications de 2024 accordent au SCRS un pouvoir plus direct et plus largement applicable pour le faire.

Les modifications à la *Loi sur l'ingérence étrangère et la protection de l'information* (*LIEPI*)

La *Loi sur la lutte contre l'ingérence étrangère* a modifié la *Loi sur la protection de l'information*, désormais appelée la « *LIEPI* », en modifiant les infractions existantes ou en en créant de nouvelles :

- **Intimidation pour le compte d'une entité étrangère** : Criminalisation de l'intimidation pour le compte d'une entité étrangère. Les menaces ou la violence constituaient déjà des infractions.
- **Commission d'un acte criminel pour le compte d'une entité étrangère** : Nouvelle infraction consistant à commettre un acte criminel (p. ex., un vol ou une fraude) sous la direction d'une entité étrangère, au profit de celle-ci ou en association avec elle.
- **Conduite trompeuse ou subreptice pour une entité étrangère** : Une nouvelle infraction générale d'ingérence étrangère est commise lorsqu'une personne adopte sciemment une conduite subreptice ou trompeuse ou omet, subrepticement ou dans l'intention de tromper, de faire quoi que ce soit sur l'ordre d'une entité étrangère, au profit de celle-ci ou en association avec elle. Cette infraction s'applique si la personne agit dans un but préjudiciable à la sécurité ou aux intérêts du gouvernement canadien, ou si elle ne se soucie pas de savoir si son comportement portera vraisemblablement atteinte aux intérêts canadiens.
- **Ingérence politique pour le compte d'une entité étrangère** : Nouvelle infraction consistant à adopter un comportement subreptice ou trompeur sur l'ordre d'une entité étrangère ou en association avec elle, dans l'intention d'influencer un processus politique ou gouvernemental canadien ou d'influencer l'exercice d'un droit démocratique au Canada. Cette infraction comprend le fait d'influencer l'investiture de candidats ou l'élaboration de programmes électoraux par les partis politiques.

La nouvelle infraction d'ingérence politique est particulièrement pertinente pour l'ingérence étrangère dans les institutions démocratiques, y compris les processus électoraux. Elle s'applique aux processus gouvernementaux et politiques à tous les niveaux de gouvernement, à la fois pendant et entre les élections. Elle concerne les processus des partis politiques, impliquant non seulement les courses à l'investiture et à la direction, mais aussi des processus comme l'élaboration des programmes des partis.

Ces infractions sont toutes punissables d'une peine maximale d'emprisonnement à perpétuité. Les peines maximales pour les actes préparatoires aux infractions selon la *LIEPI* sont passées de deux à cinq ans.

Modifications au *Code criminel*

Le projet de loi C-70 a modifié l'infraction de sabotage contenue au *Code criminel* en la recentrant sur les actes commis dans l'intention de mettre en péril la sécurité du Canada. Il a également créé une nouvelle infraction de sabotage destinée à protéger les infrastructures essentielles du Canada ainsi que la santé et la sécurité du public. Il est désormais interdit de fabriquer, de vendre ou de posséder des dispositifs destinés à être utilisés pour commettre des actes de sabotage.

La *Loi sur la transparence et la responsabilité en matière d'influence étrangère*

La *Loi sur la transparence et la responsabilité en matière d'influence étrangère* (la « ***LTRIE*** ») crée un registre pour la transparence en matière d'influence étrangère, qui est un nouveau régime réglementaire destiné à promouvoir la transparence des activités exercées pour le compte de commettants étrangers. Inspirée en partie par les régimes d'autres pays, la *LTRIE* établit un régime nouveau et quelque peu complexe au Canada. Comme je l'ai indiqué plus haut, cette loi n'est pas encore en vigueur et certains de ses aspects importants seront définis dans des règlements qui n'ont pas encore été rédigés. Je vais donc seulement fournir un résumé de haut niveau des principaux aspects de la loi.

La *LTRIE* exige que les personnes ou les entités qui concluent des arrangements avec un commettant étranger pour entreprendre ou mener certaines activités à l'égard d'un processus politique ou gouvernemental au Canada s'enregistrent. Cela inclut les situations où une personne accepte de communiquer avec le titulaire d'une charge publique, de distribuer de l'argent ou de diffuser des informations, y compris sur les médias sociaux, sur l'ordre d'un commettant étranger ou en association avec lui. Les commettants étrangers comprennent les États étrangers ou les entités qu'ils contrôlent.

À l'appui de ce projet, la *LTRIE* crée le poste de commissaire à la transparence en matière d'influence étrangère, dont le rôle consiste notamment à tenir un registre public contenant des informations sur les arrangements avec l'étranger. Le commissaire sera nommé pour un maximum de sept ans par le gouverneur en conseil (le Cabinet et le gouverneur général) après consultation des groupes reconnus au Sénat et des partis d'opposition. Il dispose de pouvoirs d'enquête pour faire respecter l'obligation d'enregistrement. Les violations des exigences de la *LTRIE* peuvent donner lieu à des poursuites judiciaires ou à l'imposition de sanctions administratives pécuniaires.

Les nouvelles règles pour la divulgation et la prise en compte d'informations sensibles dans les procédures devant la Cour fédérale

La *Loi sur la lutte contre l'ingérence étrangère* (LIEPIE) crée de nouvelles règles dans la *Loi sur la preuve au Canada* concernant le traitement des informations sensibles dans une série de procédures judiciaires devant la Cour fédérale. Le régime des « instances sécurisées de contrôle des décisions administratives » permet aux juges de la Cour fédérale d'examiner des informations sensibles dans le cadre d'une procédure de contrôle judiciaire sans que la personne qui conteste l'action gouvernementale ne soit autorisée à les voir. À la place, un avocat bénéficiant d'une habilitation de sécurité peut être désigné pour représenter les intérêts de la personne et accéder aux informations sensibles en question. Ces règles remplacent de nombreux régimes individuels qui existaient sous différentes lois et s'appliqueront au contrôle judiciaire des décisions rendues par le commissaire à la transparence en matière d'influence étrangère.

Les développements ultérieurs

Comme nous l'avons vu plus haut, certains éléments importants du mémoire AHPE sont allés de l'avant avec l'introduction du projet de loi C-70. Le projet de loi C-70 comprenait toutes les modifications à la *Loi sur le SCRS*, à la *LIEPI* et au *Code criminel* qui faisaient partie du processus de consultation publique, ainsi que la création d'un processus général de procédures sécurisées de contrôle des décisions administratives selon la *Loi sur la preuve au Canada*. Deux des six éléments relatifs au problème de l'utilisation du renseignement comme preuve (voir le chapitre 5, volume 2) qui faisaient partie des consultations ont été inclus, à savoir en limitant les appels de certaines ordonnances de divulgation après le procès et en permettant l'octroi d'ordonnances de mise sous scellés pour des raisons de sécurité nationale.

Le gouvernement reconnaît que, pour moderniser complètement la boîte à outils du Canada en matière d'ingérence étrangère, d'autres changements législatifs sont nécessaires, et il étudie les outils supplémentaires à mettre en place.

Une Stratégie AHPE publique

Comme indiqué plus haut, le gouvernement souhaitait que la Stratégie AHPE soit dotée d'une composante publique. Ainsi que l'a expliqué Tricia Geddes, actuellement sous-ministre de la Sécurité publique[18], l'objectif était de

[18] Pendant les travaux de la Commission, Tricia Geddes était sous-ministre adjointe à Sécurité publique Canada. Elle est devenue sous-ministre le 31 octobre 2024.

donner aux Canadiennes et aux Canadiens une idée générale de la menace et des moyens mis en œuvre par le gouvernement pour y faire face. Une stratégie publique n'a pas été finalisée avant le mémoire AHPE.

En novembre 2022, les premières fuites médiatiques sur l'ingérence étrangère ont eu lieu. En réponse, M. Mendicino, alors ministre de la Sécurité publique, a demandé au cabinet du premier ministre de l'aider à faire avancer le mémoire AHPE et à résoudre les débats en cours sur la communication d'une stratégie publique.

Le 14 juin 2023, Shawn Tupper, alors sous-ministre de la Sécurité publique, a envoyé un mémoire au ministre Mendicino intitulé « Stratégie canadienne de lutte contre l'ingérence étrangère ». Ce mémoire expliquait que la Stratégie AHPE serait renommée, délaissant le terme « AHPE » au profit de celui d'« ingérence étrangère ». Il s'agissait de montrer clairement au public que la Stratégie AHPE visait l'ingérence étrangère, ce qui correspondait mieux au langage utilisé par les médias à l'époque. En substance, le changement de nom reflétait un repositionnement de la Stratégie AHPE.

Le ministre Mendicino n'a pas approuvé la Stratégie de lutte contre l'ingérence étrangère avant que le ministre LeBlanc ne le remplace en juillet 2023. Sécurité publique Canada a alors demandé au ministre LeBlanc d'approuver une version publique de la Stratégie. Un mémoire adressé au ministre LeBlanc en vue d'obtenir cette approbation décrivait par ailleurs les travaux en cours sur une version classifiée de la Stratégie de lutte contre l'ingérence étrangère.

Le ministre LeBlanc a déclaré que l'évolution rapide du discours politique sur l'ingérence étrangère au Canada avait conduit à la mise en veilleuse de la Stratégie. Lui-même, ainsi que d'autres témoins, ont également déclaré que les fuites médiatiques avaient rendu difficile le fait de trouver les moyens les plus efficaces de communiquer avec le public au sujet de l'ingérence étrangère. Avec la nomination du rapporteur spécial indépendant sur l'ingérence étrangère et, plus tard, ma propre nomination pour mener une enquête publique, le gouvernement a décidé d'attendre mes recommandations avant de finaliser une stratégie. M^{me} Geddes a fait remarquer que la plupart des éléments de la Stratégie sur l'ingérence étrangère ont finalement été communiqués au public dans le cadre des consultations qui ont mené au projet de loi C-70.

Comme indiqué ci-dessus, le mémoire AHPE est l'une des deux réponses clés du gouvernement en matière de politiques visant l'ingérence étrangère, l'autre étant le Plan pour protéger la démocratie canadienne (Plan). Le mémoire AHPE proposait deux stratégies : une stratégie relative aux AHPE à l'échelle du gouvernement et une stratégie de communication et de mobilisation. Le gouvernement souhaitait également que la Stratégie AHPE ait un élément de communication avec le public. Six ans se sont écoulés depuis que le gouvernement a commencé à élaborer ces stratégies et plus de deux ans se sont écoulés depuis la ratification du mémoire AHPE. À ce jour, il n'existe aucun document, qu'il soit public ou interne, qui présente de

manière complète la stratégie du gouvernement en matière de lutte contre l'ingérence étrangère.

Les témoins considéraient encore qu'avoir une stratégie interne et orientée vers le public aurait une valeur. Ils m'ont dit que des travaux sont en cours à ce sujet. M^{me} Geddes a indiqué que le travail actuel du coordonnateur national de la lutte contre l'ingérence étrangère (CNLIE) représente un aspect clé de cet effort.

Étant donné que le mandat de la Commission se limite à l'ingérence étrangère dans les processus et institutions démocratiques, mon enquête ne s'est pas concentrée sur d'autres secteurs envisagés par le mémoire AHPE, notamment les infrastructures critiques, la prospérité économique ou la sécurité de la recherche. Ainsi, je ne suis pas nécessairement au courant des initiatives que le gouvernement a pu prendre en lien avec ces autres secteurs.

Cela dit, il m'apparaît nettement que le sort de la Stratégie AHPE illustre bien un problème que j'ai observé plus d'une fois au cours des travaux de la Commission. Le gouvernement consacre souvent beaucoup de temps et d'énergie à consulter, coordonner et discuter de mesures proposées avec les parties prenantes (qui sont souvent nombreuses), sans toutefois que ce processus ne débouche sur des actions concrètes et ultimement sur la mise en œuvre des mesures envisagées. Au lieu de cela, des mesures sont souvent mises en œuvre soudainement, en réponse à un événement qui met en lumière leur absence, ou ne sont tout simplement jamais mises en œuvre.

Il est difficile de mettre le doigt sur les raisons qui expliquent ce phénomène.

Je comprends que l'appareil gouvernemental fédéral est vaste et complexe, et que nous ne pouvons pas nous attendre à ce qu'il soit très agile. Cela dit, il serait probablement avantageux et plus efficace de désagréger les initiatives qui ratissent large en éléments plus faciles à manœuvrer, plus ciblés et qui n'impliquent pas autant de parties prenantes ni, par conséquent, autant de processus et de consultations. Comme le veut l'expression, « qui trop embrasse mal étreint ». Ces initiatives devraient évidemment être cohérentes entre elles, mais il incombe à une autorité centrale d'assurer cette cohérence.

Il me semble que ce phénomène peut aussi s'expliquer en partie par la présence de chaînes de responsabilité mal définies, particulièrement quand l'initiative ou la mesure envisagée nécessite la participation de plusieurs ministères, agences ou autres parties prenantes. En effet, les rôles et les responsabilités des ministères, des agences et du conseiller à la sécurité nationale et au renseignement (CSNR) en matière d'ingérence étrangère m'ont parfois paru peu clairs. Le Bureau du Conseil privé (BCP), Sécurité publique Canada et la CSNR ont parfois des responsabilités qui se chevauchent ou prêtent à confusion. À mon avis, cette confusion peut probablement expliquer l'hésitation que j'ai observée au sujet de la prise de décisions. Je crois que ce sujet mérite une réflexion au sein du gouvernement.

12.4 Une nouvelle stratégie de sécurité nationale

Le 25 novembre 2024, le premier ministre a adressé une lettre de mandat à la CSNR qui notamment lui confie la tâche d'élaborer une stratégie de sécurité nationale renouvelée en 2025 par l'entremise du Conseil de la sécurité nationale. Cette stratégie doit définir le cadre intégré de la sécurité nationale, de la défense et de la position diplomatique du Canada. Bien qu'il ne soit pas explicitement fait mention d'une version publique d'une stratégie de sécurité nationale, la lettre de mandat souligne la nécessité de la transparence et la responsabilité face au public. Je remarque que la dernière mise à jour de la Stratégie de sécurité nationale du Canada remonte à 2004, il y a 20 ans, soit trois ans après les attentats du 11 septembre.

Évidemment, une nouvelle Stratégie de sécurité nationale prendra en compte le cadre de réponse du Canada aux menaces d'ingérence étrangère. Je m'attends à ce que toute nouvelle stratégie de sécurité nationale aborde expressément comment les initiatives actuelles de lutte contre l'ingérence étrangère, tels le Plan et la Stratégie AHPE, ainsi que toute stratégie pour contrer l'ingérence étrangère, s'arrimeront avec cette nouvelle vision pour la sécurité nationale au Canada.

CHAPITRE 13

La réponse des autres institutions à l'ingérence étrangère

Les informations peuvent être incomplètes : *des produits de renseignement sont abordés à de nombreux endroits dans ce rapport public. Veuillez noter que ce rapport ne contient que les informations pertinentes qui peuvent être convenablement présentées de manière à ne pas porter atteinte aux intérêts cruciaux du Canada ou de ses alliés, à la défense nationale ou à la sécurité nationale. Du renseignement additionnel peut exister.*

13.1 Introduction

Au **chapitre 11**, je me suis intéressée aux ministères et aux organismes fédéraux qui jouent un rôle dans la protection du Canada contre l'ingérence étrangère. Cette discussion n'abordait toutefois qu'une partie des entités essentielles à la réponse du Canada.

En accord avec ce que j'ai entendu sur la nécessité d'une approche relative à l'ingérence étrangère qui implique l'ensemble de la société, de nombreuses autres entités contribuent à cet effort. Certaines sont des organismes publics indépendants alors que d'autres sont des institutions démocratiques elles-mêmes. D'autres encore proviennent du secteur privé ou font partie de la société civile. Certaines tentent activement de répondre à l'ingérence étrangère, et d'autres, sans se concentrer sur l'ingérence étrangère comme telle, effectuent un travail qui a des conséquences importantes sur la capacité du Canada à la détecter, à la prévenir et à la contrer.

Dans ce chapitre, j'aborde bon nombre d'entités clés qui sont extérieures au gouvernement.

13.2 Élections Canada

Élections Canada est responsable d'administrer le système électoral fédéral du Canada en vertu de la *Loi électorale du Canada* (la « ***LEC*** »). Cet organisme a à sa tête le directeur général des élections (le « **DGE** »). En tant qu'agent du Parlement, le DGE est indépendant du gouvernement.

Le mandat d'Élections Canada est double : il consiste à organiser les élections fédérales et à administrer les règles de la *LEC*, comme celles concernant l'enregistrement des partis politiques et le financement politique. L'organisme n'est pas chargé de faire appliquer la *LEC* (c'est-à-dire d'enquêter sur les infractions et de porter des accusations), une responsabilité qui appartient plutôt au commissaire aux élections fédérales.

Les formes d'ingérence étrangère qui peuvent relever de la compétence d'Élections Canada comprennent les menaces contre l'infrastructure électorale physique (par exemple, les bureaux de vote) et électronique

(par exemple, le site Web d'Élections Canada), les campagnes de désinformation concernant le processus électoral et le financement illicite de candidats, de partis ou d'autres entités. L'organisme joue également un rôle en fournissant des informations sur le système électoral dans son ensemble et en favorisant la confiance dans celui-ci, notamment en interagissant auprès des communautés qui peuvent être confrontées à des obstacles à la participation électorale.

L'administration des élections

Élections Canada organise toutes les élections générales et partielles fédérales. Cela comprend la tenue du Registre national des électeurs, la nomination des directeurs de scrutin, la formation du personnel électoral et la diffusion aux Canadiennes et aux Canadiens d'informations sur le vote.

Lorsque les élections sont déclenchées, Élections Canada doit recruter entre 230 000 et 250 000 personnes en quelques jours pour administrer les élections. En raison de l'ampleur de cette main-d'œuvre et de l'étroite fenêtre pendant laquelle ces personnes sont embauchées et travaillent, la plupart d'entre elles ne sont pas soumises à des contrôles de sécurité. Le DGE m'a dit que ce serait impossible. Au lieu de cela, Élections Canada s'appuie sur des mécanismes de protection agissant ailleurs dans le système pour maintenir son intégrité, notamment sur les différentes façons de voter, le secret du scrutin et la présence d'observateurs tiers qui veillent à ce que le personnel d'Élections Canada s'acquitte de ses tâches correctement.

Élections Canada n'administre pas les courses à l'investiture ou à la direction des partis politiques. Il administre seulement certaines règles limitées de financement politique qui s'appliquent à ces processus.

Le financement politique

La législation canadienne en matière électorale vise à établir des règles du jeu équitables et à empêcher l'influence indue de l'argent. Pour ce faire, elle établit des règles de financement politique, qui régissent la manière dont les contributions, financières ou autres, sont collectées, dépensées et déclarées. Ces règles prévoient notamment des limites pour les contributions et les dépenses pour certaines activités réglementées telles que la publicité électorale ou partisane ou les activités partisanes. Le système régit les partis, les associations de circonscription électorale[19], les candidats aux élections, les candidats à l'investiture et à la direction des partis politiques, ainsi que les tiers – collectivement appelés « entités politiques réglementées ».

[19] Aussi appelées de manière informelle les « associations de comté ».

Des règles différentes s'appliquent en période électorale et en période préélectorale. Ces règles sont complexes, mais l'une de leurs principales caractéristiques en matière d'ingérence étrangère est qu'elles interdisent d'utiliser des fonds provenant de l'étranger dans le cadre d'élections canadiennes.

Seuls les citoyens canadiens et les résidents permanents peuvent verser des contributions (par exemple, donner de l'argent, des biens ou des services) à des entités politiques réglementées. Les contributions à des « tiers » constituent une exception et sont soumises à des règles différentes. J'aborde la notion de tiers séparément ci-dessous. Les entités politiques réglementées ne sont pas tenues d'obtenir une preuve de l'admissibilité d'un donateur, bien qu'Élections Canada leur recommande de le faire. Les entités politiques réglementées doivent communiquer à Élections Canada le nom et l'adresse complets de toute personne ayant versé une contribution supérieure à 200 $. Ces informations sont publiées sur le site Web d'Élections Canada.

Les règles concernant les contributions à des tiers sont différentes. Le terme « tiers » désigne les entités qui n'entrent dans aucune des autres catégories d'entités réglementées. Il s'agit par exemple des particuliers, des syndicats, des personnes morales et des organismes communautaires.

Les tiers ne sont pas limités à recevoir des contributions de citoyens ou de résidents permanents, mais ils ne peuvent pas utiliser des fonds provenant de sources étrangères pour des activités réglementées comme la publicité électorale ou les activités partisanes. Les tiers étrangers ne sont pas autorisés à dépenser de l'argent pour une activité réglementée.

Les tiers doivent s'enregistrer auprès d'Élections Canada s'ils dépensent au moins 500 $ pour des activités réglementées pendant la période préélectorale ou électorale. Comme les autres entités réglementées, ils sont soumis à des limites de dépenses.

Les tiers doivent disposer d'un compte bancaire distinct pour toutes les contributions et dépenses liées aux activités réglementées. Toutefois, le DGE m'a dit qu'il peut être difficile de repérer du financement étranger de tiers, et ce pour diverses raisons. Ceci, à mon avis, peut constituer un risque d'ingérence étrangère. Par exemple, un tiers pourrait recevoir des fonds étrangers et nationaux en dehors d'une période électorale, les combiner et, une fois les élections déclenchées, utiliser l'argent pour des activités réglementées tout en déclarant qu'il provient de ses propres fonds. Le DGE a déjà fait des recommandations au Parlement pour modifier la *LEC* afin de remédier à certains de ces problèmes. Il a aussi fait des recommandations similaires à la Commission.

Les entités réglementées sont tenues de déposer une série de déclarations auprès d'Élections Canada, qui les examine pour s'assurer qu'elles sont complètes. L'organisme audite également certaines d'entre elles, en utilisant une approche basée sur le risque pour déterminer lesquelles devraient faire l'objet d'un examen plus approfondi.

L'éducation du public

Un élément essentiel du mandat d'Élections Canada est de fournir aux Canadiennes et aux Canadiens des informations sur le processus électoral, notamment sur la façon de voter et les mécanismes qui garantissent l'intégrité électorale. Reconnaissant que l'ingérence étrangère puisse dissuader les membres des communautés issues de diasporas de voter, Élections Canada dispose de guides multilingues pour communiquer des informations sur les mesures d'intégrité électorale et de programmes éducatifs destinés aux communautés issues des diasporas.

Élections Canada fournit des informations clés sur le vote en 51 langues sur son site Web. Pendant les campagnes électorales, il recrute des agents de relations communautaires pour interagir avec les populations confrontées à des obstacles pour voter, y compris les communautés issues des diasporas. En dehors des périodes électorales, Élections Canada collabore avec des groupes de la société civile et des éducateurs en milieu scolaire pour offrir des programmes éducatifs portant sur le processus électoral.

La surveillance des médias

Élections Canada surveille les médias traditionnels et l'environnement en ligne afin de repérer toute information inexacte à propos du processus électoral, comme des informations incorrectes sur une date d'élection ou des renseignements inexacts sur les règles d'identification des électeurs. L'organisme ne surveille pas les discussions politiques ni les plateformes qui ne sont pas accessibles à l'ensemble du public. Comme Élections Canada se concentre sur l'exactitude des informations, il n'enquête pas sur la source ni sur l'intention derrière ces informations.

Élections Canada produit des rapports de surveillance quotidiens pendant la période électorale et des rapports hebdomadaires en dehors de cette période. Ces rapports sont communiqués à ses partenaires gouvernementaux.

Élections Canada peut réagir à des informations inexactes sur le processus électoral, en particulier si elles se propagent rapidement ou si elles risquent de causer un préjudice. L'organisme intervient principalement en communiquant des informations exactes au public. Plus rarement, Élections Canada informera les plateformes de médias sociaux de l'existence d'informations inexactes et leur laissera le soin de les traiter conformément à leurs conditions d'utilisation.

Les relations avec d'autres entités gouvernementales

Élections Canada collabore étroitement avec le Centre canadien pour la cybersécurité (le « **CCC** ») afin d'assurer la sécurité de son infrastructure informatique.

Élections Canada a des canaux de communication ouverts avec le Service canadien du renseignement de sécurité (le « **SCRS** »). Le renseignement, y compris celui provenant du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (le « **Groupe de travail** »; voir au **chapitre 12**), parvient surtout à Élections Canada par l'entremise des comités de coordination de la sécurité des élections, lesquelles sont des entités co-présidées par Élections Canada et le Bureau du Conseil privé (le « **BCP** ») qui réunissent une gamme de ministères et d'organismes qui jouent un rôle dans le maintien de l'intégrité des élections. Le renseignement est parfois communiqué à Élections Canada dans le cadre de breffages directs du SCRS. Élections Canada a récemment amélioré sa capacité à accéder directement à des informations de niveau « Secret » et continue de travailler pour mettre en place des systèmes de vidéoconférence sécurisés.

Élections Canada est indépendant du Protocole public en cas d'incident électoral majeur (voir le **chapitre 12**), mais le DGE et le Panel des cinq peuvent communiquer l'un avec l'autre si des incidents électoraux majeurs se produisent. Advenant un grave incident concernant l'administration d'une élection, le DGE ferait une annonce publique. Selon les circonstances, le Panel pourrait faire une annonce distincte ou une annonce en parallèle.

L'effet des modifications législatives

Le rôle joué par Élections Canada dans la réponse à l'ingérence étrangère – ainsi que celui du Bureau du commissaire aux élections fédérales, que j'aborde ci-dessous – a récemment été un peu élargi par la législation.

En 2018, le Parlement a adopté la *Loi sur la modernisation des élections* (projet de loi C-76). Cette loi n'était pas axée sur l'ingérence étrangère, mais elle a apporté certaines modifications à la *LEC* qui sont pertinentes à cet égard. Plus particulièrement, la loi a modifié les règles de financement politique du Canada qui limitaient la mesure dans laquelle l'argent en provenance de l'étranger peut être dépensé pour des activités réglementées, comme la publicité partisane. Comme pour les autres mesures entourant le financement politique au pays, Élections Canada est responsable de mettre en œuvre ces règles.

En mars 2024, le gouvernement a présenté sa *Loi sur la participation électorale* (projet de loi C-65). Bien que ce projet de loi ait été soumis au Parlement pendant la majeure partie des travaux de la Commission, il est mort au feuilleton en janvier 2025 lorsque le Parlement a été prorogé. Étant donné que le projet de loi est toujours pertinent pour certaines des

recommandations que j'ai formulées (voir le chapitre 19, volume 5), je l'aborderai tout de même brièvement.

Comme le projet de loi C-76, le projet de loi C-65 ne visait pas précisément l'ingérence étrangère. Il aurait plutôt apporté plusieurs modifications à la *LEC*, en grande partie pour répondre aux recommandations du directeur général des élections qui découlent des élections générales de 2019 et de 2021. Plusieurs de ces modifications avaient pour but de renforcer l'intégrité électorale et auraient pu jouer un rôle dans la lutte contre l'ingérence étrangère.

En ce qui concerne les modifications aux règles relevant de la compétence d'Élections Canada, le projet de loi C-65 prévoyait des modifications aux règles de financement politique, surtout en ce qui concerne les tiers. Le projet de loi C-65 prévoyait l'adoption de règles plus strictes sur la façon dont les tiers sont autorisés à recueillir et à dépenser de l'argent pour des activités réglementées, les rapprochant ainsi des règles qui s'appliquent à d'autres entités réglementées. Ces changements visaient à accroître la transparence et à mieux contrer certains types de financement illicite, reconnus comme des tactiques d'ingérence étrangère.

13.3 Le Bureau du commissaire aux élections fédérales

Le commissaire aux élections fédérales (le « **CEF** ») est l'agent indépendant chargé de l'application de la *LEC*. Le commissaire est nommé par le DGE après consultation auprès du Directeur des poursuites pénales.

Le commissaire dirige une équipe d'environ 80 employés, dont 20 enquêteurs, qui constituent le Bureau du commissaire aux élections fédérales (le « **BCEF** »). Le BCEF est avant tout un organisme axé sur les plaintes. Il les reçoit directement du public ou elles lui sont transmises par d'autres agences. La majorité des plaintes porte sur les règles de financement politique.

L'ingérence étrangère en vertu de la *Loi électorale du Canada*

La *LEC* ne contient pas d'interdiction générale concernant l'ingérence étrangère, ni même de définition de ce terme. Par conséquent, certaines activités d'ingérence étrangère ne sont pas interdites par la *LEC*. D'autres formes d'ingérence étrangère peuvent toutefois être visées par diverses dispositions de cette loi.

La *LEC* comporte des interdictions qui s'appliquent particulièrement aux ressortissants étrangers, notamment l'interdiction d'effectuer des contributions ou des dépenses politiques, ainsi que l'interdiction visant la radiodiffusion étrangère. Le projet de loi C-76, que j'ai évoqué plus haut, a introduit une infraction relative à l'influence indue qui pouvait être exercée par des étrangers. Cette infraction est commise lorsqu'un étranger – y compris un gouvernement étranger – engage sciemment une dépense ou commet une infraction dans le but d'influencer un électeur pour qu'il vote ou ne vote pas du tout, ou qu'il vote ou ne vote pas pour un parti ou un candidat. D'autres formes d'influence, telles que les déclarations ou autres expressions d'opinion, sont autorisées.

La *LEC* contient également des interdictions qui s'appliquent à la fois aux citoyens canadiens et aux étrangers – comme l'intimidation d'un électeur – et qui peuvent englober certaines formes d'ingérence étrangère.

Lorsqu'une plainte est signalée comme impliquant potentiellement un acteur étranger ou des fonds étrangers, le BCEF la confie à un enquêteur et la traite comme « non routinière », ce qui garantit qu'une attention supplémentaire y sera portée.

Le défunt projet de loi C-65 aurait modifié la *LEC* de plusieurs façons qui relèvent de la compétence du BCEF. Il aurait établi de nouvelles interdictions et modifierait les interdictions existantes en ce qui concerne les informations fausses ou trompeuses à propos du processus électoral. Plus généralement, le projet de loi C-65 aurait élargi la portée de certaines dispositions relatives à l'administration et à l'application de la *LEC*, notamment en accordant au commissaire certains pouvoirs pour agir vis-à-vis les complots, les tentatives de commettre des infractions, la complicité après le fait ou les conseils fournis en lien avec une violation de la *LEC*.

Le BCEF reçoit de nombreuses plaintes comportant des allégations d'ingérence étrangère qui ne constituent pas une infraction en vertu de la *LEC* et celles-ci sont généralement classées sans suite. Lors des élections de 2019, le BCEF a constaté une augmentation notable des plaintes en lien avec l'ingérence étrangère, en grande partie parce que des enjeux ont été amplifiés sur les médias sociaux, et par conséquent, il a reçu de multiples plaintes sur le même sujet.

Le BCEF a recensé 201 dossiers comportant des allégations d'ingérence étrangère pour les élections de 2019, ce qui représentait environ 2 % des plaintes reçues. Pour les élections de 2021, il y a eu 22 plaintes, soit environ 0,5 % de toutes les plaintes reçues. Ces dossiers peuvent toutefois mobiliser d'importantes ressources d'enquête.

À ce jour, le BCEF n'a pas pris de mesures officielles ni porté d'accusations en lien avec l'ingérence étrangère, mais certaines plaintes ont révélé à la commission d'autres infractions à la *LEC*. Il convient de rappeler que l'autorité conférée au BCEF est limitée : il ne peut enquêter que sur les infractions à la *LEC*.

Les outils et les méthodes d'enquête

Les enquêteurs du BCEF ont recours à des méthodes qui reposent sur des sources ouvertes, des entrevues avec des témoins et sur d'autres outils d'application de la loi. Le BCEF ne dispose pas d'un service de renseignement et n'utilise pas de techniques de surveillance électronique ni d'informateurs. Le BCEF peut demander et examiner des documents publics, y compris ceux d'Élections Canada. Il peut chercher à obtenir des ordonnances de communication et des mandats de perquisition. Il peut demander une ordonnance du tribunal pour obliger des personnes à témoigner sous serment ou à produire des documents. Le BCEF peut aussi demander de l'aide à l'étranger en vertu de l'un des traités d'assistance judiciaire dont le Canada est signataire.

Le BCEF n'est pas un destinataire désigné des informations du Centre d'analyse des opérations et déclarations financières du Canada (le « **CANAFE** »), l'autorité du renseignement financier du Canada. De ce fait, il ne reçoit pas d'informations directes comme les déclarations d'opérations douteuses. Le BCEF doit plutôt passer par la Gendarmerie royale du Canada (la « **GRC** ») pour demander des informations au CANAFE. Le BCEF a récemment fait une demande pour être ajouté en tant que destinataire désigné des informations du CANAFE. Le BCEF pense que cela permettrait de générer des pistes d'enquête et de s'attaquer aux enjeux de traçabilité, de confusion et de dissimulation des fonds. Je n'ai pas entendu de témoignage de la part du CANAFE et ne connais donc pas son point de vue à ce sujet. Cela dit, à première vue, cette demande semble raisonnable et justifiée.

Le respect de la *Loi électorale du Canada* et son application

Le BCEF applique la *LEC* par le biais de procédures administratives et pénales et dispose à cette fin d'un éventail d'outils. Ceux-ci comprennent des mesures informelles telles que l'envoi de lettres d'avertissement, ainsi que des mesures formelles pouvant prendre la forme d'engagements, d'accords de conformité, de sanctions administratives pécuniaires (des « **SAP** ») et d'accusations criminelles. Les poursuites pour infractions électorales en vertu de la *LEC* doivent satisfaire à la norme exigeante de la preuve hors de tout doute raisonnable.

Les SAP sont destinées à promouvoir le respect de la *LEC*. Actuellement, la SAP maximale pour une violation commise par un particulier est de 1 500 $, et de 5 000 $ pour une personne morale ou une entité. La commissaire aux élections fédérales a suggéré d'augmenter le montant de ces sanctions, particulièrement en cas d'ingérence étrangère.

En vertu du régime pénal de la *LEC*, les personnes reconnues coupables d'une infraction sont passibles d'une peine maximale de cinq ans d'emprisonnement, d'une amende de 50 000 $ pour une personne physique et de 100 000 $ pour une entité, ou de l'application simultanée de ces deux sanctions. La CEF a proposé que ces sanctions soient elles aussi augmentées.

Je suis d'accord avec la suggestion d'augmenter à la fois les sanctions administratives pécuniaires et les amendes maximales pour les condamnations pénales en vertu de la *LEC*. J'y reviendrai dans mes recommandations.

La préparation des élections et le travail en période électorale

Le BCEF se prépare soigneusement aux élections, en s'appuyant sur les enseignements des élections passées et en consolidant ses capacités à gérer les plaintes. Pendant les périodes électorales, il donne la priorité à la réception, au triage et à l'examen des plaintes afin d'assurer la conformité avec les exigences de la *LEC* avant le jour de l'élection. Le BCEF travaille également avec les partis politiques, en désignant des points de contact pour les questions urgentes survenant pendant les périodes électorales.

En prévision des élections générales de 2019, le BCEF a établi des relations avec la communauté des chercheurs et des experts, tant à l'intérieur qu'à l'extérieur du gouvernement, afin d'échanger des connaissances sur des sujets tels que l'ingérence étrangère. Il collabore également avec des représentants d'organismes provinciaux et étrangers chargés de la gestion des élections sur des questions d'intérêt commun relatives à l'application de la loi.

Depuis les élections de 2019, le BCEF s'inquiète d'images ou de vidéos altérées susceptibles d'enfreindre la *LEC*. Il collabore avec des experts de la GRC pour comprendre et atténuer ces risques. La GRC fournit une assistance sur appel, en particulier pendant les moments critiques que sont les périodes électorales. L'équipe analytique du BCEF est chargée de suivre tous les produits de l'intelligence artificielle et les hypertrucages dont elle a connaissance en lien avec les élections. Le BCEF a également surveillé des dizaines d'élections dans le monde en 2024 pour apprendre et se préparer aux prochaines élections fédérales qui auront lieu au Canada.

Les relations avec d'autres entités gouvernementales

Le BCEF entretient des relations avec plusieurs partenaires de la communauté de la sécurité et du renseignement, ainsi qu'avec des organismes d'application de la loi. Le BCEF a des protocoles d'entente avec le SCRS et la GRC pour faciliter l'échange d'information et l'assistance. Le

BCEF participe aux comités de coordination sur la sécurité des élections. Il participe également au groupe de travail interministériel sur les élections générales qui réunit des organismes d'application de la loi, afin d'accroître l'efficacité de la communication du renseignement pendant les élections.

Le BCEF ne fait pas partie du Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections (le Groupe de travail). Toutefois, il a assisté à certaines réunions du Groupe de travail, y compris une série de rencontres traitant spécifiquement de l'ingérence étrangère. Ces rencontres ont eu lieu entre novembre 2023 et juin 2024 et comprenaient un ensemble élargi de participants. Si le Groupe de travail devait s'élargir et offrir un statut d'observateur, le BCEF souhaiterait en discuter.

Le BCEF s'efforce également de mieux s'équiper pour pouvoir utiliser du renseignement classifié dans le cadre de son travail. Depuis mars 2023, il travaille en étroite collaboration avec la GRC pour comprendre le cadre Une Vision, conçu pour faciliter l'échange d'informations entre le SCRS et la GRC. Le BCEF prévoit utiliser le renseignement dans ses activités pour sensibiliser le personnel aux tactiques utilisées par d'autres pays. Il prévoit l'employer dans le cadre de ses enquêtes et pour éclairer la planification stratégique. Le BCEF continue de travailler avec le SCRS pour s'assurer d'être inclus dans la distribution du renseignement que ce dernier produit. S'il ne le fait pas, le BCEF a remarqué qu'il peut parfois passer sous le radar du SCRS.

Par exemple, avant de prendre connaissance d'un rapport de février 2024 du Groupe de travail qui résume l'ingérence électorale de la République populaire de Chine (la « **RPC** »), la directrice exécutive, Contrôle d'application de la loi du BCEF, n'était pas au courant d'une évaluation du SCRS figurant dans le document. Elle a expliqué que même si ces informations n'auraient pas changé les décisions ni les mesures d'enquête prises par le BCEF, de telles informations classifiées sont utiles pour comprendre le contexte de la menace et contextualiser les enquêtes.

Pour pouvoir utiliser le renseignement, le BCEF est en train de développer sa capacité à recevoir, à traiter et à conserver des informations classifiées. Actuellement, le personnel doit se rendre dans les locaux d'autres agences pour prendre connaissance des informations et du renseignement sur format papier, ce qui est inefficace, surtout durant les périodes électorales.

Le BCEF a réalisé des progrès notables dans ses efforts pour se doter d'une infrastructure de communication sécurisée. Il évalue depuis un an la faisabilité d'un projet visant à lui donner accès à des communications de niveau « Secret » dans ses bureaux. Il a également déterminé qu'il avait besoin d'un accès au Réseau canadien Très secret (le « **RCTS** »). On m'a rapporté qu'il restait encore plusieurs étapes à franchir avant que le BCEF puisse accéder au RCTS, notamment en ce qui concerne les qualifications, l'expérience et la formation particulières que cela nécessite. La demande du BCEF me semble tout à fait justifiée et des efforts devraient être entrepris pour y répondre le plus rapidement possible.

Les plateformes numériques

Le BCEF interagit avec les plateformes numériques pour garantir une réponse rapide aux activités en ligne qui enfreignent la *LEC*. En période électorale, la principale préoccupation du BCEF consiste à assurer le respect de la réglementation. Il collabore avec Élections Canada et d'autres partenaires relativement aux activités préoccupantes sur les médias sociaux. Dans le cas de certaines plateformes, le BCEF peut demander le retrait de publications qui enfreignent la *LEC*.

Le BCEF n'entretient aucune relation suivie avec WeChat, mais l'organisme a déjà eu des contacts avec cette plateforme sur des questions sans rapport avec l'ingérence étrangère.

13.4 Le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)

Une grande partie du cadre stratégique du gouvernement sur le plan des médias relève de la responsabilité du Conseil de la radiodiffusion et des télécommunications canadiennes (le « **CRTC** »), une entité publique indépendante chargée de réglementer et de superviser la radiodiffusion et les télécommunications au Canada. Le CRTC délivre des licences de radiodiffusion, en plus de réglementer le contenu diffusé par la télévision, la radio et désormais les services de diffusion en continu. Selon ses principes directeurs, les Canadiennes et les Canadiens devraient être exposés à une diversité de points de vue et de nouvelles et décider des informations qu'ils jugent pertinentes. Le CRTC doit par ailleurs interpréter son mandat et conduire ses activités de manière à ne pas porter atteinte à la liberté d'expression.

Le CRTC réglemente aussi une partie de l'écosystème médiatique canadien, ce qui signifie qu'il pourrait éventuellement contribuer à répondre à l'ingérence étrangère, en particulier dans les cas de mésinformation et de désinformation.

L'octroi de licences et la réglementation de la télévision et de la radio

Tous les diffuseurs et distributeurs de contenus médiatiques par câble et par satellite relèvent de la compétence du CRTC. Les fournisseurs de services de télévision et de radio doivent être titulaires d'une licence, sauf s'ils bénéficient d'une exemption. Tous les titulaires de licence doivent être de

propriété canadienne et sous contrôle canadien. Cette dernière exigence signifie qu'un titulaire de licence doit exercer un contrôle réel sur son activité, y compris le contrôle du contenu éditorial et des décisions en matière de programmation.

L'expression « entreprises de distribution de radiodiffusion » (les « **EDR** ») désigne les opérateurs de télévision par câble, par protocole Internet et par satellite, tels que Bell ou Rogers. La programmation télévisuelle des EDR peut inclure des forfaits d'abonnement qui comprennent des stations émettrices non canadiennes, mais uniquement si ces stations émettrices figurent sur la liste du CRTC. Pour qu'une station soit sur la liste « approuvées pour distribution », elle doit être parrainée par une entité canadienne, comme une EDR. Lorsqu'une station est inscrite sur la liste, elle est soumise à certaines obligations, mais elle n'est pas elle-même titulaire d'une licence.

La réponse à l'ingérence étrangère

Le directeur exécutif de la radiodiffusion du CRTC m'a dit que le plus grand défi de l'organisme en matière d'ingérence étrangère est son incapacité à réagir rapidement. Il s'agit d'un tribunal dont les processus réglementaires sont basés sur des procédures et des dossiers publics, ainsi que sur le respect des règles d'équité procédurale. S'il reçoit une plainte selon laquelle un État étranger a demandé à une station de diffuser une fausse information le jour d'une élection, il est très peu probable que le CRTC puisse réagir en temps réel.

Une plainte de l'organisme espagnol *Safeguard Defenders*, un organisme de défense des droits de la personne, est un exemple dont j'ai entendu parler montrant à quel point le processus du CRTC peut être lent. L'organisme s'est plaint au CRTC en décembre 2019 que deux chaînes médiatiques d'État de la République populaire de Chine, approuvées pour distribution au Canada, avaient diffusé des aveux obtenus sous la torture. La plainte cherchait à faire retirer ces stations de la liste des stations approuvées. Or, cette demande est toujours en cours d'examen par le CRTC plus de cinq ans après le dépôt de la plainte.

Ces retards regrettables ne sont pas exclusifs au CRTC, mais je ne peux m'empêcher de remarquer qu'ils risquent de décourager le dépôt de plaintes.

Par ailleurs, le CRTC a une autorité limitée sur le contenu que les internautes génèrent et publient sur Internet, et aucune autorité sur les utilisateurs de médias sociaux.

Les titulaires de licence sont soumis au *Règlement sur la télédiffusion* du CRTC et au règlement équivalent pour la radio. Ces règlements interdisent de diffuser du contenu susceptible notamment d'exposer une personne, un groupe ou une catégorie de personnes à la haine ou au mépris pour divers motifs incluant le sexe, la race ou l'origine ethnique. Ils interdisent également aux titulaires de licence de diffuser des informations fausses ou trompeuses.

Le Groupe de travail sur les menaces en matière de sécurité et de renseignement visant les élections a reconnu que la manipulation et l'influence des médias traditionnels et en ligne dans le but de contrôler les récits et de diffuser de la désinformation représentaient une menace potentielle sur le plan de l'ingérence étrangère. L'interdiction des nouvelles fausses et trompeuses prévue par les règlements pourrait empêcher la diffusion de la propagande, ainsi que de la mésinformation et de la désinformation. Cependant, les objectifs de la *Loi sur la radiodiffusion* visent principalement à soutenir l'expression culturelle en français, en anglais et en langues autochtones, ainsi qu'à défendre et à préserver la liberté de la presse dans toute la mesure du possible. Le CRTC est donc très réticent à devenir l'arbitre de la vérité ou à agir comme un censeur. Ce point de vue est également partagé par d'autres parties prenantes au gouvernement.

Si un message est diffusé affirmant que les bureaux de vote sont fermés alors que ce n'est pas le cas, le CRTC pourrait considérer qu'il s'agit là d'une information fausse ou trompeuse. Toutefois, le témoin du CRTC m'a dit que l'organisme ne disposait pas de normes de preuve permettant d'évaluer les questions factuelles contestées ni de la capacité nécessaire pour mener des enquêtes factuelles intensives.

Par ailleurs, même si le CRTC constatait qu'un titulaire de licence ou une station approuvée pour distribution transmettait des informations fausses ou trompeuses sur ses ondes, l'organisme ne peut empêcher la diffusion de telles informations sur Internet. Les événements ayant entouré la décision de bannir *Russia Today* (« **RT** ») des ondes au Canada illustrent bien cette situation.

RT est un média d'État russe, qui figurait sur la liste des stations approuvées pour distribution et pouvait donc être diffusé au Canada. En 2022, lorsque la Russie a envahi l'Ukraine, RT a diffusé du contenu visant à justifier son offensive en faisant la promotion d'un discours qui propageait la haine contre les Ukrainiens. En réponse, la gouverneure en conseil (c'est-à-dire la gouverneure générale agissant sur l'avis du Cabinet) a demandé au CRTC d'évaluer si le contenu de RT était conforme ou contraire à la *Loi sur la radiodiffusion*.

Le CRTC a donc tenu une audience et a conclu qu'il n'était pas dans l'intérêt public de maintenir l'autorisation de distribuer RT. RT n'était pas titulaire d'une licence, mais si elle l'avait été, le contenu qu'elle diffusait aurait enfreint le *Règlement sur la télédiffusion* parce qu'il exposait les Ukrainiens à la haine ou au mépris. La chaîne a donc été retirée de la liste. C'était la première fois qu'une station non canadienne était retirée de la liste des stations approuvées pour distribution pour des raisons non administratives.

Même si le contenu de RT n'est plus offert à la télévision, il est toujours accessible en ligne au Canada puisque la décision du CRTC ne s'applique pas à Internet.

Les relations avec d'autres entités gouvernementales

Le CRTC a conclu des protocoles d'entente sur l'échange d'informations avec des entités telles qu'Élections Canada et le BCEF. Le CRTC a ainsi transmis certaines plaintes à Élections Canada et vice versa. En septembre 2024, le CRTC a reçu des informations du BCEF concernant la propriété ou le contrôle potentiel qu'exercerait la RPC sur des titulaires de licence canadiens. Au moment de rédiger le présent rapport, le CRTC était toujours en train de déterminer les prochaines étapes qu'il conviendrait d'entreprendre.

13.5 La Chambre des communes

La Chambre des communes (la « **Chambre** ») est l'assemblée élue du Parlement du Canada. Elle est composée de 338 députés élus par les Canadiennes et les Canadiens. Son Président guide les travaux de la Chambre et préside le Bureau de régie interne, l'organe responsable des questions administratives et financières de la Chambre. Le Bureau supervise ainsi l'administration de la Chambre.

En tant qu'institution démocratique, le Parlement et ses députés peuvent être la cible d'ingérence étrangère. Les questions d'ingérence étrangère impliquant des députés sont traitées comme des questions relatives à la sécurité générale de la Chambre. Le Bureau du sergent d'armes et de la sécurité institutionnelle (le « **sergent d'armes** ») est non seulement responsable de la sécurité institutionnelle de la Chambre, mais aussi de la sécurité personnelle des députés en dehors de la Cité parlementaire. Cela comprend leurs bureaux de circonscription et leurs résidences privées[20].

La Direction des services numériques et des biens immobiliers (les « **Services numériques** »), avec à sa tête le dirigeant général de l'information (le « **DGI** »), est responsable de la sécurité de l'information et de la cybersécurité.

La sécurité personnelle

Le sergent d'armes supervise environ 114 employés, qui élaborent les politiques et les programmes de sécurité institutionnelle. Le sergent d'armes assure la liaison avec les agences de renseignement et les organismes d'application de la loi pour traiter des questions de sécurité, y compris l'ingérence étrangère. Ces organismes d'application de la loi incluent la GRC,

[20] Dans la Cité parlementaire, la sécurité des parlementaires relève de la responsabilité du Service de protection parlementaire, qui est une entité distincte de l'Administration de la Chambre.

les services de police compétents selon le cas, et le Service de protection parlementaire.

Le sergent d'armes communique régulièrement avec la GRC et le Service canadien du renseignement de sécurité (SCRS). Il a conclu un protocole d'entente avec le Bureau du Conseil privé (BCP), le SCRS et la GRC permettant l'échange d'informations.

Le sergent d'armes surveille le renseignement de sources ouvertes pour rester à l'affût des menaces et du harcèlement à l'encontre des députés. S'il détecte une menace physique, il la porte à l'attention de l'équipe de gestion des risques qui travaille avec la GRC et les services de police compétents. Tous les matins de semaine, le sergent d'armes et la GRC produisent des rapports sur les menaces qui pèsent sur les députés. Les rapports de la GRC sont alimentés par le Secrétariat de la sécurité et du renseignement du BCP.

Le sergent d'armes effectue les filtrages de sécurité pour la Chambre. Ce filtrage est obligatoire pour les employés potentiels de l'Administration de la Chambre, le personnel des députés, les étudiants, les bénévoles et les prestataires de services qui demandent à avoir accès à la Cité parlementaire ou au réseau informatique de la Chambre. Le filtrage ne s'applique pas aux députés eux-mêmes, qui n'ont pas besoin d'une autorisation de sécurité pour siéger au Parlement.

L'accès physique au site du Parlement est accordé sur la base d'une analyse des informations reçues du SCRS et de la GRC. Il s'agit d'un processus distinct des autorisations de sécurité requises pour accéder aux documents classifiés et délivrées par le gouvernement.

Pour effectuer les filtrages de sécurité permettant l'accès au site du Parlement, le sergent d'armes vérifie les antécédents criminels et mène des enquêtes sur la « loyauté envers le Canada » avec l'aide de la GRC et du SCRS. Lorsque des questions se posent, le sergent d'armes peut mener un entretien dit de « levée de doute ». Le nombre de ces entretiens a considérablement augmenté au fil du temps : il y en a eu 10 en 2019, et 128 en 2023. Seule une poignée d'accréditations ont été refusées au cours de la dernière décennie en raison de préoccupations liées à l'ingérence étrangère. Deux de ces refus ont toutefois eu lieu entre mars et septembre 2024.

Le fait que deux filtrages de sécurité aient conduit à des refus liés à l'ingérence étrangère entre mars et septembre 2024 – alors que de tels refus étaient rares par le passé – peut signifier plus d'une chose : l'ingérence étrangère est plus présente, les filtrages de sécurité sont désormais plus approfondis, ou ce n'est là que le fruit du hasard.

L'information et la cybersécurité

Le DGI dirige une équipe d'environ 760 employés qui supervisent et fournissent l'infrastructure de sécurité informatique, les applications et le soutien à la Chambre, aux députés, aux employés de la Chambre et au personnel des députés. Le système de cybersécurité de la Chambre comprend la politique de sécurité, la conformité, la détection des menaces ainsi que la sensibilisation et la formation du personnel.

Les systèmes informatiques de la Chambre sont indépendants de ceux du gouvernement. Les Services numériques prennent en charge l'infrastructure de réseau commune à tous les partenaires parlementaires, à savoir le Sénat, le Service de protection parlementaire et la Bibliothèque du Parlement.

Le programme de sécurité informatique de la Chambre repose sur des mesures à la fois proactives et réactives. La Chambre adopte une approche multicouche basée sur les normes de l'industrie pour réduire les risques et s'assurer que les députés peuvent mener leurs affaires efficacement, que ce soit en caucus, dans leur bureau de circonscription ou au Parlement. Des contrôles sont en place pour les appareils et les utilisateurs, en plus des contrôles de périmètre, notamment aux points de connexion avec Internet et les réseaux gouvernementaux.

La Chambre fournit aux députés des ordinateurs pour leurs bureaux sur la Colline du Parlement et pour leurs bureaux de circonscription. Les députés ne sont pas censés utiliser ces appareils pour des activités partisanes, comme recueillir des fonds ou chercher à se faire réélire. Cela signifie que les députés peuvent en arriver à utiliser leurs appareils personnels à la fois pour des activités partisanes et des activités parlementaires. Les députés ont des approches différentes quant au nombre d'appareils qu'ils utilisent et à la manière dont ils les utilisent.

Le député John McKay a déclaré que la frontière entre les affaires parlementaires et partisanes peut parfois être floue et que, selon lui, il y aura inévitablement des cas où l'équipement de la Chambre sera utilisé pour des activités considérées comme partisanes. Le député Garnett Genuis a expliqué quant à lui qu'il recevait souvent des communications de ses électeurs sur des questions législatives ou d'autres travaux parlementaires sur ses appareils personnels.

L'Administration de la Chambre n'a aucune autorité sur l'utilisation par les députés de leurs appareils personnels et elle n'a pas la capacité de contrôler leur utilisation comme elle contrôle l'infrastructure informatique du Parlement. En outre, la Chambre ne fournit pas de services informatiques pour l'accès à Internet à domicile, même si certains députés peuvent utiliser le réseau de leur domicile pour effectuer du travail parlementaire. Toutefois, si un député soupçonne qu'un appareil personnel a été piraté, il peut demander aux Services numériques d'examiner et d'analyser l'appareil.

Les Services numériques mettent aussi à la disposition des députés le programme ParlVoyage, un service donnant accès à un environnement informatique sécurisé pour les fonctions parlementaires lors de voyages vers des destinations à haut risque. Dans le cadre de ce programme, les Services numériques proposent des breffages sur la cybersécurité et des séances de sensibilisation.

Les Services numériques ont un protocole d'entente et une relation de longue date avec le Centre canadien pour la cybersécurité (CCC) du Centre de la sécurité des télécommunications (le « **CST** »). Le personnel des Services numériques et celui de CCC se réunissent régulièrement. Les réunions sont soit prévues au calendrier ou organisées en réponse à des incidents précis. Le rôle du CCC est de contribuer à la protection du périmètre de l'infrastructure de la Chambre et à la gestion des incidents.

Les Services numériques et le CCC échangent aussi des informations sur la sensibilisation à la cybersécurité, les meilleures pratiques et les nouvelles tendances. Le CCC communique du renseignement aux Services numériques en fonction du « besoin de savoir » et de son mandat de protection de la Chambre contre les cybermenaces. Les Services numériques ne peuvent pas communiquer des informations sur les députés sans le consentement de ces derniers.

Les Services numériques reçoivent régulièrement des informations du CCC sur les cybermenaces. Ces informations se présentent sous la forme de bulletins techniques officiels du CCC, accompagnés d'une demande d'action ou d'une recommandation. Les Services numériques ne sauront pas nécessairement si une menace donnée est le fait d'un gouvernement étranger.

Le CCC peut demander des informations aux Services numériques pour l'aider à comprendre une cybermenace. Le CCC peut enquêter sur le périmètre du réseau informatique de la Chambre, mais pas à l'intérieur, et doit donc se tourner vers les Services numériques pour obtenir de l'information.

Si les Services numériques détectent ou ont connaissance d'une cyberattaque, ils ne la divulguent pas nécessairement aux parlementaires. D'autre part, ils n'informent personne des cyberattaques infructueuses, puisqu'il y en a chaque jour un nombre faramineux. Les attaques qui visent un parlementaire en particulier peuvent toutefois être signalées à ce dernier. Le Président de la Chambre est informé lorsqu'une attaque affecte les activités parlementaires ou présente un risque pour la réputation de la Chambre.

Il serait impossible, et probablement contre-productif, d'informer les parlementaires de toutes les cyberattaques. Cependant, je suis d'avis que les parlementaires visés directement par une cyberattaque devraient en être informés. Ils pourraient alors prendre les mesures qu'ils jugent appropriées.

La formation sur l'ingérence étrangère à l'intention des députés et de leur personnel

Comme je l'explique plus en détail au chapitre 15 (volume 4), la Chambre se coordonne avec les organismes nationaux chargés de la sécurité et du renseignement, et avec les organismes d'application de la loi, pour organiser des breffages non classifiés sur l'ingérence étrangère à l'intention des députés et de leur personnel. Ces breffages sont aussi fournis aux caucus de tous les partis reconnus, au Parti vert du Canada (le « **Parti vert** ») et aux députés indépendants. Cette année, des breffages ont également été organisés à l'intention du personnel de la Chambre. Ces breffages portent sur le contexte actuel de la menace liée à l'ingérence étrangère et sur les précautions à prendre.

Les Services numériques offrent des formations en cybersécurité aux députés et à leur personnel. Ils ont aussi mis en place un programme général de sensibilisation à la cybersécurité à l'intention des députés sur l'évolution du contexte des cybermenaces. Par exemple, les Services numériques ont ajouté un bouton dans le logiciel de courriel pour que les utilisateurs puissent facilement signaler les tentatives d'hameçonnage présumées. De plus, les Services numériques élaborent actuellement du matériel de sensibilisation sur l'ingérence étrangère en général, ainsi que du contenu sur la cybermenace dans ce domaine.

13.6 Le Sénat

Le Sénat est la Chambre haute du Parlement du Canada. Il compte 105 sénateurs nommés par le gouverneur général sur recommandation du premier ministre. Dans le cadre de leur rôle législatif, les sénateurs examinent les lois et peuvent proposer des amendements aux projets de loi. Les sénateurs peuvent aussi proposer leurs propres projets de loi. Ils jouent un rôle important dans l'examen des questions d'importance nationale, notamment par le travail des comités.

Comme c'est le cas pour la Chambre, le Sénat s'autorégule. Il est soutenu par une administration non partisane dirigée par le greffier du Sénat. L'administration du Sénat est organisée en trois secteurs : le secteur législatif, le secteur corporatif et le secteur juridique.

Tout comme la Chambre, le Sénat traite les questions d'ingérence étrangère comme des questions de sécurité générale. La sécurité institutionnelle du Sénat relève de la responsabilité de la Direction de la sécurité institutionnelle (la « **DSInst** »), tandis que les aspects de la sécurité relevant des technologies de l'information sont gérés par la Direction des services d'information (la « **DSInf** »).

La sécurité institutionnelle et la sécurité personnelle des sénateurs

La DSInst compte environ 42 employés. Elle agit comme conseillère stratégique principale pour toutes les questions de sécurité institutionnelle, y compris les plans et mesures de sécurité physiques. Les opérations de sécurité physique relèvent toutefois de la responsabilité du Service de protection du Parlement. Les responsabilités de la DSInst comprennent l'accréditation, la sécurité de la résidence des sénateurs et la sécurité des sénateurs lors de leurs déplacements.

Lorsque les sénateurs sont nommés, la DSInst leur propose une formation d'intégration facultative, destinée à leur intention et à celle de leur personnel. Cette formation prévoit du contenu sur l'ingérence étrangère. La DSInst organise également des breffages à l'intention des groupes sénatoriaux et des réunions de caucus. Lorsque les sénateurs voyagent à l'étranger pour le compte du Sénat, la DSInst leur fournit, ainsi qu'à leur personnel, des conseils et des breffages.

La DSInst collabore avec les organismes d'application de la loi et les agences de renseignement, de manière proactive et en réponse à des incidents précis. La DSInst et le SCRS se réunissent généralement au moins quatre fois par an, parfois plus. La GRC participe parfois à ces réunions. La DSInst partage quotidiennement des informations de sources ouvertes avec la Chambre, la GRC, le SCRS, la police locale et Affaires mondiales Canada, et elle reçoit des informations de leur part.

L'information et la cybersécurité

La Direction des services d'information (DSInf) est responsable de l'équipement informatique de tous les sénateurs et employés du Sénat. La DSInf fournit également des services tels que la détection de l'hameçonnage. Elle dispose d'une équipe chargée de la cybersécurité et de la sécurité des technologies de l'information. Les problèmes d'ingérence étrangère relevant des technologies de l'information sont relayés à cette équipe.

La DSInf fournit aux sénateurs essentiellement le même équipement et la même assistance que les Services numériques pour les députés, mais elle le fait indépendamment de la Chambre. La DSInf ne fournit généralement pas d'assistance aux sénateurs pour le courriel personnel et les médias sociaux. Cependant, la DSInf peut proposer son aide pour prévenir la propagation de logiciels malveillants ou les attaques visant la réputation d'un sénateur.

La DSInf dispense des formations obligatoires aux sénateurs et aux membres de leur personnel. Deux formations sont obligatoires pour les sénateurs. La première explique comment traiter l'information tout au long de son cycle de vie. La seconde sensibilise à la cybersécurité et est dispensée dans les deux premières semaines suivant l'entrée en fonction d'un sénateur. Le chef de la

DSInf, ou un membre de son équipe, rencontre aussi chaque nouveau sénateur pour lui parler des risques liés à la cybersécurité. La DSInf organise également des simulations d'hameçonnage destinées aux sénateurs.

La DSInf a établi des lignes directrices à l'intention des sénateurs lorsqu'ils voyagent et leur demande de la contacter avant de partir. La DSInf évalue les risques en fonction du lieu où les sénateurs se rendent et des personnes qu'ils rencontrent.

La DSInf a mis en œuvre plusieurs pratiques exemplaires recommandées par le Centre canadien pour la cybersécurité (CCC). Contrairement à la Chambre, elle n'a pas de protocole d'entente avec le CCC. Toutefois, en ce qui touche les cybermenaces, la DSInf collabore avec le CCC, la Chambre des communes, la Direction de la sécurité institutionnelle (DSInst) et la GRC. Il serait souhaitable qu'un protocole d'entente officialise cette collaboration.

13.7 Les partis politiques

Les partis politiques sont en première ligne de nos institutions démocratiques. Ils sont également une cible potentielle d'ingérence étrangère. Tous les représentants des partis politiques qui ont témoigné lors des audiences publiques ont d'ailleurs exprimé une certaine inquiétude quant au fait que les partis puissent être la cible d'ingérence étrangère.

Cela dit, les chefs de ces partis politiques semblent généralement réticents à l'idée de prendre des mesures pour contrer l'ingérence étrangère, qui auraient aussi pour effet de limiter leur autonomie. Les représentants qui ont témoigné devant la Commission étaient tous fermement opposés à ce que les courses à la direction et à l'investiture soient réglementées. Ils ont tous affirmé que les mesures internes mises en place pour garantir l'intégrité de ces courses sont suffisantes. À mon avis, elles ne le sont pas.

Les partis politiques sont des entités autonomes. Ils sont essentiellement libres d'établir leurs propres règles pour régir leurs membres, choisir leurs candidats et sélectionner leurs chefs.

Les critères d'adhésion et les cotisations

De manière générale, les membres d'un parti politique déterminent qui peut voter lors d'une course à la direction ou à l'investiture, qui peut occuper des fonctions au sein d'un parti et qui peut participer aux conventions au cours desquelles les politiques du parti sont généralement déterminées. Les règles d'un parti témoignent avec force de ses valeurs et de ses engagements, telles que la mobilisation des jeunes ou la participation démocratique.

Le Parti conservateur du Canada (le « **Parti conservateur** »), le Nouveau Parti démocratique du Canada (le « **NPD** ») et le Parti vert exigent que leurs membres soient citoyens ou résidents permanents. Au moment des audiences publiques, le Parti libéral du Canada (le « **Parti libéral** ») étendait l'admissibilité à tous ceux qui vivent habituellement au Canada et aux Canadiennes et aux Canadiens vivant à l'étranger ayant droit de vote aux élections fédérales. Le 9 janvier 2025, il a annoncé sa décision de modifier ses règles relatives à l'accès et au maintien du statut de membre du Parti libéral. En vertu de ces règles, une personne doit avoir la citoyenneté canadienne, avoir le statut d'Indien en vertu de la *Loi sur les Indiens*, ou être résident permanent. Le Bloc Québécois n'impose aucune condition de citoyenneté ou de résidence.

La plupart des partis exigent que leurs membres soient âgés d'au moins 14 ans, bien que l'âge requis par le NPD varie entre 12 et 14 ans en fonction de la province ou du territoire.

La plupart des partis demandent une cotisation à ses membres. Certains autorisent les paiements en espèces (le Parti vert, le NPD et le Bloc Québécois), tandis que d'autres ne le permettent pas, comme le Parti conservateur. Le Parti libéral ne demande pas de cotisation.

Les partis ont recours à diverses mesures pour faire respecter leurs règles d'adhésion. Ils demandent par exemple aux personnes qui adhèrent au parti d'attester qu'elles respectent les conditions d'admissibilité en cochant une case, ils contrôlent les adresses IP des personnes qui adhèrent en ligne et ils interdisent les adhésions en masse.

Les courses à l'investiture et la sélection des candidats

Chaque parti fixe et applique ses propres règles pour les courses à l'investiture, notamment en ce qui concerne les qualifications exigées des candidats, la convocation ou non d'une assemblée d'investiture (où se déroule le vote) et le déroulement de cette assemblée. Ces règles prévoient généralement une répartition des responsabilités et des pouvoirs entre le parti central et les associations de circonscription électorale.

Les associations de circonscription électorale sont des organisations partisanes actives dans une circonscription donnée. Elles participent généralement au recrutement des candidats qui pourraient représenter la circonscription pour le parti. Elles s'occupent également de l'organisation et de l'animation des assemblées d'investiture.

Les partis ont généralement recours à un processus de vérification avant qu'une personne puisse se présenter à une course à l'investiture. Bien que les partis n'examinent pas précisément les questions d'ingérence étrangère, le processus de vérification pourrait révéler de telles informations. En général, les partis examinent la présence du candidat potentiel sur les médias sociaux et sur Internet, ses antécédents de carrière et ses liens

professionnels ainsi que son affiliation à des organisations ou à d'autres groupes. Certains partis vérifient les antécédents criminels et un parti demande aux candidats potentiels à l'investiture de consentir à la divulgation d'informations provenant d'un ensemble d'agences et de ministères du gouvernement. Un autre parti fait appel à une société externe pour effectuer cette vérification. Il n'y a donc pas de processus de vérification standard.

Le vote lors d'une course à l'investiture est généralement limité aux membres du parti qui vivent dans la circonscription. Chaque parti utilise un processus de vérification différent pour confirmer l'admissibilité au vote. La plupart demandent aux membres de présenter une pièce d'identité comportant leur nom, leur adresse et une photo. Au moins un parti dispense de l'obligation de présenter une pièce d'identité lorsque des circonstances exceptionnelles le justifient. Des mécanismes sont généralement en place si un candidat à l'investiture souhaite en appeler du déroulement ou des résultats de l'assemblée d'investiture.

En vertu de la *Loi électorale du Canada*, le chef d'un parti doit signer la documentation de chacun des candidats que son parti soutient. Si le chef décide de ne pas signer les documents d'un candidat, cette personne ne peut se présenter sous le nom du parti, même si elle a remporté la course à l'investiture. En fait, les partis ne sont pas tenus d'organiser de courses à l'investiture.

L'autorité d'un chef de rejeter les candidats choisis dans le cadre d'une course à l'investiture a été suggérée comme un moyen de se défendre contre l'ingérence étrangère. Comme je l'explique au chapitre 15 (volume 4), si un chef de parti a connaissance suffisamment tôt de problèmes d'ingérence étrangère concernant un candidat, il peut l'empêcher de se présenter pour le parti.

Comme je l'explique au **chapitre 10**, le Groupe de travail suggère que les courses à l'investiture pourraient être exploitées par des États étrangers pour cibler des candidats et des circonscriptions afin d'influencer le choix des députés. Je suis d'accord. Cela dit, les éléments de preuve dont je dispose n'indiquent pas que l'ingérence étrangère dans les processus d'investiture fédéraux ait été généralisée jusqu'à présent. Jai entendu des témoignages concernant une ingérence étrangère potentielle dans une seule course à l'investiture fédérale, dans la circonscription de Don Valley-Nord (voir le chapitre 7, volume 2). Je note qu'il s'agit là du seul cas de course à l'investiture qui figure dans la liste du gouvernement des cas soupçonnés d'ingérence étrangère significative dans les processus électoraux du Canada (voir au **chapitre 10**).

Les courses à la direction

On m'a rapporté que les courses à la direction des partis politiques pouvaient aussi constituer une source de vulnérabilité à l'ingérence étrangère.

De nos jours, les courses à la direction s'appuient sur le principe « un membre, une voix » qui permet à chaque membre d'un parti de voter pour élire leur chef. Le principe « un membre, une voix » incite les candidats à recruter le plus grand nombre de membres possible.

Les partis politiques organisent leurs propres courses à la direction et sont libres d'en fixer les règles. Par exemple, les partis peuvent déterminer les dates limites d'inscription des candidats et d'adhésion des membres. Ils peuvent fixer des plafonds de dépenses pour les candidats, ou exiger d'eux qu'ils versent un dépôt ou des frais minimums au parti. Les partis déterminent la durée de la course à la direction, les règles pour voter et comment les résultats seront communiqués.

Les partis ont tendance à déterminer les particularités de chaque course à la direction au cas par cas, ce qui signifie que les règles changent au fil du temps, en fonction des tendances générales en matière de démocratie et de culture, et des circonstances particulières du moment.

La Commission a reçu de la preuve sur les allégations d'ingérence du gouvernement indien dans une course à la direction du Parti conservateur. Les témoins du Service canadien du renseignement de sécurité (SCRS) ont indiqué qu'ils n'avaient aucune raison de croire que le candidat touché aurait été au courant d'un quelconque soutien présumé. Ils ont également noté que, bien qu'elles soient préoccupantes, ce ne sont pas toutes les activités de l'Inde dans cette affaire qui étaient clandestines.

Le renseignement à ce sujet a été transmis à de hauts fonctionnaires du Bureau du Conseil privé (BCP) et à la Conseillère à la sécurité nationale et au renseignement auprès du premier ministre sous la forme de deux produits, l'un d'eux ayant aussi été transmis à de hauts fonctionnaires de Sécurité publique Canada. Il était également inclus dans une évaluation du renseignement largement diffusée dans la communauté du renseignement et faisait partie d'une mise à jour du Groupe de travail au Comité de coordination des sous-ministres sur la sécurité des élections (voir le chapitre 6, volume 2). Les représentants du SCRS n'avaient aucun souvenir d'avoir communiqué ce renseignement à l'échelon politique, y compris aux candidats eux-mêmes.

En janvier 2024, le SCRS et le Centre intégré d'évaluation du terrorisme (le « **CIET** ») ont présenté un breffage défensif au chef de cabinet du chef du Parti conservateur[21]. Ce breffage était le résultat d'un produit du CIET, qui était principalement axé sur la menace d'extrémisme violent. Il comprenait

[21] Le SCRS a proposé plusieurs breffages défensifs aux députés. Je reviens sur ce point au chapitre 15 (volume 4).

également des informations de haut niveau sur les menaces d'ingérence étrangère susceptibles de viser le chef du Parti conservateur. Le SCRS n'a pas communiqué d'informations sur les allégations d'ingérence dans la course à la direction au chef de cabinet à cette occasion, étant donné que le breffage n'était pas classifié.

En juin 2024, le SCRS a présenté un breffage classifié au chef de cabinet du chef du Parti conservateur. La sous-directrice des Opérations du SCRS a expliqué que ce breffage était un exemple d'efforts plus larges visant à fournir des informations classifiées afin d'accroître la résilience face à l'ingérence étrangère. L'objectif du breffage était de fournir des informations générales, étayées par différents exemples précis d'activités et de tactiques de menace d'ingérence étrangère. C'est à ce moment-là que le chef de cabinet du chef du Parti conservateur a été informé des allégations d'ingérence dans la course à la direction.

13.8 Les médias

Étant donné que la mésinformation et la désinformation peuvent avoir un effet important sur l'ensemble de la population canadienne, il est important de disposer d'un écosystème médiatique sain pour renforcer la résilience des citoyens face à l'ingérence étrangère.

Dans ce contexte, la résilience a été définie comme la capacité de la population à savoir quand valider une information auprès de sources crédibles d'informations avant de l'accepter comme véridique. Les Canadiennes et les Canadiens doivent être en mesure de comprendre que toute information n'est pas nécessairement vraie et qu'on ne devrait pas accorder le même poids à chacune.

Il est donc important pour la démocratie canadienne que notre population dispose de sources d'information crédibles et fiables pour faire contrepoids à la mésinformation et à la désinformation. Les journalistes et les médias d'information sont essentiels pour protéger les institutions démocratiques du Canada, y compris les élections. Les témoins du ministère du Patrimoine canadien ont parlé de l'importance d'appuyer les médias canadiens pour s'assurer que les nouvelles soient dignes de confiance et de bonne qualité. À la lumière des témoignages entendus, je suis d'accord, mais j'ajouterais qu'il est aussi important que les médias soient indépendants du gouvernement et des partis politiques.

13.9 Les organisations de la société civile

De nombreux témoins ont déclaré que le rôle de la société civile est crucial dans une approche qui implique l'ensemble de la société et qui vise à détecter, prévenir et contrer l'ingérence étrangère. La Commission n'avait pas la capacité d'enquêter sur tous les groupes de la société civile susceptibles de jouer un rôle dans la réponse à l'ingérence étrangère dans les institutions démocratiques. Néanmoins, cette section décrit le travail effectué pour aider les Canadiennes et les Canadiens à se défendre contre la mésinformation et la désinformation. Selon les témoins gouvernementaux et non gouvernementaux entendus, ces dernières sont des méthodes majeures d'ingérence étrangère. Elles sont aussi les plus répandues et les plus difficiles à contrer.

L'observatoire de l'écosystème médiatique

J'ai entendu trois témoins de l'observatoire de l'écosystème médiatique (le Media Ecosystem Observatory ou le « **MEO** »). Le MEO a été créé à l'approche des élections fédérales de 2019, dans le cadre d'une collaboration entre l'École Max Bell de politiques publiques de l'Université McGill et la Munk School of Global Affairs & Public Policy de l'Université de Toronto. Il visait à combler des lacunes dans la compréhension qu'avaient les chercheurs de ce qui se passait dans l'écosystème canadien de l'information, notamment en période électorale. Le MEO étudie comment les informations circulent dans l'écosystème médiatique et les réactions comportementales à ces informations. Il a observé les élections fédérales de 2019 et de 2021 et produit des rapports examinant l'écosystème de l'information numérique durant ces deux périodes (voir les chapitres 7 et 8, volume 2).

L'approche du MEO reconnaît que la mésinformation et la désinformation circulent de la même manière que les informations véridiques, et qu'il est souvent difficile de déterminer la véracité ou la fausseté d'une affirmation. De plus, l'origine d'une information est souvent impossible à connaître. Au lieu de se concentrer sur des éléments d'information individuels ou d'essayer de reconnaître une éventuelle manipulation en fonction de la source, le MEO essaie plutôt de comprendre l'écosystème de l'information dans son ensemble. Pour ce faire, le MEO collecte principalement trois types d'informations.

Tout d'abord, il recueille des données de traçage numériques sur les plateformes en ligne, notamment des métadonnées telles que les mentions « J'aime », les partages, le nombre de commentaires, les liens intégrés, les photos téléchargées, les mots-clics et les mentions. Ces données lui permettent de suivre la diffusion des informations entre les utilisateurs sur et entre les plateformes. Le MEO surveille environ 4 000 comptes canadiens qui

semblent avoir le plus d'effet sur la diffusion d'informations politiques, ainsi que des comptes clés en provenance de pays étrangers (principalement de la RPC, de la Russie et de l'Inde) qui produisent de la mésinformation et de la désinformation pertinentes pour le Canada.

Deuxièmement, le MEO sonde les Canadiennes et les Canadiens. Il utilise des sondages pour évaluer l'effet sur la population des événements survenus dans l'écosystème de l'information. Ces sondages tentent de déterminer si l'information qui circule modifie les opinions ou les comportements des gens.

Troisièmement, le MEO assure une veille médiatique dans le cadre de laquelle les chercheurs lisent les informations en ligne afin d'obtenir des données qualitatives sur l'écosystème. Ces informations permettent de contextualiser les données empiriques obtenues par le MEO et de décrire les tendances en matière d'information.

Le Réseau canadien de recherche sur les médias numériques (RCRMN)

En avril 2022, le MEO a reçu une subvention du Programme de contribution en matière de citoyenneté numérique (dont je parle au **chapitre 12**) pour la mise en place du Réseau canadien de recherche sur les médias numériques (le « **RCRMN** »). Ce Réseau est un partenariat entre le MEO et neuf autres organisations. Il tente de comprendre l'écosystème canadien de l'information, de décrire la base de référence ordinaire de l'environnement et de réagir aux « incidents liés à l'information », c'est-à-dire aux perturbations de l'écosystème de l'information qui ont un effet important sur la circulation normale ou l'intégrité de l'information.

L'une des conclusions du MEO découlant de l'observation des élections de 2021 était qu'il serait utile de pouvoir comprendre et contextualiser rapidement les interventions extérieures survenant dans l'écosystème des médias, plutôt que d'avoir à attendre une analyse après coup. Cela a conduit ses organisateurs à réfléchir à la manière de développer une plus grande capacité à comprendre l'écosystème des médias, en particulier pendant les périodes électorales.

Le protocole de réponse aux incidents du RCRMN est destiné à fournir cette capacité. Les incidents liés à l'information peuvent être détectés grâce à la surveillance du MEO ou aux indications fournies par des partenaires de recherche ou des journalistes. Le MEO évaluera si l'incident est suffisamment grave et, si c'est le cas, il désignera une équipe de réponse. Il utilisera les ressources du RCRMN pour analyser l'incident et fournir des rapports fréquents, opportuns et publics au fur et à mesure de l'évolution de l'incident. Le RCRMN produira finalement un résumé de l'incident.

Pendant les élections, le RCRMN joue un rôle quelque peu similaire à celui du Mécanisme de réponse rapide du Canada d'Affaires mondiales Canada (voir

au chapitre 11). Le RCRMN est toutefois indépendant du gouvernement sur le plan opérationnel. Bien qu'il reçoive un financement important du gouvernement et qu'il informe régulièrement les fonctionnaires de ses conclusions publiques, le MEO ne reçoit pas d'instructions du gouvernement et ses rapports sont publics. Les informations qu'il fournit au gouvernement sont les mêmes que celles fournies au public.

Les défis auxquels le MEO et le RCRMN sont confrontés

Le RCRMN compte surveiller l'écosystème en ligne pendant les prochaines élections fédérales. Cependant, on m'a mentionné deux éléments qui risquent de menacer la capacité du MEO et du RCRMN à effectuer ce travail. Le premier élément est le financement. Le travail du MEO et du RCRMN demande beaucoup de ressources et dépend du financement du gouvernement. Alors que le gouvernement s'attend à ce que le RCRMN joue un rôle d'importance lors des prochaines élections, celui-ci n'est financé que jusqu'à la fin du mois de mars 2025. L'incertitude quant au financement au-delà de 2025 nuit à la capacité du MEO à planifier ses activités et à recruter et conserver son personnel.

La deuxième source de préoccupation concerne les changements dans la capacité du MEO et d'autres organisations de la société civile à accéder à des données critiques par le biais des interfaces de programmation d'applications (des « **API** ») des plateformes de médias sociaux. Les plateformes, qui donnaient aux chercheurs non gouvernementaux un accès gratuit ou à faible coût à leur API, ont récemment considérablement augmenté les prix d'accès aux données ou ont limité les données qui sont accessibles, voire les deux. Les restrictions d'accès aux API limitent considérablement la capacité du MEO à faire son travail et ont créé ce que les témoins ont décrit comme étant une crise dans la communauté de la recherche au niveau mondial. Cette question dépasse le mandat de la Commission, mais je crois que le gouvernement devrait s'y intéresser.

13.10 Conclusion

Tenter de répertorier toutes les entités qui jouent un rôle dans la réponse à l'ingérence étrangère serait une tâche impossible dans le cadre d'un rapport de cette taille. Défendre la souveraineté et la démocratie du Canada exige nécessairement des efforts de la part de l'ensemble de la société.

La conclusion que l'on peut tirer de ce chapitre est qu'il existe de nombreux types d'institutions et d'acteurs qui jouent un éventail de rôles pertinents dans la manière dont le Canada répond à l'ingérence étrangère. Une réponse efficace à cette ingérence exige des efforts de la part de chacun d'entre eux.

ANNEXE A

Glossaire

Terme	Sigle ou abréviation	Définition
Affaires mondiales Canada (Global Affairs Canada)	AMC (GAC)	Ministère fédéral qui gère les relations diplomatiques, fait la promotion du commerce international et fournit de l'aide consulaire. Il dirige également les efforts internationaux en matière de développement, d'aide humanitaire et d'appui à la paix et à la sécurité, et contribue à la sécurité nationale et au développement du droit international.
Agent des relations avec les clients (Client Relations Officer)	ARC (CRO)	Fonctionnaire des services de renseignement chargé de transmettre des produits de renseignement pertinents aux responsables et au personnel du gouvernement qui disposent d'une autorisation de sécurité.
Avocats de la Commission (Commission Counsel)		Avocats qui travaillent pour la Commissaire au sein de la Commission sur l'ingérence étrangère.
« Besoin de savoir » ("Need to know")		Terme décrivant une condition devant être satisfaite pour accéder à de l'information classifiée. Même si une personne dispose de l'autorisation de sécurité nécessaire pour accéder à une information, elle ne peut y accéder que si cela est nécessaire dans l'exercice de ses fonctions officielles.
Breffage préventif de sécurité (Protective Security Briefing)	BPS (PSB)	Type de breffage non classifié fourni par le Service canadien du renseignement de sécurité (SCRS) pour sensibiliser un individu à une menace. Également appelé « breffage sur la sécurité défensive ».
Breffage sur la sécurité défensive (Defensive briefing)		Voir « Breffage préventif de sécurité ».

Terme	Sigle ou abréviation	Définition
Bureau du commissaire aux élections fédérales (Office of the Commissioner of Canada Elections)	BCEF (OCCE)	Organisation dirigée par le commissaire aux élections fédérales (CEF) au sein du Bureau du directeur général des élections (DGE). Dans le cadre de ses responsabilités en matière de conformité et d'application de la *Loi électorale du Canada*, le BCEF agit indépendamment du DGE.
Bureau du Conseil privé (Privy Council Office)	BCP (PCO)	Ministère dont le rôle principal est la coordination de l'administration gouvernementale. Souvent qualifié de ministère du premier ministre. Fournit des conseils non partisans au premier ministre, au Cabinet et aux comités du Cabinet sur des questions qui revêtent une importance nationale et internationale. Appuie le processus décisionnel du Cabinet et veille à la mise en œuvre du programme politique et législatif du gouvernement par tous les ministères et organismes du gouvernement fédéral.
Bureau du directeur général des élections (Office of the Chief Electoral Officer)	DGE (OCEO)	Agence indépendante composée d'Élections Canada et du Bureau du commissaire aux élections fédérales (BCEF).
Cabinet		Organe décisionnel politique présidé par le premier ministre. Composé des ministres nommés par la gouverneure générale sur recommandation du premier ministre. Par convention, ces ministres (membres du Cabinet) sont généralement des députés. Ils dirigent les ministères du gouvernement.
Cabinet du premier ministre (Prime Minister's Office)	CPM (PMO)	Soutient le premier ministre dans l'exercice de ses responsabilités à titre de chef du gouvernement, de chef de parti politique et de député. Le cabinet du premier ministre est composé de personnel politique et non de fonctionnaires de carrière.

Terme	Sigle ou abréviation	Définition
Camouflage de pourriels (Spamouflage)		Tactique qui utilise des réseaux de nouveaux comptes de médias sociaux ou des comptes piratés pour publier et amplifier des messages de propagande à travers de multiples plateformes.
Centre canadien pour la cybersécurité (Canadian Centre for Cyber Security)	CCC (CCCS)	Fait partie du Centre de la sécurité des télécommunications (CST). Il s'agit de la source unifiée de conseils, d'avis, de services et de soutien spécialisés en matière de cybersécurité pour les Canadiennes et les Canadiens.
Centre de la sécurité des télécommunications (Communications Security Establishment)	CST CSE)	Organisme du gouvernement fédéral qui fournit au gouvernement du renseignement électromagnétique étranger, et est responsable de la cybersécurité et de la protection de l'information. Le Centre canadien pour la cybersécurité fait partie du CST.
Comités interministériels (Inter-departmental Committees)		Comités composés de hauts fonctionnaires issus de divers ministères et organismes afin d'assurer une action coordonnée. Existent généralement au niveau des sous-ministres, des sous-ministres adjoints et des directeurs généraux.
Comité des parlementaires sur la sécurité nationale et le renseignement (National Security and Intelligence Committee of Parliamentarians)	CPSNR (NSICOP)	Comité statutaire composé de députés et de sénateurs et régi par la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*. Examine les opérations de renseignement du gouvernement, notamment les cadres législatif, réglementaire, stratégique, administratif et financier de la sécurité nationale et du renseignement. Examine aussi les activités des ministères liées à la sécurité nationale ou au renseignement (à moins qu'une activité ne soit une opération en cours et que le ministre compétent ne détermine que l'examen serait préjudiciable à la sécurité nationale). Enquête également sur toute question liée à la sécurité nationale ou au renseignement dont il est saisi par un ministre.

Terme	Sigle ou abréviation	Définition
Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Standing Committee on Access to Information, Privacy and Ethics)	ETHI	Composé de députés. Étudie des questions qui touchent : • le Commissariat à l'information du Canada • le Commissariat à la protection de la vie privée du Canada • le Commissariat au lobbying du Canada. Étudie aussi certaines questions relatives au Commissariat aux conflits d'intérêts et à l'éthique.
Comité permanent de la procédure et des affaires de la Chambre (Standing Committee on Procedure and House Affairs)	PROC	Composé de députés. Étudie les questions suivantes et en fait rapport : • règles et pratiques de la Chambre des communes et de ses comités • questions électorales • questions de privilège • conflits d'intérêts des députés.
Comités de coordination de la sécurité des élections (Elections Security Coordinating Committees)	CCSE (ESCCs)	Comités de hauts fonctionnaires du gouvernement et d'Élections Canada créés pendant les élections fédérales (au niveau des sous-ministres, des sous-ministres adjoints ou des directeurs généraux). Coprésidés par le Bureau du Conseil privé et Élections Canada. Assurent une approche coordonnée et une compréhension commune entre la communauté de la sécurité nationale et du renseignement, Élections Canada et le commissaire aux élections fédérales.
Commissaire aux élections fédérales (Commissioner of Canada Elections)	CEF (CCE)	Veille au respect de la *Loi électorale du Canada* et de la *Loi référendaire*. Nommé par le directeur général des élections, après consultation auprès du directeur des poursuites pénales.
Commission sur l'ingérence étrangère (Foreign Interference Commission)	Commission	Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Terme	Sigle ou abréviation	Définition
Communauté de la sécurité et du renseignement (Security and Intelligence Community)	(S&I Community)	Ministères et agences du gouvernement du Canada qui travaillent à la sécurité nationale et à la collecte du renseignement : AMC, BCP, CST, GRC, MDN, SCRS et Sécurité Publique Canada.
Confidentialité à des fins de sécurité nationale (National security confidentiality)	CSN (NSC)	Vise à restreindre l'accès à certaines informations du gouvernement ainsi qu'à empêcher leur divulgation afin de protéger les intérêts de la sécurité nationale.
Conseil privé du Roi pour le Canada (King's Privy Council for Canada)		Groupe de personnes nommées par la gouverneure générale pour conseiller le Roi : membres du Cabinet, anciens ministres, juge en chef du Canada, anciens juges en chef, anciens présidents de la Chambre des communes, anciens présidents du Sénat, anciens gouverneurs généraux et autres personnes éminentes.
Conseil de la radiodiffusion et des télécommunications canadiennes (Canadian Radio-television and Telecommunications Commission)	CRTC	Organisme public chargé de réglementer et de superviser la radiodiffusion et les télécommunications au Canada. Le CRTC exerce ses activités indépendamment du gouvernement fédéral et met en œuvre les lois et règlements adoptés par le Parlement.
Conseil de la sécurité nationale (National Security Council)	CSN (NSC)	Comité du Cabinet créé en 2023 et présidé par le premier ministre pour prendre des décisions stratégiques sur les intérêts du Canada en matière de sécurité publique, de sécurité nationale, de politique étrangère et de renseignement.
Conseiller à la sécurité nationale et au renseignement auprès du premier ministre (National Security and Intelligence Advisor to the Prime Minister)	CSNR (NSIA)	Haut fonctionnaire qui donne des conseils stratégiques et opérationnels au premier ministre et au Cabinet en matière de sécurité nationale afin d'assurer la coordination de la réponse du gouvernement aux menaces. Reçoit de l'information de ses secrétariats et de la communauté de la sécurité et du renseignement. A maintenant le statut de sous-greffier au sein du Bureau du Conseil privé et relève du greffier du Conseil privé et secrétaire du Cabinet.

Terme	Sigle ou abréviation	Définition
Coordonnateur national de la lutte contre l'ingérence étrangère (National Counter Foreign Interference Coordinator)	CNLIE (NCFIC)	Poste créé en 2023 pour coordonner la réponse sur le plan des politiques du gouvernement du Canada en matière d'ingérence étrangère. Cela inclut le travail qui vise à améliorer la transparence de la réponse gouvernementale par le biais d'un dialogue public avec tous les Canadiens et Canadiennes, y compris les groupes des diasporas, les universités, les organisations non gouvernementales et d'autres partenaires nationaux et internationaux.
Décret (Order in council)	(OIC)	Instrument juridique faisant état d'une décision prise par la gouverneure en conseil en vertu d'un pouvoir prévu par une loi (ou, à l'occasion, de la prérogative royale). Toujours préparé sur recommandation du ministre responsable et n'entre en vigueur qu'une fois approuvé par la gouverneure générale.
Désinformation (Disinformation)		Informations fausses ou inexactes propagées délibérément dans le but de tromper ou d'induire en erreur. Voir aussi « Mésinformation ».
Directeur général des élections (Chief Electoral Officer)	DGE (CEO)	Chef d'Élections Canada. Chargé de la conduite des élections et de la conformité aux règles électorales. Relève directement du Parlement, et non du gouvernement.
Élections Canada (Elections Canada)		Entité responsable de l'administration des élections fédérales. Dirigée par le directeur général des élections (DGE). Fonctionne indépendamment du gouvernement.
Gendarmerie royale du Canada (Royal Canadian Mounted Police)	GRC (RCMP)	Service de police national du Canada. Prévient la criminalité et mène des enquêtes, assure le maintien de l'ordre, fait respecter les lois, contribue à la sécurité nationale, assure la sécurité des représentants de l'État désignés, des dignitaires étrangers et du corps diplomatique, et fournit un soutien opérationnel à d'autres services de police et organismes d'application de la loi au Canada et à l'étranger.

Terme	Sigle ou abréviation	Définition
Gouverneure en conseil (Governor in Council)	GEC (GIC)	Gouverneure générale agissant sur l'avis du Conseil privé du Roi pour le Canada. Par convention, la gouverneure générale n'exerce ses pouvoirs que sur l'avis des membres du Conseil privé du Roi, qui comprend les membres du Cabinet (voir la définition de « Conseil privé du Roi pour le Canada »). En pratique, la notion de gouverneure en conseil fait référence au Cabinet et à la Gouverneure générale. Les décisions de la gouverneure en conseil sont souvent rendues officiellement par des décrets.
Greffier du Conseil privé et secrétaire du Cabinet (Clerk of the Privy Council and Secretary to the Cabinet)	Greffier (Clerk)	Haut fonctionnaire du Bureau du Conseil privé qui exerce aussi les fonctions de secrétaire du Cabinet et de sous-ministre auprès du premier ministre.
Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (Security and Intelligence Threats to Elections Task Force)	Groupe de travail (SITE TF)	Groupe de travail gouvernemental composé de représentants des entités suivantes : • Service canadien du renseignement de sécurité (SCRS) • Centre de la sécurité des télécommunications (CST) • Affaires mondiales Canada (AMC) • Gendarmerie royale du Canada (GRC). Créé pour protéger les élections fédérales canadiennes contre l'ingérence étrangère.
Groupe des cinq (Five Eyes)		Alliance de renseignement composée de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis. Ces pays sont parties à l'accord multilatéral UK-USA, un traité de coopération commune en matière de renseignement d'origine électromagnétique.
Huis clos *(In camera)*		Terme juridique signifiant « en privé ». Par exemple, les audiences à huis clos sont des audiences qui se déroulent sans la présence du public ou des médias.
Hypertrucage (Deepfake)		Images, séquences vidéo ou audio synthétiques qui sont altérées ou générées numériquement à l'aide d'outils d'intelligence artificielle.

Terme	Sigle ou abréviation	Définition
Information classifiée (Classified information)		Information que le gouvernement déclare comme pouvant raisonnablement porter préjudice à l'intérêt national si elle est divulguée. Répartie en trois catégories selon les niveaux suivants : • Confidentiel (préjudice limité ou modéré) • Secret (préjudice grave) • Très secret (préjudice extrêmement grave).
Information cloisonnée (Compartmented information)		Information classifiée soumise à un système de contrôle supplémentaire (un cadre administratif) qui établit des normes pour l'accès, le marquage, le traitement et le contrôle de l'information.
Information protégée (Protected information)		Information dont la divulgation publique pourrait raisonnablement, selon le gouvernement, causer un préjudice à un intérêt autre que national. Elle comprend trois catégories : • Protégé A (préjudice limité ou modéré) • Protégé B (préjudice grave) • Protégé C (préjudice extrêmement grave).
Ingérence étrangère (Foreign Interference)	IE (FI)	Aux fins de la Commission, on entend par ingérence étrangère toute activité clandestine, trompeuse ou menaçante à laquelle se livrent un État étranger ou ceux qui agissent en son nom et qui s'avère préjudiciable aux intérêts du Canada.
Initiative de citoyenneté numérique (Digital Citizen Initiative)	ICN (DCI)	Programme du ministère du Patrimoine canadien officiellement établi en 2020 pour lutter contre la désinformation en ligne, soutenir la démocratie et promouvoir un écosystème d'information sain par le biais d'initiatives de recherche et de partenariats.

Terme	Sigle ou abréviation	Définition
Intelligence artificielle / Intelligence artificielle générative (Artificial Intelligence/Generative Artificial Intelligence)	IA / IA générative (AI / GenAI)	Technologie de l'information qui effectue des tâches dont la réalisation nécessiterait normalement la puissance du cerveau humain. L'IA générative est un type d'IA qui produit diverses formes de contenu telles que du texte, de la voix ou de l'audio, du code, des vidéos et des images. Elle apprend à partir du contenu existant et utilise les modèles et les structures pour générer du nouveau contenu, sur la base d'informations fournies par les utilisateurs.
Intervenant (Intervener)		Entité ayant la « qualité pour agir » (voir la définition) à titre d'intervenant auprès de la Commission sur l'ingérence étrangère, avec des droits de participation limités. Un intervenant est aussi un participant. A le droit de recevoir les avis d'audiences publiques de la Commission et d'y assister à titre de participant, de présenter des observations et de recevoir des pièces provenant des audiences publiques. Peut avoir d'autres droits s'ils sont expressément accordés par la Commissaire.
Mandat (Terms of Reference)	(ToR)	Mandat de la Commission sur l'ingérence étrangère énoncé dans le Décret C.P. n° 2023-0882 (ce décret a créé la Commission sur l'ingérence étrangère et a nommé la Commissaire).
Mécanisme de réponse rapide du G7 (G7 Rapid Response Mechanism)	MRR du G7 (G7 RRM)	Mécanisme du G7 (Canada, France, Allemagne, Italie, Japon, Royaume-Uni et États-Unis) visant à déceler les menaces étrangères contre les démocraties, et à y répondre. Le MRR du G7 est coordonné par le Secrétariat du MRR du G7, qui fait partie d'Affaires mondiales Canada.
Mémoire au Cabinet (Memorandum to Cabinet)	MC	Document écrit qui présente une initiative législative ou de politique, et qui est utilisé pour obtenir l'approbation du Cabinet.
Mésinformation (Misinformation)		Informations fausses ou inexactes (sans intention d'induire en erreur). Voir aussi « Désinformation ».

Terme	Sigle ou abréviation	Définition
Ministère de la Défense nationale (Department of National Defence)	MDN (DND)	Ministère fédéral de qui relèvent les Forces armées canadiennes, qu'il soutient.
Mesure de réduction de la menace (Threat reduction measure)	MRM (TRM)	Mesure opérationnelle prise par le Service canadien du renseignement de sécurité (SCRS) pour réduire les menaces à la sécurité du Canada, en vertu de l'article 12.1 de la *Loi sur le SCRS*, lequel exige que la mesure soit raisonnable et proportionnelle à la gravité de la menace.
Observatoire de l'écosystème médiatique (Media Ecosystem Observatory)	(MEO)	Organisation résultant d'une collaboration interdisciplinaire entre l'Université McGill et l'Université de Toronto qui étudie la santé de l'écosystème des médias. Il s'agit de l'organe de coordination du « Réseau canadien de recherche sur les médias numériques » (voir la définition).
Office de surveillance des activités en matière de sécurité nationale et de renseignement (National Security and Intelligence Review Agency)	OSSNR (NSIRA)	Organisme de surveillance statutaire externe créé par la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* et qui relève du Parlement. Examine les activités du gouvernement en matière de sécurité nationale et de renseignement et mène des enquêtes pour s'assurer qu'elles sont légales, raisonnables et nécessaires. Examine également les plaintes du public concernant les principales agences et activités de sécurité nationale.
Panel des cinq (Panel of Five or Panel)		Voir « Protocole public en cas d'incident électoral majeur ».
Participant		Individu ou entité ayant la « qualité pour agir » (voir la définition) auprès de la Commission sur l'ingérence étrangère, soit en tant que partie, soit en tant qu'intervenant.

Terme	Sigle ou abréviation	Définition
Partie (Party)		Individu ou entité ayant la « qualité pour agir » (voir la définition) auprès de la Commission sur l'ingérence étrangère et disposant de tous les droits de participation, notamment le droit de consulter les documents avant les audiences et d'interroger les témoins. Une partie est également un participant.
Patrimoine canadien (Canadian Heritage)		Ministère fédéral chargé de promouvoir l'identité et les valeurs canadiennes, le développement culturel et le patrimoine.
Persona non grata	PNG	Terme latin signifiant « personne indésirable ». En diplomatie, il fait référence à la pratique d'un État hôte qui demande à un diplomate étranger de quitter son territoire. Lorsqu'un État hôte déclare un diplomate « *persona non grata* », cela revient à l'expulser du pays.
Pouvoir exécutif (Executive branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir législatif et le pouvoir judiciaire. Chacun a des pouvoirs et des responsabilités différents, définis dans la Constitution. Le pouvoir exécutif met en œuvre les lois et les politiques. Le premier ministre et le Cabinet constituent le pouvoir exécutif du gouvernement.
Pouvoir judiciaire (Judicial branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir législatif et le pouvoir exécutif. Chacun a des pouvoirs et des responsabilités différents définis dans la Constitution. Le pouvoir judiciaire interprète et applique le droit. Le pouvoir judiciaire est constitué des tribunaux canadiens et il est indépendant du gouvernement.

Terme	Sigle ou abréviation	Définition
Pouvoir législatif (Legislative branch)		L'un des trois pouvoirs du régime gouvernemental canadien. Les deux autres sont le pouvoir exécutif et le pouvoir judiciaire. Chacun a des pouvoirs et des responsabilités différents définis dans la Constitution. Le pouvoir législatif crée les lois. Le Parlement (Sénat et Chambre des communes) constitue le pouvoir législatif du gouvernement fédéral.
Privilèges		
— Privilège du secret professionnel de l'avocat (Solicitor-client privilege)		Protège les communications (y compris les documents) entre un avocat et son client, produites pour une consultation ou un avis juridique, et destinées à demeurer confidentielles. Ce privilège appartient au client qui est la seule personne à pouvoir y renoncer.
— Privilège en vertu de l'article 38 de la *Loi sur la preuve au Canada* (Section 38 of the *Canada Evidence Act* privilege)		Protège les informations qui, si elles sont divulguées, sont susceptibles de porter préjudice aux relations internationales, à la défense nationale ou à la sécurité nationale. La protection de cette dernière s'appelle aussi « privilège de la sécurité nationale ». L'information protégée par l'article 38 ne peut être divulguée que si un tribunal l'ordonne ou si le procureur général du Canada y consent.
— Privilège parlementaire (Parliamentary privilege)		Ensemble des droits et immunités nécessaires pour que la Chambre des communes, le Sénat et leurs membres puissent exercer leurs fonctions. Par exemple : la liberté de parole à la Chambre et aux comités de la Chambre et le droit de ne pas être forcé à comparaître comme témoin devant un tribunal. Également, pouvoir de la Chambre et du Sénat de se protéger et de protéger les députés ou sénateurs et leurs procédures, de toute ingérence indue afin qu'ils puissent s'acquitter efficacement de leurs principales fonctions.

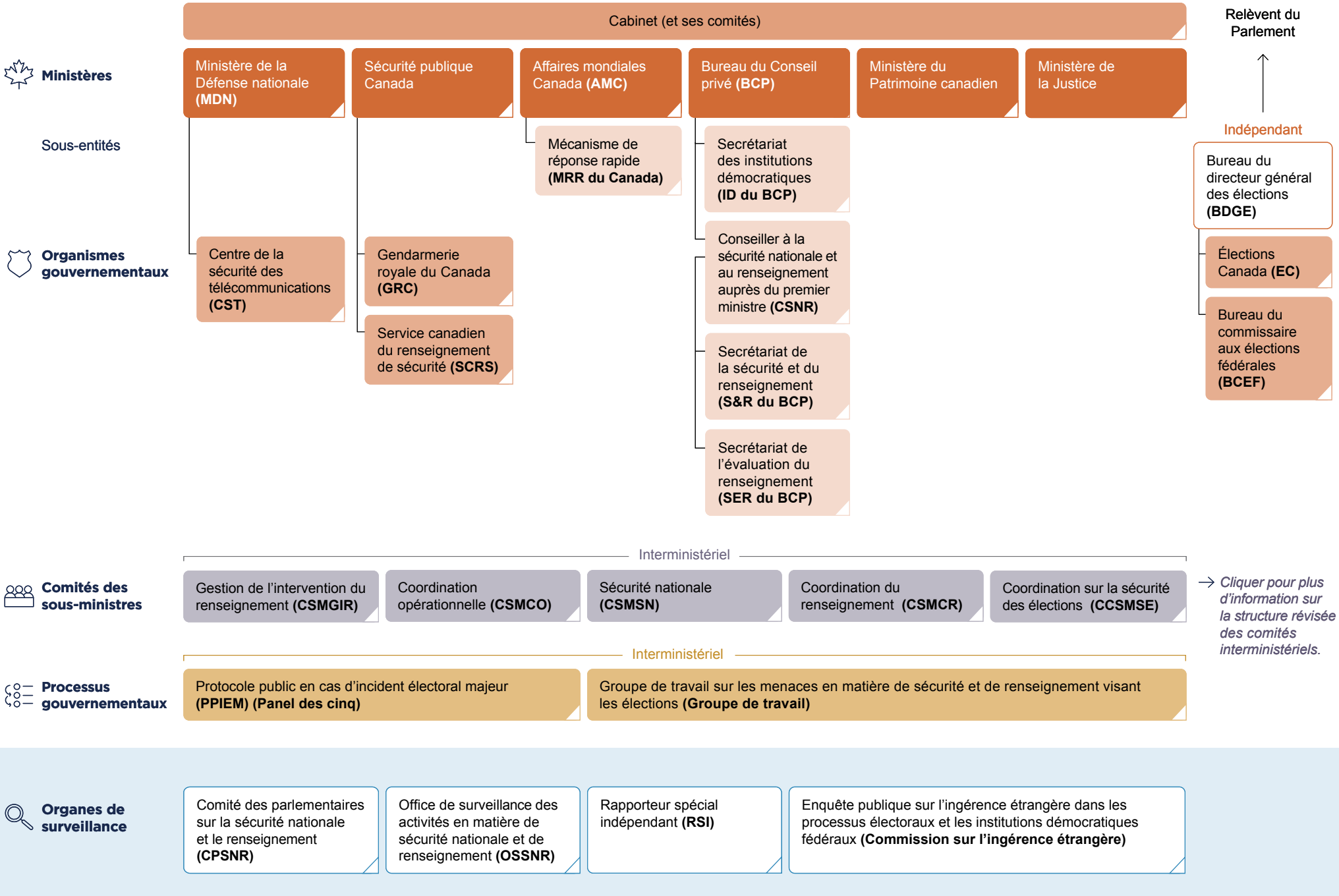
Terme	Sigle ou abréviation	Définition
— Privilège relatif au litige (Litigation privilege)		Protège les communications (y compris les documents) entre un avocat et ses clients ou une tierce partie, produites principalement en préparation d'un litige existant ou anticipé.
— Privilège relatif aux renseignements confidentiels du Cabinet (Cabinet confidences privilege)		Protège la confidentialité des échanges ayant lieu au sein du Cabinet. La protection des renseignements confidentiels du Cabinet est une règle de common law et une règle édictée à l'article 39 de la *Loi sur la preuve au Canada* et reconnue par la *Loi sur l'accès à l'information*. S'applique à toute personne qui participe aux réunions du Cabinet, même si elle n'est pas ministre.
— Protection des renseignements d'intérêt public (article 37 de la *Loi sur la preuve au Canada*) (Public interest privilege, section 37 of the Canada Evidence Act)		Protège l'information pour des raisons d'intérêt public déterminées. Tout intérêt public suffisamment important peut justifier de ne pas divulguer une information. Peut par exemple servir à protéger l'identité d'informateurs confidentiels, des informations sur des enquêtes criminelles en cours, des informations sur des techniques d'enquête sensibles, et des informations qui, si elles étaient divulguées, mettraient en danger la sécurité des titulaires d'une charge publique ou du public. Aussi appelée « immunité relative aux renseignements d'intérêt public ».
Procureur général du Canada (Attorney General of Canada)	PGC (AGC)	• Dirige des poursuites au nom du gouvernement du Canada. • Ne représente pas les ministères ou les organismes individuellement, mais leur offre des conseils juridiques et des services législatifs. • Agit dans l'intérêt du public, notamment en faisant respecter la Constitution, le principe de la primauté du droit et l'indépendance des tribunaux.

Terme	Sigle ou abréviation	Définition
Protocole public en cas d'incident électoral majeur (Critical Election Incident Public Protocol)	PPIEM (CEIPP)	Protocole appliqué pendant les élections fédérales par un groupe de cinq hauts fonctionnaires (Panel des cinq) : • le greffier du Conseil privé • le conseiller à la sécurité nationale et au renseignement auprès du premier ministre • le sous-ministre de la Justice et sous-procureur général du Canada • le sous-ministre de la Sécurité publique • le sous-ministre des Affaires étrangères. Destiné à protéger les élections fédérales contre les ingérences, y compris l'ingérence étrangère.
Qualité pour agir (Standing)		Possibilité de participer directement à des procédures (par exemple en cour ou devant des tribunaux administratifs) en bénéficiant de certains droits. Les *Règles de pratique et de procédure* de la Commission sur l'ingérence étrangère déterminent qui peut avoir la qualité pour agir comme partie ou comme intervenant (collectivement appelés les « participants ») dans les procédures de la Commission.
Répression transnationale (Transnational repression)	RTN (TNR)	Aux fins de la Commission, la répression transnationale se produit lorsque des pays font usage de mesures au-delà de leurs frontières pour intimider, réduire au silence, contraindre, harceler ou blesser des individus, en particulier des membres des communautés issues des diasporas au Canada.
Réseau canadien de recherche sur les médias numériques (Canadian Digital Media Research Network)	RCRMN (CDMRN)	Communauté de recherche au Canada visant à renforcer la résilience de l'information et à protéger la démocratie canadienne. Le réseau est coordonné par l'Observatoire des écosystèmes médiatiques (voir la définition).
Sanction royale (Royal assent)		Octroyée lorsque la gouverneure générale approuve un projet de loi adopté par le Parlement, ce qui en fait une loi fédérale.

Terme	Sigle ou abréviation	Définition
Secrétariat de l'évaluation du renseignement (Intelligence Assessment Secretariat)	SER du BCP (PCO-IAS)	Unité du Bureau du Conseil privé chargée de l'analyse et de l'évaluation stratégique du renseignement collecté par les agences de sécurité et de renseignement. Fournit des analyses et des évaluations au premier ministre, au Cabinet, au greffier du Conseil privé et secrétaire du Cabinet et aux hauts fonctionnaires du gouvernement.
Secrétariat de la sécurité et du renseignement du Bureau du Conseil privé (Security and Intelligence Secretariat of the Privy Council Office)	S et R du BCP (PCO-S&I)	Secrétariat du Bureau du Conseil privé qui offre des conseils stratégiques et de l'aide au conseiller à la sécurité nationale et au renseignement auprès du premier ministre afin qu'il l'informe, ainsi que le Cabinet, sur les principales questions de sécurité nationale. Joue un rôle de coordination lorsque le Cabinet est saisi de questions de sécurité nationale ou de renseignement. Collabore avec Sécurité publique Canada et d'autres ministères pour organiser et appuyer les réunions régulières de la haute gouvernance consacrées aux menaces d'ingérence étrangère et aux mesures à prendre.
Secrétariat des institutions démocratiques du Bureau du Conseil privé (Democratic Institutions Secretariat of the Privy Council Office)	ID du BCP (PCO-DI)	Secrétariat du Bureau du Conseil privé qui fournit un soutien et des conseils en matière de politiques au premier ministre et au ministre des Institutions démocratiques sur les enjeux qui ont des répercussions sur les institutions démocratiques canadiennes.
Sécurité publique Canada (Public Safety Canada)	SITE TF (Groupe de travail)	Ministère fédéral responsable de la gestion de la sécurité publique, de la sécurité nationale et des urgences.
Sergent d'armes (Sergeant-at-Arms)	(SAA)	Exerce plusieurs fonctions protocolaires à la Chambre des communes et est responsable, à titre de directeur de la sécurité institutionnelle, de la sécurité de la Chambre et de ses membres à l'extérieur de la Colline du Parlement.

Terme	Sigle ou abréviation	Définition
Service canadien du renseignement de sécurité (Canadian Security Intelligence Service)	SCRS (CSIS)	Organisme du gouvernement fédéral régi par la *Loi sur le Service canadien du renseignement de sécurité*. • Enquête sur les activités qui pourraient constituer une menace pour la sécurité du Canada et en fait rapport au gouvernement. • Peut prendre des mesures visant à réduire les menaces pour la sécurité du Canada. • Peut aussi prêter assistance à certains ministres pour collecter du renseignement étranger au Canada.
Sources ouvertes (Open source)	PROC	Information accessible au public.

Les principales entités fédérales chargées de répondre à l'ingérence étrangère



Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux