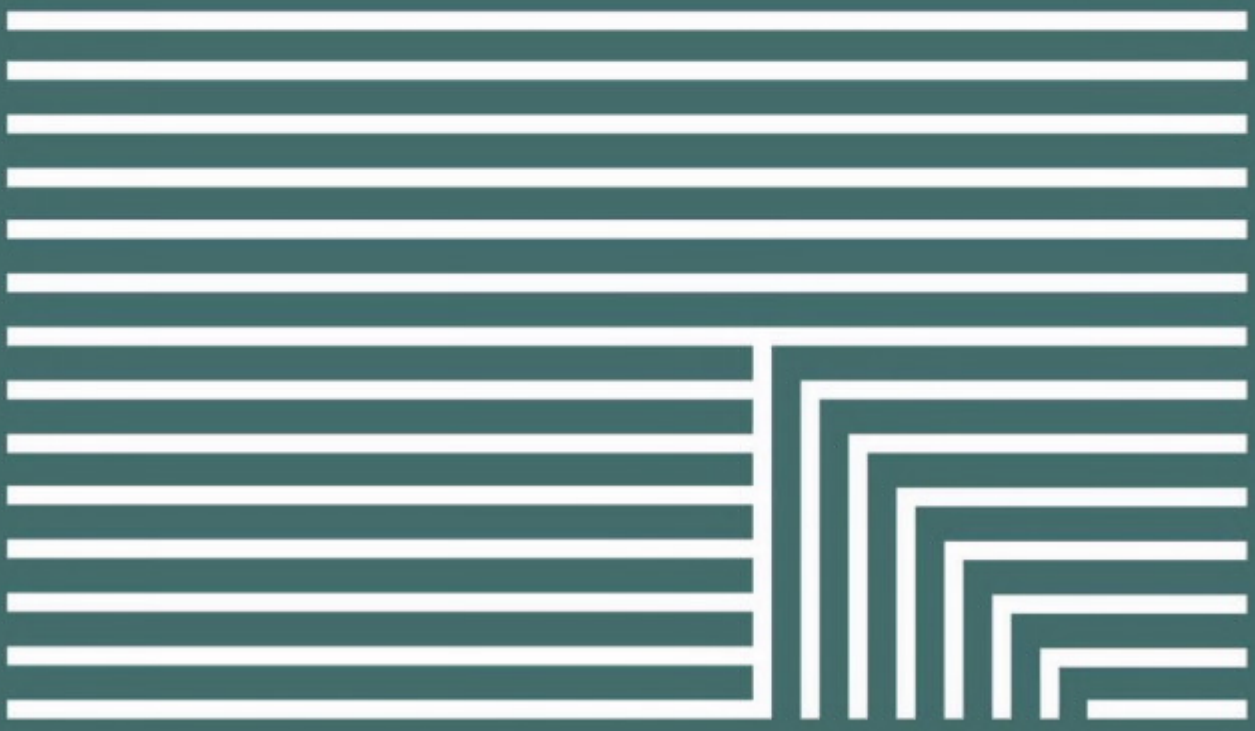
Protecting Democracy Unit | Unité pour la protection de la démocratie

Groupe de coordination de direction pour la protection de la démocratie

Mardi, 16 mai 2023

15h00 – 16h00

80, Wellington, Ottawa, ON



Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

Canada

Protecting Democracy Unit
Unité pour la protection de la démocratie

Table des matières

Unité pour
la protection de
la démocratie
—
Protecting
Democracy
Unit

Ordre du jour - Groupe de coordination de direction pour la protection de la démocratie

ITEMS À L'ORDRE DU JOUR	DURÉE
1. Introduction - Unité pour la protection de la démocratie (UPLD)	5 min.
2. Mesures pour protéger la démocratie canadienne - Activités à venir concernant le Plan pour protéger la démocratie (UPLD) - Tour de table (tous)	25 min.
3. Survol du rapport Contrer une menace en évolution: mise à jour sur les recommandations visant à prévenir l'ingérence étrangère dans les institutions démocratiques canadiennes - UPLD et Groupe de travail sur l'ingérence étrangère	10 min.
4. Structure de gouvernance et prochaines étapes - Tous	10 min.

Unité de protection de la démocratie

L'Unité pour la protection de la démocratie (UPLD)

- L'UPLD a été créée dans le cadre du Budget de 2022 en vue de coordonner,
- d'élaborer et de mettre en œuvre des mesures pangouvernementales visant à
- lutter contre la désinformation et à protéger notre démocratie

Coordination

Mettre en place une réponse interministérielle intégrée

Recherche et intégration des politiques

Améliorer la compréhension et l'utilisation des faits probants au sein du gouvernement

Mobilisation

Apprendre des autres, établir des partenariats et mobiliser la société civile

Communications : Observation et réponse

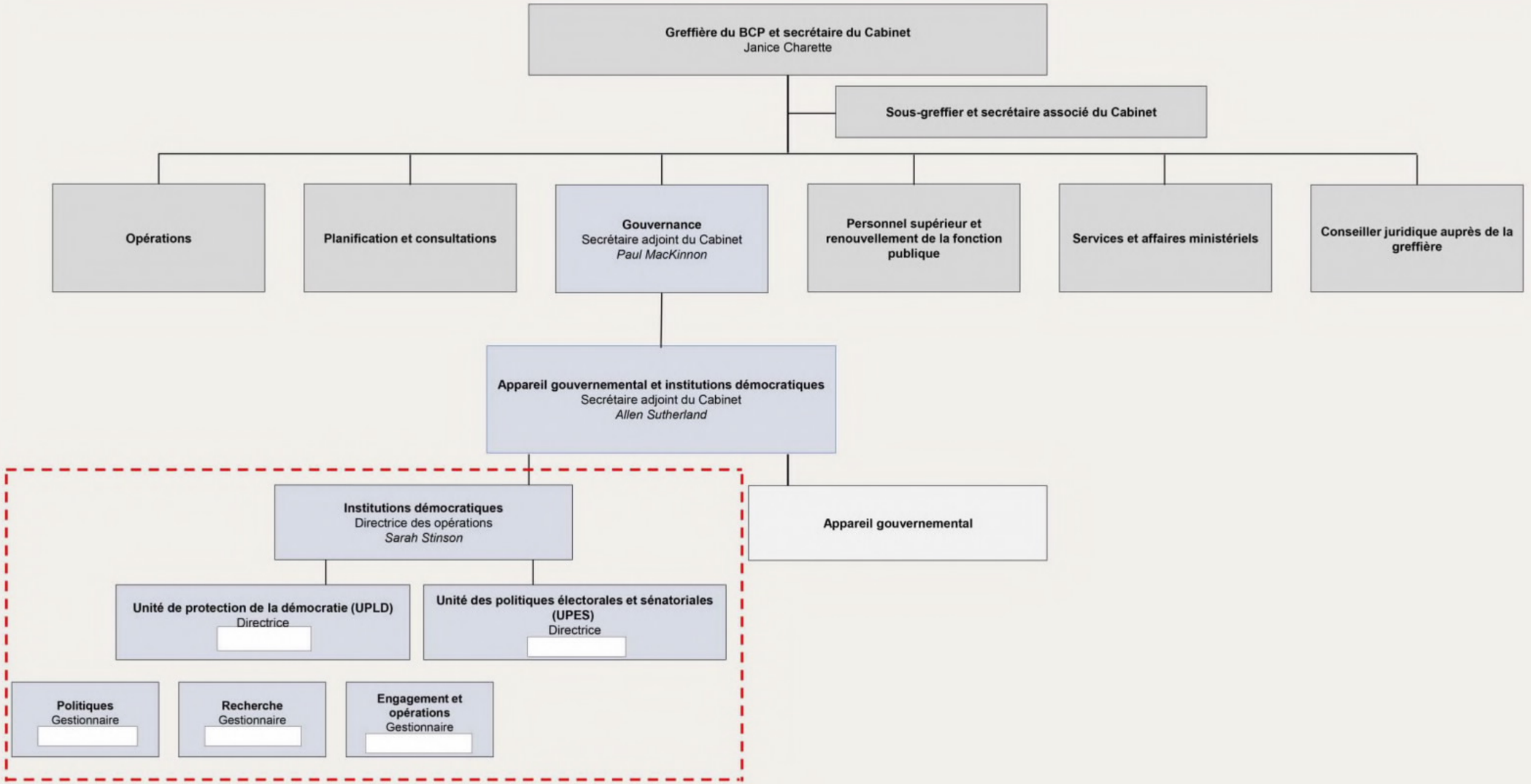
Élaborer un cadre pour les interventions de communication

Parmi ses champs d'activité figurent les suivants :

- L'amélioration de la compréhension de la mésinformation et de la désinformation au Canada.
- La création du Réseau canadien de recherches sur les médias numériques (financé par le biais de l'Initiative de citoyenneté numérique de Patrimoine canadien).
- L'amélioration du Plan pour protéger la démocratie canadienne
- La coordination interministérielle et la gouvernance.
- L'appui aux efforts gouvernementaux pour prévenir et contrer l'ingérence étrangère.
- La collaboration avec l'Organisation de coopération et de développement économiques, les provinces et les territoires et d'autres organisations de la société civile et du secteur public.
- La favorisation de la sensibilisation et la compréhension des menaces à la démocratie et des facteurs qui érodent la confiance envers le gouvernement, y compris la mésinformation et la désinformation.
- Le développement d'outils pour aider à identifier et à mieux contrer les menaces à la démocratie et leur partage

Unité pour la protection de la démocratie

La position du UPLD dans l'organigramme du BCP



MESURES DE LUTTE CONTRE L'INGÉRENCE ÉTRANGÈRE DANS LES ÉLECTIONS

2016-2017

Mise en place du Mécanisme de réponse rapide (MRR)

- Sommet du G7, Charlevoix

Loi sur la modernisation des élections - Sanction royale

- Resserrement des mesures de financement politique
- Transparence accrue des publicités
- Nouveaux pouvoirs au Commissaire aux élections fédérales
- Nouvelles infractions, notamment l'utilisation non autorisée d'ordinateurs

Modifications à la LEC

- *Loi modifiant la Loi électorale du Canada (financement politique)* - Adoption d'un régime concernant la publicité et la production de rapports sur les activités de financement auxquelles participent des ministres, des chefs de parti ou des candidats à la direction

2018

Initiatives du Centre de la sécurité des télécommunications (CST)

Production de rapport sur les menaces

- Cybermenaces contre le processus démocratique du Canada

Services offerts aux partis politiques :

- Séance d'information aux représentants des partis enregistrés présents sur leur rapport public sur les menaces

Services offerts à Élections Canada :

- Organisation de séances d'information sur les rapports de menaces

2019

Plan de protection de la démocratie

Quatre piliers :

- **Améliorer l'état de préparation des citoyens**
  - Protocole public en cas d'incident électoral majeur
  - Initiative de citoyenneté numérique
- **Renforcer la préparation organisationnelle**
  - Séances d'information classifiées sur les menaces et sur la cybersécurité offertes aux partis politiques
- **Lutter contre l'ingérence étrangère**
  - Groupe de travail sur les MSRE, MRR du G7
- **Compter sur les plateformes de médias sociaux pour qu'elles agissent**
  - Déclaration du Canada sur l'intégrité électorale en ligne

Budget 2019

Patrimoine canadien :

- 19,4 millions de dollars sur 4 ans

Centre de la sécurité des télécommunications

- 4,2 millions de dollars sur 3 ans

Affaires mondiales Canada :

- 2,1 millions de dollars sur 3 ans

Services canadiens de renseignement de sécurité :

- 23 millions de dollars sur 5 ans

Mise à jour du rapport 2017 du CST

Le point sur les cybermenaces contre le processus démocratique du Canada en 2019 :

- Offre un aperçu de l'environnement de menaces

Soutien à l'appel de Paris pour la confiance et la sécurité dans le cyberespace (Appel de Paris)

- Neuf principes axés sur l'amélioration de la cyberhygiène et la protection du Canada contre l'ingérence étrangère

Ateliers de l'Appel de Paris

Six ateliers :

- Axés sur l'amélioration de l'échange multilatéral d'information, la définition de l'ingérence étrangère, les éventualités reliées à la COVID-19, l'atténuation et la réponse, la lutte contre l'ingérence dans les infrastructures électorales et la responsabilisation des citoyens

Protocole public en cas d'incident électoral majeur (Protocole)

- Publication de l'évaluation du Protocole par un ancien haut fonctionnaire, James Judd.
- Constatation générale que le Protocole a été mis en œuvre avec succès

2020

Mise à jour du Plan pour protéger la démocratie canadienne

- **Nouveau pilier : Bâtir un écosystème de l'information sain**

Rapports publiés

- **Rapport du SCRS**
  - Menaces d'ingérence étrangère visant les processus démocratiques du Canada
- **Rapport du SCRS**
  - Interférence étrangère et vous
- **Rapport du CST**
  - Cybermenaces contre le processus démocratique du Canada: Mise à jour de juillet 2021
- **Rapport des signataires de l'Appel de Paris pour le principe de défense des processus électoraux**
  - Recueil sur la défense des processus électoraux

MRR d'Affaires mondiales Canada

- Réunion des ministres des affaires étrangères et du développement du G7 à Londres, et engagement à produire des rapports thématiques annuels
- Publication du rapport annuel du MRR du G7 de 2021

2021

Budget 2022

- 2 mill de dollars par année pour le Bureau du Conseil privé afin de coordonner, d'élaborer et de mettre en œuvre des mesures pangouvernementales pour lutter contre la désinformation et à protéger la démocratie
- 13,4 mill de dollars sur 5 ans et 2,8 millions de dollars par année suivante pour renouveler et élargir le MRR

Énoncé économique d'automne

- Renouvellement de l'Initiative de citoyenn-eté numérique

2022

Protocole public en cas d'incident électoral majeur (Protocole)

- Publication de l'évaluation du Protocole par un ancien haut fonctionnaire, Morris Rosenberg
- A permis de constater que le Protocole fonctionnait bien et devrait être conservé moyennant quelques améliorations proposées

Projets en cours

- Recherche visant à dresser un portrait global de la désinformation au Canada
- Engagement continu avec les intervenants pertinents de l'industrie, les provinces et territoires, du milieu universitaire et de la société civile

2023

Unité pour la protection de la démocratie

Plan pour protéger la démocratie canadienne

Initiatives en cours pour protéger la démocratie et contrer la mésinformation et la désinformation

Une stratégie à quatre piliers - accent important mis sur les élections et la période électorale

Accroître la résilience citoyenne

- Protocole public en cas d'incident électoral majeur (groupe de 5)
- Rapports publics sur les menaces au processus démocratique du Canada (CST, SCRS)
- Initiative de citoyenneté numérique (financement des connaissances numériques, des nouvelles et des compétences civiques pour la société civile)

Améliorer la préparation organisationnelle

- Séances d'information classifiées sur les menaces à l'intention des partis politiques
- Directives en matière de cybersécurité à l'intention des partis politiques
- Ligne d'assistance sur la cybersécurité pour les partis politiques pendant la campagne électorale
- Collaborer avec Élections Canada

Lutter contre l'ingérence étrangère

- Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (CST, SCRS, AMC, GRC)
- Mécanisme d'intervention rapide

Créer un écosystème d'information sain

- Déclaration du Canada sur l'intégrité électorale en ligne (avec Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter, YouTube)

Créé en 2019 et renouvelé en 2021

48 millions de dollars sur cinq ans dans le cadre du budget de 2019

Document d'information
Mesures prises afin de protéger la démocratie au Canada

- Le Plan pour protéger la démocratie canadienne est une approche pangouvernementale et sociétale visant à protéger les élections et les institutions démocratiques du Canada contre toute ingérence.

- Le Plan a d'abord été mis en œuvre avant l'élection générale de 2019, puis renouvelé et mis à jour avant l'élection de 2021, à la suite d'évaluations approfondies.

- Le Plan comprend des activités réparties en quatre piliers :
    - **Améliorer l'état de préparation des citoyens** en améliorant les aptitudes en pensée critique et en littératie numérique de la population canadienne, et en établissant le Protocole public en cas d'incident électoral majeur afin d'assurer que les Canadiennes et Canadiens sont avisés de toute tentative sérieuse d'ingérence envers leur capacité à tenir des élections libres et impartiales.
    - **Renforcer la préparation organisationnelle** en offrant des séances d'information classifiées sur les menaces aux partis politiques représentés à la Chambre des communes, en offrant des conseils en matière de cybersécurité aux partis politiques et en collaborant avec Élections Canada.
    - **Lutter contre l'ingérence étrangère** en activant le mécanisme de réponse rapide du G7 et en tirant profit du nouveau Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections.
    - **Bâtir un écosystème de l'information sain** en renouvelant et en élargissant les engagements volontaires des plateformes numériques et des médias sociaux pour améliorer la transparence, l'authenticité et l'intégrité de leurs systèmes par l'entremise de la Déclaration du Canada sur l'intégrité électorale en ligne.

- **Le budget 2022** a annoncé des investissements clés dans le Plan, y compris le renouvellement du mécanisme de réponse rapide (13,4 millions de dollars sur cinq ans et 2,8 millions de dollars par la suite) et 10 millions de dollars sur cinq ans (et 2 millions de dollars par la suite) en nouvelles ressources pour le Bureau du Conseil privé afin de coordonner, d'élaborer et de mettre en œuvre des mesures pangouvernementales conçues pour lutter contre la désinformation et protéger la démocratie.

Les activités particulières suivantes ont été entreprises dans le cadre de chacun des quatre piliers.

1. ***Améliorer l'état de préparation des citoyens***

- Mise en œuvre de l'**Initiative de citoyenneté numérique**, dirigée par Patrimoine canadien, pour appuyer les programmes et les outils de nouvelles numériques et de littératie civique pour améliorer la résilience des Canadiennes et des Canadiens contre la désinformation (Patrimoine canadien).
- Publication de **rapports publics sur les menaces qui pèsent sur le processus démocratique du Canada,** notamment les mises à jour de 2019 et 2021 sur les *Cybermenaces contre le processus démocratique du Canada* (Centre de la sécurité des télécommunications) et un rapport de 2021 sur les *Menaces d'ingérence étrangère visant les processus démocratiques du Canada* (Service canadien du renseignement de sécurité).
- Adoption du **Protocole public en cas d'incident électoral majeur**. Ce processus a été mis en place pour communiquer de façon claire, transparente et impartiale avec les Canadiennes et les Canadiens pendant la période de transition lorsqu'il est question d'incidents qui menacent l'intégrité des élections (Bureau du Conseil privé).
- Augmentation de la portée et du champ d'action de l'initiative **Pensez cybersécurité**, qui est une campagne nationale de sensibilisation au sujet de la cybersécurité et des mesures simples à prendre pour se protéger en ligne, en établissant davantage de liens entre les cybermenaces et les processus démocratiques du Canada (Centre de sécurité des télécommunications).

2. ***Renforcer la préparation organisationnelle***

- Présentation de **séances d'information classifiées sur les menaces à l'intention des principaux dirigeants** des partis politiques représentés à la Chambre des communes afin de promouvoir leur connaissance de la situation et de les aider à renforcer les pratiques et les comportements de sécurité interne (Bureau du Conseil privé, Centre de la sécurité des télécommunications, Service canadien du renseignement de sécurité, Gendarmerie royale du Canada).
- Formulation d'**avis et de conseils techniques** supplémentaires **en matière de cybersécurité** à l'intention des partis politiques pour améliorer la sécurité (Centre de sécurité des télécommunications).

- Meilleure coordination à l'échelle du gouvernement, y compris un engagement approfondi avec Élections Canada, qui est responsable de la conduite opérationnelle des élections, pour assurer une intégration transparente avec l'appareil de sécurité nationale du gouvernement du Canada.

3. Lutter contre l'ingérence étrangère

- Le **Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections** vise à améliorer la sensibilisation aux menaces étrangères et à soutenir l'évaluation et l'intervention connexes, ainsi que le travail continu des agences de sécurité pour empêcher les activités secrètes, clandestines ou criminelles d'interférer avec l'élection (Centre de la sécurité des télécommunications, Service canadien du renseignement de sécurité, Gendarmerie royale du Canada et Affaires mondiales Canada).

- Le **Mécanisme de réponse rapide du G7** améliore la coordination de la réponse aux menaces à la démocratie entre les démocraties du G7 et pour surveiller les acteurs malveillants sur les médias sociaux (Affaires mondiales Canada).

4. Bâtir un écosystème de l'information sain

- Établissement d'une compréhension commune des plateformes quant à leurs responsabilités dans l'espace démocratique en ligne par l'entremise de la Déclaration du Canada sur l'intégrité électorale en ligne, qui a été adoptée en 2019 et mise à jour en 2021, avec de nouveaux engagements et signataires (Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter, YouTube).

Document d'information
Protocole public en cas d'incident électoral majeur

Aperçu

- Le Protocole public en cas d'incident électoral majeur (le Protocole) établit un mécanisme permettant à de hauts fonctionnaires (appelés le groupe d'experts) de communiquer de façon claire, transparente et impartiale avec la population canadienne pendant une élection en cas d'incident ou d'une série d'incidents menaçant l'intégrité d'une élection fédérale.

- Mis en œuvre pour la première fois en 2019, le Protocole a fait l'objet d'une évaluation indépendante à la suite de la 43e élection générale et a été renouvelé et actualisé pour les prochaines élections.

- Le seuil pour justifier une annonce du groupe d'experts est très élevé et se limite à des circonstances exceptionnelles qui pourraient nuire à la capacité des Canadiennes et des Canadiens de tenir des élections libres et justes, que ces circonstances découlent d'un seul incident ou d'une accumulation d'incidents. Les incidents en question poseraient un risque important d'atteinte aux droits démocratiques de la population canadienne ou pourraient miner la crédibilité de l'élection.

- Pendant les élections générales de 2019 et 2021, le groupe d'experts a participé à des séances d'information régulières sur la sécurité. Le groupe d'experts n'a pas observé d'activités répondant au seuil d'une annonce publique.

Évaluation du Protocole après l'élection de 2019 par Jim Judd

- L'évaluation du Protocole à la suite de l'élection fédérale de 2019 a été menée par James Judd, ancien fonctionnaire canadien et directeur du Service canadien du renseignement de sécurité (SCRS). La version classifiée de son rapport a été fournie au premier ministre et au Comité des parlementaires sur la sécurité nationale et le renseignement, conformément à la Directive du Cabinet. Une version non classifiée du rapport d'évaluation est également accessible au public depuis novembre 2020.

- D'après l'ensemble des conclusions de l'évaluation, la mise en œuvre du Protocole était réussie, et sa mise en place est recommandée pour la prochaine élection générale.

- Il y est aussi recommandé que le groupe d'experts demeure composé des titulaires des mêmes postes. Ces membres sont la greffière du Conseil privé, la conseillère 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 et le sous-ministre des Affaires étrangères du Canada.

- Il a également été recommandé de conserver le même seuil justifiant une annonce. Un seuil élevé permet d'éviter que le groupe d'experts n'intervienne fréquemment dans toute élection générale.

Modifications apportées au Protocole en 2021

- Le Cabinet a publié une directive modifiée en mai 2021, retirant la référence à l'application du Protocole pendant une élection générale en particulier. Par conséquent, il sera en place pour les prochaines élections générales jusqu'à ce qu'il soit révoqué ou modifié par le Cabinet.

- D'autres modifications importantes ont été apportées :
    - correspondance de la période d'application du Protocole à celle de la convention de transition;
    - disposition explicite permettant au groupe d'experts de consulter le directeur général des élections, le cas échéant;
    - possibilité pour les partis politiques d'alerter les organismes de sécurité des incidents qui pourraient menacer une élection libre et juste;
    - reconnaissance de la capacité du groupe d'experts à examiner les incidents d'ingérence à l'échelle nationale, ainsi qu'à recevoir des renseignements de sources autres que les organismes de sécurité, à sa discrétion.

Évaluation du Protocole après l'élection de 2021 par Morris Rosenberg

- L'évaluation de 2021, menée par M. Morris Rosenberg, qui a été sous-ministre de 1998 à 2013, a été rendue publique le 28 février 2023. Elle a permis de constater que le PPIEM fonctionnait bien et devrait être conservé moyennant quelques améliorations proposées. Le gouvernement du Canada examinera les 16 recommandations avec soin et y répondra en temps opportun.

ANNEXE

Directive du Cabinet sur le Protocole public en cas d'incident électoral majeur

1.0 Introduction

L'une des responsabilités fondamentales du gouvernement fédéral consiste à protéger et à préserver les institutions et les pratiques démocratiques du Canada.

Les évaluations des menaces relatives à la sécurité nationale et du risque, ainsi que les expériences vécues par nos principaux alliés internationaux, indiquent que les élections générales au Canada pourraient être vulnérables à l'ingérence dans un certain nombre de domaines. Pour cette raison, d'importants travaux ont été entrepris au sein du gouvernement fédéral en vue de protéger et de défendre les systèmes et les processus électoraux. Dans ce contexte, le gouvernement du Canada a établi le Protocole public en cas d'incident électoral majeur afin d'informer la population canadienne de façon cohérente et uniforme, durant la période d'application de la convention de transition, des incidents pouvant menacer la tenue d'élections libres et justes au pays.

2.0 Objectif

La *Directive du Cabinet sur le Protocole public en cas d'incident électoral majeur* énonce les attentes des ministres en ce qui touche les directives générales et les principes à suivre pour informer le public de tout incident pouvant menacer la tenue d'élections libres et justes au pays durant la période d'application de la convention de transition.

Le Protocole est conforme à la convention de transition, qui suit le principe selon lequel le gouvernement doit faire preuve de retenue et restreindre la prise de décisions en matière de politiques, de dépenses et de nominations pendant la période électorale, sauf si cela est impératif sur le plan de l'intérêt national ou en cas de situation d'urgence. La convention de transition commence généralement à la dissolution du Parlement. Elle prend fin lorsqu'un nouveau gouvernement est assermenté ou qu'un résultat ramenant un gouvernement en place est clair.

Pendant la période d'application de la convention de transition, toute annonce jugée nécessaire doit être faite au nom d'un ministère, afin de faire la distinction entre les activités officielles du gouvernement et les activités partisanes.

3.0 Champ d'application

Le Protocole public en cas d'incident électoral majeur aura un champ d'application limité. Il sera uniquement appliqué pour faire face aux incidents qui surviendront durant la période d'application de la convention de transition et qui ne relèvent pas

des domaines de responsabilité d'Élections Canada (en ce qui concerne l'administration de l'élection, tels qu'énoncé dans la *Loi électorale du Canada*). Tout incident se produisant hors de la période d'application de la convention de transition sera géré dans le cadre des activités courantes du gouvernement du Canada.

4.0 Groupe d'experts

Le Protocole sera administré par un groupe de hauts fonctionnaires qui, en collaboration avec les agences de sécurité nationale relevant du mandat actuel de leurs organisations respectives, seront chargés de déterminer si les critères rendant nécessaire que les Canadiens soient informés sont remplis, que ce soit dans le cas d'un incident isolé ou de l'accumulation d'incidents distincts.

Ce groupe d'experts réunira :

- 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.

5.0 Processus

Le Protocole établit la procédure à suivre pour informer les Canadiens de tout incident pouvant menacer la tenue d'élections libres et justes au pays, si cela était nécessaire.

Durant la période d'application de la convention de transition, le protocole à suivre pour toute annonce publique est le suivant :

1. Les agences de sécurité nationale donneront des séances d'information régulières au groupe d'experts sur les développements touchant la sécurité nationale et les menaces possibles pesant sur l'intégrité de l'élection. Le groupe d'experts pourrait également recevoir des informations et des conseils de sources autres que les agences de sécurité et de renseignement.
2. Les partis politiques recevront des instructions sur la manière de signaler toute interférence qu'ils pourraient subir pendant l'élection.
3. Les dirigeants des agences de sécurité nationale (Centre de la sécurité des télécommunications, Service canadien du renseignement de sécurité, Gendarmerie royale du Canada ou Affaires mondiales Canada, travaillant dans le cadre de leurs mandats respectifs), s'ils sont informés d'une ingérence dans lors d'une élection

générale, examineront en consultation concertée, tous les moyens possibles pour remédier efficacement à la situation. Dans le cadre de ce processus, ils informeront le groupe d'experts. À moins de motifs impérieux liés à la sécurité nationale et à l'intérêt public, les agences informeront directement la partie touchée de l'incident (p. ex. un candidat, un parti politique ou Élections Canada).

4. Le groupe d'experts évaluera les incidents en vue de déterminer si les critères rendant nécessaire que les Canadiens soient informés sont remplis (tels qu'ils sont énoncés à l'article 6 ci-dessous). Le groupe d'experts prendra ses décisions par consensus, en tirant parti de l'expertise de l'ensemble du gouvernement, y compris des agences de sécurité nationale dans l'exercice de leur mandat. Le groupe d'experts pourrait consulter le directeur général des élections (DGE) pour s'assurer que les mandats sont respectés si des questions d'interférence se posent qui peuvent concerner à la fois le groupe d'experts et le DGE.
5. Si une annonce publique est jugée nécessaire, le groupe d'experts en informera le premier ministre, les chefs des autres grands partis (ou les représentants principaux désignés des partis ayant reçu leur autorisation de sécurité, parrainés par le BCP), ainsi qu'Élections Canada. Tous ces dirigeants recevront la même séance d'information à ce sujet.
6. Immédiatement après avoir informé le premier ministre, les autres partis politiques et Élections Canada, le greffier du Conseil privé, au nom du groupe d'experts, pourrait soit publier une déclaration, ou demander aux dirigeants responsables de tenir une conférence de presse pour informer les Canadiens de l'incident.

6.0 Critères à remplir pour informer le public

Une annonce publique durant la période d'application de la convention de transition ne sera faite que si le groupe d'experts détermine qu'il s'est produit un incident ou une accumulation d'incidents qui menace la tenue d'élections libres et justes au pays.

Une grande rigueur sera requise pour établir si les critères sont remplis. Différents facteurs pourraient être examinés en vue de prendre une décision à ce sujet, par exemple :

- la mesure dans laquelle l'incident ou l'accumulation d'incidents compromet la capacité des Canadiens de participer à des élections libres et justes;
- la possibilité que l'incident ou l'accumulation d'incidents mine la crédibilité de l'élection;
- le degré de confiance des responsables à l'égard du renseignement ou de l'information.

Le groupe d'experts, de par sa composition particulière, disposera d'une vue d'ensemble englobant la sécurité nationale, les affaires étrangères, la gouvernance démocratique et les considérations juridiques, y compris une conception claire des droits démocratiques consacrés par la *Charte canadienne des droits et libertés*.

Un événement perturbateur ou un incident d'interférence peut émaner d'acteur nationaux et/ou étrangers. Il pourrait être difficile, voire impossible, d'attribuer la responsabilité de tentatives d'interférence dans les délais permis par les événements, étant donné les malversations et la désinformation susceptibles d'être impliquées dans les tentatives d'exercer une influence néfaste sur les élections. De plus, il est possible que des acteurs étrangers travaillent en collaboration avec des acteurs nationaux ou par l'entremise de ces derniers. En fin de compte, c'est l'incidence sur la tenue d'élections libres et justes au Canada qui permettra de déterminer si les critères sont remplis et qu'une annonce publique est requise. Il est entendu que les intérêts de la population canadienne – et la démocratie – sont le mieux servis par les campagnes électorales qui offrent un large éventail de débats et de positions différentes. Le Protocole n'a pas pour but de limiter le débat démocratique et ne sera pas utilisé à cette fin.

7.0 Annonce

L'annonce serait centrée sur les éléments suivants :

a. la notification de l'incident;

b. les renseignements connus à propos de l'incident (selon ce qui est jugé approprié);

c. les mesures que les Canadiens devraient prendre pour se protéger (s'assurer qu'ils sont bien informés, avoir de bonnes pratiques informatiques, etc.), le cas échéant.

8.0 Pouvoirs actuels

Aucun élément de la présente Directive ne modifie ou n'élargit de quelque façon que ce soit le mandat de chacune des agences de sécurité nationale ou de tout autre ministère ou organisme. Plus précisément, aucune disposition du Protocole n'a préséance sur l'indépendance de la GRC.

9.0 Évaluation

Après l'élection de 2019, un rapport indépendant sera préparé pour évaluer la mise en œuvre du Protocole public en cas d'incident électoral majeur et la mesure dans laquelle il a permis de gérer efficacement les menaces pesant sur l'élection de 2019. Ce rapport sera présenté au premier ministre et au Comité des parlementaires sur la sécurité nationale et le renseignement. Une version publique sera aussi préparée. Ces rapports ont pour but d'aider à déterminer si des ajustements doivent être apportés au protocole pour le renforcer.

Government of Canada / Gouvernement du Canada

PROTOCOLE PUBLIC EN CAS D'INCIDENT ÉLECTORAL MAJEUR

PROTOCOLE PUBLIC EN CAS D'INCIDENT ÉLECTORAL MAJEUR

1 PRISE DE CONNAISSANCE

LE GOUVERNEMENT DU CANADA PREND CONNAISSANCE D'UNE TENTATIVE D'INGÉRENCE LORS DE L'ÉLECTION PENDANT LA PÉRIODE ÉLECTORALE.

2 DIFFUSION DE L'INFORMATION

LES DIRIGEANTS DES ORGANISMES DE SÉCURITÉ NATIONALE INFORMENT LE GROUPE D'INTERVENTION EN CAS D'INCIDENT CRITIQUE LIÉ AUX ÉLECTIONS :

Greffier du Conseil privé

Conseiller à la sécurité nationale et au renseignement

Sous-ministres de la Justice, de la Sécurité publique et d'Affaires mondiales Canada

3 ÉVALUATION DE LA MENACE

SI LE GROUPE DÉTERMINE QUE LA TENTATIVE D'INGÉRENCE POSE UNE MENACE GRAVE À LA TENUE D'UNE ÉLECTION LIBRE ET JUSTE :

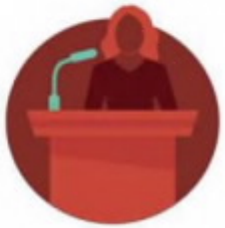
Le groupe signale l'incident au premier ministre, aux responsables des partis politiques ainsi qu'à Élections Canada, et les informe qu'une conférence de presse aura lieu

4 ANNONCE PUBLIQUE

LES CANADIENS SONT INFORMÉS DE :

Ce que l'on sait au sujet de l'incident

Toutes mesures nécessaires à prendre pour se protéger



Government of Canada / Gouvernement du Canada

GROUPE DE TRAVAIL SUR LES MENACES EN MATIÈRE DE SÉCURITÉ ET DE RENSEIGNEMENT VISANT LES ÉLECTIONS

NON CLASSIFIÉ/RÉSERVÉ À UN USAGE OFFICIEL

Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections– Rôles des partenaires

Préparation aux élections de 2019

GROUPE DE TRAVAIL SUR LES MENACES EN MATIÈRE DE SÉCURITÉ ET DE RENSEIGNEMENTS VISANT LES ÉLECTIONS

DE QUOI PARLONS-NOUS?

Il s'agit d'activités secrètes, clandestines ou criminelles qui entravent ou influencent les processus électoraux du Canada.

	MANDAT/RÔLE	ACTIVITÉS
CST Centre de la sécurité des télécommunications	**Sécurité de la technologie de l'information** • Fournir des conseils, de l'orientation et des services pour aider à assurer la protection de l'information électronique et des systèmes importants. **Renseignements étrangers** • Recueillir des renseignements étrangers destinés au gouvernement du Canada sur les auteurs de menaces. **Soutien au Service canadien du renseignement de sécurité (SCRS) et à la Gendarmerie royale du Canada (GRC)** • Fournir de l'assistance pour les opérations techniques.	• Fournir des renseignements et des cyber-évaluations sur les intentions, activités et capacités des auteurs étrangers de menaces. • Protéger les systèmes et les réseaux du gouvernement liés aux élections à l'aide de mesures de cyber-défense. • Fournir des conseils et une orientation en matière de cybersécurité aux partis politiques, aux provinces et aux autres institutions qui contribuent aux processus démocratiques.
SCRS Service canadien du renseignement de sécurité	**Renseignements et réduction des menaces** • Recueillir des renseignements sur les activités influencées par l'étranger qui nuisent aux intérêts du Canada, sont clandestines ou trompeuses, ou représentent une menace pour quiconque. • Contrecarrer de telles activités par des mesures de réduction des menaces. **Évaluation des renseignements** • Fournir des conseils, des rapports de renseignement et des évaluations de renseignements au gouvernement du Canada sur les activités influencées par l'étranger.	• Fournir des comptes rendus de menaces et des rapports de renseignement à Élections Canada et au commissaire aux élections fédérales. • Fournir aux décideurs du gouvernement du Canada une évaluation des méthodes utilisées et des capacités pour mener des activités hostiles à l'État.
AMC Affaires mondiales Canada	**Mécanisme de réponse rapide du G7** • Effectuer des recherches en libre accès sur les tendances et les données mondiales concernant les menaces pour la démocratie. • Établir des partenariats avec les pays du G7 afin d'échanger des renseignements et de coordonner les réponses aux menaces, au besoin.	• Effectuer des recherches sur les campagnes de désinformation ciblant le Canada et menées par des acteurs étrangers. • Rendre compte des tendances, des mesures et des incidents mondiaux. • Coordonner l'attribution des incidents.
GRC Gendarmerie royale du Canada	**Sécurité nationale** • Principale organisation chargée de prévenir, de détecter et de repousser les menaces criminelles liées à la sécurité nationale au Canada et d'y répondre. • Enquêter sur les actes criminels liés au terrorisme, à l'espionnage, aux cyberattaques et aux activités influencées par l'étranger. • Constituer, pour Élections Canada, le principal organe d'enquête si une activité criminelle est suspectée.	• Enquêter sur toute activité criminelle visant à entraver ou à influencer les processus électoraux du Canada. • Travailler en étroite collaboration avec les organismes de renseignement, d'application de la loi et de réglementation.

Gouvernement du Canada / Government of Canada

Canada

Document d'information
Initiative de citoyenneté numérique et Programme de contributions en matière de citoyenneté numérique

L'Initiative de citoyenneté numérique (ICN) est une stratégie à volets multiples visant à appuyer la démocratie et l'inclusion sociale au Canada en renforçant la résilience des citoyennes et des citoyens à l'égard de la désinformation en ligne et en établissant des partenariats pour soutenir un écosystème d'information sain. Elle a été lancée en 2019 dans le cadre du Plan pour protéger la démocratie canadienne du gouvernement du Canada basé sur quatre piliers.

L'ICN soutient une communauté de chercheurs canadiens par l'entremise de son Programme de contributions en matière de citoyenneté numérique (PCCN) qui fournit une aide financière pour la recherche et les activités axées sur les citoyennes et les citoyens. Les projets financés visent à soutenir la démocratie et l'inclusion sociale au Canada en améliorant ou en soutenant les efforts pour contrer la désinformation et d'autres préjudices et menaces en ligne.

Depuis janvier 2020, le PCCN a fourni un financement de 15 millions de dollars à des organisations tierces qui entreprennent des activités de recherche et d'apprentissage, comme des outils de sensibilisation du public et des ateliers en ligne, afin d'aider les Canadiennes et les Canadiens à renforcer leur résilience et à faire preuve d'esprit critique face aux informations qu'ils rencontrent en ligne. Ces projets ont touché plus de 12 millions de Canadiennes et Canadiens en ligne et hors ligne, dans les communautés minoritaires ainsi que dans les communautés autochtones, et ce, dans les deux langues officielles.

Exemples d'appels passés et actuels

En 2020, le PCCN a consacré environ 4,3 millions de dollars spécifiquement aux organisations aidant les citoyens à accroître leur résilience et à faire preuve d'esprit critique à l'égard des informations sur la santé qu'ils trouvent en ligne, à identifier la mésinformation et la désinformation, et à limiter les répercussions du contenu en ligne raciste ou trompeur relatif à la pandémie de COVID-19.

En mars 2022, le PCCN a lancé un appel d'offres spécial ciblé pour financer des initiatives qui aident les gens à cerner la mésinformation et la désinformation en ligne liées à la guerre en Ukraine et à d'autres menaces nationales pour la cohésion sociale. En conséquence, 11 projets ont reçu un financement total de plus de 2,4 millions de dollars pour des activités allant d'ateliers éducatifs à des baladodiffusions documentaires, en passant par de nouvelles ressources éducatives et des efforts pour contrer la désinformation russe.

Le dernier appel ouvert du PCCN a été clôturé en août 2022 et a fourni plus de 1,2 million de dollars pour financer 16 projets de recherche visant à évaluer l'efficacité des plateformes en ligne dans la lutte contre la désinformation et d'autres préjudices en ligne, à comprendre le rôle que jouent les autres sources médiatiques non informatives dans la sphère de la désinformation et à déterminer les fondements comportementaux et psychologiques de la diffusion de la désinformation et des contenus préjudiciables.

Contrer une menace en évolution :

mise à jour sur les recommandations visant à prévenir l'ingérence étrangère dans les institutions démocratiques canadiennes

Canada

Table des matières

Introduction

Le 6 mars 2023, le gouvernement du Canada a annoncé plusieurs mesures de lutte contre l'ingérence étrangère dans les processus démocratiques canadiens. Ces mesures comprenaient une demande d'élaboration d'un plan pour donner suite aux recommandations en suspens du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) de 2018 et 2019[1], du rapport Judd[2] et du rapport Rosenberg[3]. Le plan, exposé ci-après, énonce ces recommandations, résume les mesures prises jusqu'à maintenant afin d'en assurer le suivi et propose d'autres mesures.

Entre 2018 et 2023, 26 recommandations ont été formulées, dont 16 reçues au début de 2023 dans le cadre du rapport Rosenberg. Comme les recommandations de chacun des rapports portent sur des enjeux similaires, elles ont été regroupées sous les thèmes suivants :

- Communiquer avec la population canadienne à propos de l'ingérence étrangère et la protection de la démocratie canadienne;
- Gouvernance efficace et cadres juridiques solides;
- Risques, vulnérabilités, et mesures de sécurité;
- Dialogue avec les partenaires afin d'augmenter la sensibilisation et de renforcer la résilience face à l'ingérence étrangère

À **l'annexe A** se trouve un tableau indiquant le statut de chaque recommandation.

Le présent plan énonce les recommandations formulées dans le cadre des rapports afin de protéger les institutions et les processus démocratiques canadiens, récapitule les mesures prises, ou en cours, pour mettre en œuvre les recommandations et propose d'autres démarches à étudier afin de renforcer la réponse canadienne aux menaces d'ingérence étrangère. Des travaux supplémentaires seront nécessaires afin de concrétiser ces démarches supplémentaires, y compris une approche stratégique, la tenue de consultations, l'éventuelle présentation de projets de loi pour examen par les parlementaires, et la mise en œuvre.

---

[1] Le rapport annuel de 2019 du CPSNR (CPSNR, 2019), et le rapport spécial de 2018 du CPSNR sur les allégations entourant la visite officielle du premier ministre Trudeau en Inde en février 2018 (CPSNR, 2018). Les autres rapports publiés par le CPSNR et l'Office de surveillance des activités en matière de sécurité nationale et de renseignement n'ont pas été examinés, car ils ne contenaient pas de recommandations relatives à l'ingérence étrangère.

[2] Le rapport sur la Directive sur le Protocole public en cas d'incident électoral majeur de 2019 (rapport Judd)

[3] Le rapport sur la Directive sur le Protocole public en cas d'incident électoral majeur de 2021 (rapport Rosenberg)

Recommandations des quatre rapports examinés – Statut de la mise en œuvre, lacunes potentielles et prochaines étapes

Beaucoup de travail a été accompli pour mettre en œuvre bon nombre des recommandations des rapports, et le gouvernement continue de travailler à la mise en œuvre d'autres recommandations.

Les cinq recommandations formulées dans les deux rapports du CPSNR (2018 et 2019) ont été partiellement mises en œuvre. Certaines mesures ont été prises en regard de chaque recommandation, et des options supplémentaires pour étude ont été cernées.

Quatre des cinq recommandations du rapport Judd ont été mises en œuvre en tout ou en partie. Une des recommandations (nº 2) propose d'étendre la période d'application du Protocole public en cas d'incident électoral majeur aux périodes où aucune élection n'a lieu. Cela n'a pas été mis en œuvre, car les ministres possèdent déjà la responsabilité et les pouvoirs nécessaires pour gérer toute préoccupation relative à l'ingérence étrangère se produisant entre les élections. La responsabilité ministérielle est un principe fondamental de la démocratie parlementaire canadienne.

Le rapport Rosenberg, reçu en février 2023, faisait état de 16 recommandations qui sont présentement étudiées afin d'être mises en œuvre rapidement.

Communiquer avec la population canadienne à propos de l'ingérence étrangère et la protection de la démocratie canadienne	CPSNR 2019 (nº 1) Judd (nºs 1, 5) Rosenberg (nºs 1, 4-5, 10-11, 15, 16)

Les quatre rapports font valoir que le fait de doter les citoyennes et les citoyens de connaissances constitue la meilleure défense contre ceux qui tentent de s'immiscer dans les processus démocratiques canadiens. Dans son rapport de 2019, le CPSNR indique que, en ce qui a trait à l'ingérence étrangère, « l'amélioration de la sensibilisation du public sur les menaces qui pèsent sur le Canada » est essentielle. M. Rosenberg souligne, dans son récent rapport, l'importance « d'une formulation claire du problème et de l'approche adoptée pour le résoudre ».

Situation actuelle

Le gouvernement du Canada a pris des mesures en vue d'accroître la sensibilisation du public sur l'ingérence étrangère et de favoriser l'adoption d'une approche pansociétale afin de contrer cette menace. Depuis 2018, le Service canadien du renseignement de sécurité (SCRS) souligne l'existence de la menace d'ingérence étrangère dans son rapport annuel. Avant les élections

fédérales de 2021, le SCRS a publié un rapport public portant sur l'ingérence étrangère et les menaces visant les processus démocratiques du Canada. Le Centre de la sécurité des télécommunications (CST) a aussi commencé en 2017 à publier des rapports sur les cybermenaces étrangères dans le contexte des élections. Le gouvernement du Canada a aussi mené des activités de sensibilisation afin de mobiliser les Canadiennes et les Canadiens et les communautés, notamment en vue de mobiliser les partenaires du SCRS (industrie, universités, communautés canadiennes, société civile), du CST et du Centre canadien pour la cybersécurité (industrie, petites entreprises, infrastructures essentielles privées), et de la Gendarmerie royale du Canada (GRC) grâce à des activités de sensibilisation communautaire.

À l'approche des élections fédérales de 2019, le Canada a mis en œuvre le Plan pour protéger la démocratie canadienne. Le Plan a été le premier du genre à l'échelle internationale et reconnaissait, par le biais de la création de l'Initiative de citoyenneté numérique, l'importance d'avoir des citoyennes et des citoyens éclairés afin de résister à l'ingérence étrangère. Cette initiative appuie la démocratie et l'inclusion sociale au Canada en renforçant la résilience contre la désinformation en ligne et en établissant des partenariats à l'appui d'un écosystème de l'information sain. Le Plan reconnaissait aussi l'importance de la collaboration avec les alliés et les partenaires aux vues similaires afin d'intensifier le rôle de leadership du Canada dans le cadre du Mécanisme de réponse rapide du G7, qui a été lancé lors de la réunion du G7 accueillie par le Canada en 2018. Ce mécanisme aide le G7 et d'autres pays alliés à collaborer en mettant en commun l'information relative à l'ingérence étrangère sur les médias sociaux. Depuis 2018, le gouvernement du Canada a investi près de 20 millions de dollars dans le Mécanisme de réponse rapide du G7, dont 13,4 millions de dollars sur cinq ans en mai 2022, afin d'approfondir la coordination entre les pays pour cerner les menaces étrangères à la démocratie, notamment la désinformation instiguée par des États, et réagir à ces menaces.

Le Plan pour protéger la démocratie canadienne indiquait aussi que les institutions gouvernementales doivent continuer à travailler de concert afin de se préparer aux menaces d'ingérence étrangère et de les contrer. La Directive du Cabinet sur le Protocole public en cas d'incident électoral majeur (le Protocole) contribue à ces efforts. Le Protocole est administré par un groupe non partisan de hauts fonctionnaires (le Groupe d'experts) chargés d'informer la population canadienne des incidents se produisant lors de la période électorale qui menacent l'intégrité de l'élection fédérale.

Les délibérations du Groupe d'experts sont éclairées par un autre outil innovant, le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, formé de représentants de la GRC du CST, du SCRS et d'Affaires mondiales Canada afin de rendre compte des activités secrètes, clandestines ou criminelles d'acteurs étrangers.

Le Plan a reconnu que les défis posés par l'ingérence et la désinformation menées par les États étrangers sont complexes et interreliés – la désinformation étant une tactique utilisée par les États étrangers. À ce titre, le Plan décrit une approche pansociétale pour s'attaquer à ces problèmes. Le gouvernement du Canada s'emploie à mieux outiller les milieux universitaires, la société civile, et les provinces et les territoires des ressources nécessaires pour améliorer la

sensibilisation à ces menaces. La collaboration avec ces partenaires est essentielle pour que le Canada continue de s'adapter à des défis en constante évolution.

L'approche du gouvernement continue d'évoluer. Depuis les élections fédérales de 2019, le Plan pour protéger la démocratie canadienne a été révisé et amélioré en mettant l'accent sur quatre domaines stratégiques d'amélioration :

- Renforcer une perception des menaces tout au long du cycle électoral;
- Élargir le point de vue du gouvernement sur la sensibilisation aux menaces;
- Développer un leadership central en matière de désinformation;
- Assurer le renforcement continu de la résilience des institutions et des citoyennes et des citoyens.

Le Plan pour protéger la démocratie canadienne a été amélioré par le biais de la mise en œuvre des recommandations de M. Judd pour le Protocole public en cas d'incident électoral majeur. Ces changements comprenaient :

- l'harmonisation de la période d'application du Protocole avec celle de la convention de transition;
- une disposition explicite permettant au Groupe d'experts de consulter le directeur général des élections selon les besoins;
- une disposition permettant aux partis politiques d'aviser les organismes de sécurité des incidents pouvant menacer la tenue d'élections libres et justes;
- la reconnaissance de la capacité du Groupe d'experts d'examiner les cas d'ingérence provenant de l'intérieur ainsi que de recevoir de l'information de sources autres que les organismes de sécurité.

La Déclaration du Canada sur l'intégrité électorale en ligne a été renforcée en recrutant des signataires s'ajoutant aux quatre premiers (Facebook, Google, Microsoft et Twitter). En 2021, TikTok, LinkedIn et YouTube ont appuyé la Déclaration. Créée en 2019, la Déclaration est une entente volontaire avec les plateformes des médias sociaux en vue d'améliorer la transparence, l'authenticité et l'intégrité de leurs systèmes pour contribuer à la protection des élections fédérales du Canada. La Déclaration reconnaît que les médias sociaux et les autres plateformes en ligne, ainsi que le gouvernement du Canada, assument des responsabilités respectives afin de contribuer à protéger les processus électoraux canadiens. Cela répondait directement à la recommandation nº 5 de M. Judd et a contribué à réduire la désinformation.

Le Plan pour protéger la démocratie canadienne renouvelé reconnaissait aussi l'importance de la collaboration entre les ministères et les organismes afin de relever les défis émergents. Il a aussi renforcé la collaboration interministérielle visant à contrer la désinformation. Tirant avantage des connaissances acquises dans le cadre du modèle RESIST du Royaume-Uni, ces travaux se fondent sur la nécessité de repérer la désinformation et de comprendre son fonctionnement. Bien qu'ils en soient encore à leurs débuts, ces efforts visent aussi à améliorer la disponibilité de l'information fiable sur les programmes et services gouvernementaux, à

mettre en œuvre une trousse d'outils contre la désinformation et à offrir une formation sur l'ingérence étrangère et la désinformation aux parlementaires et aux fonctionnaires.

Plus récemment, le gouvernement du Canada a créé l'Unité de protection de la démocratie au sein du Bureau du Conseil privé et lui a donné le mandat de coordonner, de concevoir et de mettre en œuvre des mesures pangouvernementales visant à lutter contre la désinformation et à protéger les institutions démocratiques canadiennes. Conjointement, ces efforts contribuent à l'objectif ultime d'une des recommandations du rapport du CPSNR de 2019, celui de « renforcer la résilience des institutions et de la population » grâce à « une direction et une coordination centrales durables ».

Lacunes potentielles et prochaines étapes

Éclairé par les examens antérieurs et par les faits recueillis dans le cadre des élections fédérales de 2019 et de 2021, pendant lesquelles les mesures susmentionnées étaient en vigueur, M. Rosenberg constate que « le plan et les communications publiques du gouvernement doivent reconnaître que le problème d'ingérence se pose aussi bien avant le déclenchement de l'élection que pendant la période d'application de la convention de transition ». Le problème d'ingérence ne se cantonne pas qu'à la période électorale, mais est plutôt permanent.

M. Rosenberg constate également que le gouvernement devrait préciser que « le Protocole n'est qu'un élément d'un ensemble beaucoup plus vaste de mesures visant à lutter contre l'ingérence dans les élections ». M. Rosenberg recommande « une approche de communication rapide et complète » qui explique « l'ensemble des activités qui se déroulent pendant la période d'application de la convention de transition ». Ces constatations sont très similaires aux constatations antérieures du CPSNR, qui recommande au gouvernement « de communiquer de façon plus approfondie avec les institutions canadiennes relativement aux importantes menaces [reliées à l'ingérence étrangère] qui planent sur elles ». Cependant, il peut être difficile de parler ouvertement de l'ingérence étrangère, compte tenu du risque de révéler des renseignements ainsi que de la nécessité de protéger les sources et de maintenir des relations essentielles avec les partenaires du renseignement du Canada. Le CPSNR a reconnu ce fait dans son rapport de 2019 lorsqu'il a souligné les « défis liés à la communication d'informations » associés à l'ingérence étrangère « en raison de leur nature délicate ».

Néanmoins, une constatation fondamentale des quatre rapports étudiés est reliée à la nécessité de faire preuve de davantage de transparence avec la population canadienne à propos de la portée et de la nature de l'ingérence étrangère dans les processus démocratiques. Il reste du travail à effectuer afin d'assurer une sensibilisation à plus grande échelle concernant les menaces auxquelles le Canada est confronté et les mesures visant à les contrer. Au vu des recommandations de M. Rosenberg de communiquer plus à fond et plus fréquemment avec les Canadiennes et les Canadiens à propos de l'ingérence étrangère et des efforts du Canada pour protéger la démocratie canadienne, le gouvernement, y compris les ministres responsables et les représentants de la sécurité nationale et du renseignement, trouveront davantage d'occasions de tenir les Canadiennes et les Canadiens au courant de l'ampleur de l'ingérence

étrangère qui touche tous les aspects de la société, y compris la démocratie. Une population mobilisée, informée et résiliente est l'une des meilleures défenses contre les tentatives visant à miner la démocratie et ses institutions. Veiller à ce que la population canadienne soit informée des activités entreprises en leur nom et adopter les meilleures pratiques émergentes en matière de communication inspirées des récents efforts du Canada et de l'OTAN pour cerner et contrer la désinformation instiguée par la Russie dans le cadre de l'invasion de l'Ukraine permettront de rassurer la population canadienne quant à la solidité et la sécurité de leur démocratie.

Précisément, le gouvernement prendra avantage du nouveau Bureau national de lutte contre l'ingérence étrangère et du prochain rapport annuel du SCRS pour améliorer la communication avec la population canadienne.

En plus, de nouvelles réunions d'information seront offertes aux députés et aux sénateurs afin d'accroître leur résilience à la menace que constitue l'ingérence étrangère. Le nouveau Bureau national de lutte contre l'ingérence étrangère travaillera à accroître les mécanismes de partage d'information avec les représentants provinciaux, territoriaux, municipaux et autochtones.

Le financement récemment annoncé en vue de renforcer la capacité des partenaires de la société à contrer la désinformation, y compris celle provenant de sources étrangères, aidera également à accroître la résilience. Le gouvernement accélère présentement ses efforts en vue de renforcer la capacité du gouvernement du Canada et de partenaires à combattre la désinformation, y compris la désinformation parrainée par des États, par le biais de communications stratégiques inspirées du modèle RESIST.

Ces mesures sont conformes aux engagements énoncés dans la lettre de mandat du ministre LeBlanc, qui lui confie le mandat de « diriger une réponse gouvernementale intégrée pour protéger les institutions démocratiques du Canada, dont le processus électoral fédéral, de l'ingérence étrangère et de la désinformation ». Ces travaux devront être réalisés en étroite collaboration avec d'autres intervenants, notamment le ministre de la Sécurité publique, lequel assume la responsabilité générale de mener les efforts pangouvernementaux visant à combattre l'ingérence étrangère. Les efforts seront également orientés par des partenaires clés comme le directeur général des élections, dont les rapports de recommandations postélectorales fournissent des renseignements importants sur l'évolution du système électoral du Canada.

À partir des conclusions et des recommandations de l'examen de l'ingérence étrangère par le rapporteur spécial indépendant, ainsi que des examens en cours du CPSNR et de l' Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), le gouvernement prendra des mesures supplémentaires.

9 Contrer une menace en évolution

Gouvernance efficace et cadres juridiques solides	CPSNR, 2019 (nº 1c-d) CPSNR, 2018 (nº 2) Rosenberg (nº 8)

Les rapports étudiés ont mis en lumière l'importance de disposer, afin de contrer l'ingérence étrangère, d'un cadre juridique et de gouvernance moderne et robuste trouvant un équilibre entre les facteurs relatifs à la sûreté nationale et ceux liés à la protection de la vie privée et aux autres protections assurées par la *Charte canadienne des droits de la personne*.

Situation actuelle

En 2017, le Parlement a créé le CPSNR, qui offre une tribune aux députés de tous les partis politiques reconnus et aux sénateurs ayant une cote de sécurité de niveau très secret pour examiner les renseignements classifiés. Conformément à la recommandation nº 1d) de 2019 du CPSNR, qui propose d'élaborer des mécanismes pangouvernementaux afin de déceler l'ingérence étrangère et d'y répondre, le gouvernement a récemment pris plusieurs mesures afin de réagir à l'ingérence étrangère au moyen de mécanismes stratégiques et opérationnels. En premier lieu, le premier ministre a annoncé la création du Bureau national de lutte contre l'ingérence étrangère au sein de Sécurité publique Canada, une nouvelle fonction dont la raison d'être est expressément la coordination des efforts de lutte contre l'ingérence étrangère. Le budget de 2023 a annoncé un investissement de 13,5 millions de dollars sur cinq ans et de 3,1 millions de dollars par année pour le Bureau et ses activités. En second lieu, le gouvernement a lancé des consultations publiques à propos de la mise en œuvre d'un registre visant la transparence en matière d'influence étrangère afin d'enrichir la trousse d'outils du Canada face à cette menace en évolution. Ces consultations doivent se terminer au printemps de 2023.

En outre, le rapport spécial de 2018 du CPSNR a souligné le rôle clé joué par le conseiller à la sécurité nationale et au renseignement (CSNR) auprès du premier ministre qui consiste à fournir des conseils en qualité de coordonnateur de la collectivité de la sécurité et du renseignement et de conseiller du premier ministre. Depuis, des mesures ont été prises afin de renforcer davantage le cadre de gouvernance de la sécurité nationale et de veiller à ce que le CSNR soit bien au fait des menaces et des mesures d'atténuation en cours, y compris celles liées à l'ingérence étrangère.

Le rapport de 2019 du CPSNR a recommandé (nº 1c) que le gouvernement évalue les lois en vigueur relatives à l'ingérence étrangère comme la *Loi sur la protection de l'information* et la *Loi sur le Service canadien du renseignement de sécurité* et apporte des changements législatifs au besoin. Les ministères et les organismes ont procédé à une analyse stratégique et juridique exhaustive de ces lois, ont repéré les lacunes et continuent de concevoir des options pour y remédier en vue de renforcer le cadre juridique canadien.

La *Loi sur la modernisation des élections*, que le Parlement a adoptée en 2018, interdit l'utilisation de fonds provenant d'entités étrangères et comprend des mesures de transparence accrues. Le gouvernement a également présenté d'autres mesures législatives, notamment le projet de loi C-26, *Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*, afin de renforcer la cybersécurité.

En 2019, le gouvernement a créé l'OSSNR, qui est chargé d'effectuer un examen indépendant des activités liées à la sécurité nationale et au renseignement dans tous les ministères et organismes fédéraux et d'informer le Parlement et la population canadienne de la légalité de ces activités.

De plus, le budget de 2023 prévoit 53 millions de dollars sur deux ans pour aider les ministères et les organismes qui ont des mandats de sécurité nationale et de renseignement à s'acquitter de leur obligation de se conformer aux exigences législatives en matière d'examen de façon rapide et efficace, ainsi qu'à mettre en œuvre les recommandations.

Lacunes potentielles et prochaines étapes

Dans le but de moderniser la trousse à outils juridique du Canada pour contrer les menaces d'ingérence étrangère et de mettre intégralement en œuvre la recommandation du CPSNR sur le renforcement du cadre juridique, le ministre de la Sécurité publique, s'appuyant sur les travaux en cours du rapporteur spécial indépendant et sur les examens du CPSNR et de l'OSSNR, prendra les mesures suivantes :

- Travailler à la modernisation de la *Loi sur le SCRS*, qui a été rédigée avant qu'Internet ne soit largement accessible. Des changements pourraient être apportés pour permettre au SCRS de mieux fonctionner à l'ère numérique en recueillant et en utilisant les données numériques de façon efficace, de partager des renseignements avec des partenaires non gouvernementaux en vue de les aider à neutraliser les menaces, et de recueillir des renseignements et de mener des activités de lutte contre les menaces étrangères qui n'avaient pas été envisagées lorsque la *Loi sur le SCRS* a reçu la sanction royale en 1984. Ce travail devrait également s'appuyer sur les recommandations du rapport final de la Commission sur l'état d'urgence qui ont trait à la *Loi sur le SCRS*. Puisqu'il est nécessaire que les Canadiennes et les Canadiens, en particulier les membres des communautés de la diaspora, aient confiance que les organismes de sécurité nationale travaillent à protéger leurs intérêts et à respecter leurs droits garantis par la *Charte*, un dialogue et une consultation solides sur toute proposition seront nécessaires;
- Examiner, en collaboration avec les partenaires du domaine de l'application de la loi et les organismes de sécurité nationale, si d'autres modifications aux dispositions existantes sont nécessaires et s'il faut créer de nouvelles infractions en vertu de la *Loi sur la protection de l'information* et du *Code criminel* pour faciliter les poursuites relatives aux activités d'ingérence étrangère.

11 Contrer une menace en évolution

En mentionnant la *Loi sur la modernisation des élections* de 2018, M. Rosenberg remarque que « les lois électorales canadiennes ont été modifiées pour contrer plus efficacement l'ingérence étrangère ». Le ministre des Affaires intergouvernementales, de l'Infrastructure et des Collectivités s'emploie actuellement à modifier la *Loi électorale du Canada*. Dans le cadre de ce processus, il examinera les modifications possibles pour contrer également l'ingérence étrangère.

Risques, vulnérabilités et mesures de sécurité	CPSNR, 2019 (nº 1a-b) Rosenberg (nºs 2-3)

Les rapports examinés ont formulé plusieurs recommandations liées à la nécessité pour le gouvernement d'avoir la capacité d'évaluer les risques et les vulnérabilités découlant de la menace croissante posée par l'ingérence étrangère en vue de pouvoir adapter la trousse d'outils du gouvernement face à l'évolution de la menace.

Situation actuelle

Le rapport de 2019 du CPSNR a mis en lumière le besoin de définir les risques et les préjudices pour les institutions découlant des menaces d'ingérence étrangère (nº 1a) ainsi que l'exigence de mener un examen complet des vulnérabilités subséquentes (nº 1b). En guise de suivi, les ministères et les organismes ont préparé des évaluations des menaces et des risques posés par l'ingérence étrangère et conçu des mesures visant à contrer ces menaces. Les dirigeants principaux de la sécurité (DPS) et les dirigeants principaux de l'information (DPI) ministériels, sous la direction du Bureau du Conseil privé, ont suivi une formation afin de mieux informer la communauté des DPS et des DPI des menaces et des stratégies d'atténuation possibles (p. ex., des protections techniques et des conseils en matière de cyberhygiène). En outre, dans le cadre des évaluations des menaces et des risques, les ministères et les organismes ont ouvert un dialogue avec les intervenants de secteurs d'intérêt stratégique, comme les exploitants d'infrastructures essentielles, afin qu'ils contribuent à cerner les risques et à éliminer les vulnérabilités associées à leurs secteurs opérationnels particuliers.

Afin de contrer les efforts des États étrangers en vue de s'ingérer dans la démocratie canadienne en intimidant les communautés de la diaspora au Canada, le budget de 2023 prévoit de verser 48,9 millions de dollars sur trois ans à la GRC pour protéger les Canadiennes et les Canadiens contre le harcèlement et l'intimidation, augmenter sa capacité d'enquête, et s'engager de manière plus proactive auprès des communautés qui sont plus à risque d'être ciblées.

Lacunes potentielles et prochaines étapes

L'ingérence étrangère peut être subtile et ses incidences éventuelles difficiles à cerner, à quantifier et à exposer. Les ministères et les organismes poursuivent donc le dialogue avec les intervenants

du milieu universitaire et au moyen d'autres programmes de sensibilisation afin d'évaluer les incidences à court, à moyen et à long terme de l'ingérence étrangère au Canada, tout en continuant à mettre à jour les évaluations au fur et à mesure de l'évolution de la menace.

M. Rosenberg a recommandé (recommandation nº 2) que « les préparatifs de la prochaine élection devraient comprendre une évaluation de l'adéquation des capacités de la sécurité ministérielle, de la police de protection de la [GRC] et des services de police locaux par rapport au niveau et à la persistance des menaces, et de l'efficacité de la coordination entre ces organes. Il faudrait également revoir la coordination entre les partis politiques et le gouvernement en ce qui concerne les campagnes et les opérations de sécurité. » Le ministre de la Sécurité publique et le ministre des Affaires intergouvernementales, de l'Infrastructure et des Collectivités ont entrepris une analyse exhaustive des menaces reliées à la sécurité, y compris les menaces d'ingérence étrangère, et des mesures de protection disponibles pour les ministres, les autres parlementaires et les hauts fonctionnaires. Les ministres évaluent les outils pour qu'ils soient adaptés à l'environnement de menaces et qu'ils atténuent les risques et les vulnérabilités.

M. Rosenberg a aussi recommandé (nº 3) « d'évaluer si des ajustements doivent être apportés au rôle des membres du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections à la lumière du problème croissant de l'ingérence nationale ». Cela sera examiné dans le cadre d'autres améliorations au Plan pour protéger la démocratie canadienne en tirant parti de l'orientation énoncée dans la lettre de mandat du ministre LeBlanc et comprendra un examen de la possibilité de rendre permanent le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, avec le mandat de produire des rapports réguliers sur les activités d'ingérence étrangère.

Mobilisation en vue d'améliorer la sensibilisation et d'augmenter la résilience face à l'ingérence étrangère	CPSNR, 2019 (nos 1e, 1f, 1g, 2) CPSNR, 2018 (nos 1 (A et B)) Judd (nos 3-4) Rosenberg (nos 6-7, 12-14)

L'ingérence étrangère est une menace à la fois mondiale et locale. Elle touche les individus, les organisations, les entreprises ainsi que les processus démocratiques de tous niveaux. Aucune entité ou aucun ordre de gouvernement agissant isolément ne peut la contrer avec efficacité. Elle évolue rapidement, ce qui fait de la mise en commun de l'information un des outils les plus efficaces pour connaître les risques. Le gouvernement du Canada doit collaborer avec ses partenaires tant au sein du pays qu'à l'étranger afin de veiller à mettre en place les meilleures défenses disponibles. Chacun des quatre rapports a formulé des recommandations indiquant la nécessité d'une approche pansociétale pour contrer l'ingérence étrangère. Cela comprend des recommandations visant à améliorer le dialogue tant sur le plan intérieur que sur le plan international ainsi qu'à s'assurer que les partenaires et les intervenants sont informés et à même de contribuer aux efforts collectifs.

Situation actuelle

En réponse aux recommandations formulées par le CPSNR en 2018 et 2019, le gouvernement a déployé plusieurs efforts. Le premier ministre a annoncé la création du Bureau national de lutte contre l'ingérence étrangère au sein de Sécurité publique Canada, ce qui donne directement suite à la recommandation n° 2 de 2019 du CPSNR. Le gouvernement a aussi enregistré des progrès dans la mise en œuvre de deux autres recommandations de 2019 du CPSNR. Par exemple, les organismes responsables de la sécurité et du renseignement, notamment la GRC, le SCRS, Sécurité publique Canada, et le Centre canadien pour la cybersécurité, ont intensifié le dialogue avec les représentants provinciaux, territoriaux et municipaux, les leaders et communautés autochtones ainsi que les propriétaires et exploitants d'infrastructures essentielles afin d'améliorer la sensibilisation aux menaces et d'accroître la résilience (recommandation n° 1e). La GRC travaille également avec les forces de police locale compétentes afin de contrer l'ingérence étrangère, y compris afin de contrer le harcèlement et l'intimidation soutenus par les États, puisque les forces de police locale compétentes sont souvent les premières à prendre connaissance des activités d'ingérence étrangère. De plus, les organismes de sécurité et de renseignement et d'autres poursuivent un dialogue régulier avec les partenaires internationaux sur les efforts collaboratifs pour contrer l'ingérence étrangère, notamment par le partage de renseignement. Le ministre de la Sécurité publique coopère également avec les alliés du Canada en tant que représentant du Canada à la réunion ministérielle des cinq pays, où les ministres de la Sécurité du Groupe des cinq se réunissent pour collaborer sur diverses questions de sécurité nationale, notamment l'ingérence étrangère, discuter de leurs approches respectives concernant des enjeux communs et coordonner une réponse cohérente du Groupe des cinq (recommandation n° 1g).

Dans son rapport spécial de 2018, le CPSNR a recommandé (n° 1) que, « dans l'intérêt de la sûreté nationale, il faudrait informer les députés de la Chambre des communes et les sénateurs des risques que représentent l'ingérence étrangère et l'extrémisme au Canada au moment de leur assermentation, et un suivi en ce sens devrait être effectué régulièrement par la suite ». Il recommandait aussi de « rappeler aux ministres du Cabinet les attentes énoncées dans le document du gouvernement *Pour un gouvernement ouvert et responsable* ... [et que]... conformément à la *Loi sur les conflits d'intérêts*, les titulaires d'une charge publique doivent toujours accorder la priorité à l'intérêt public avant leurs intérêts personnels ». Des mesures ont été prises afin de donner suite à cette recommandation. En premier lieu, les obligations des ministres et les attentes à l'égard de leurs actions ont été rendues publiques dans le cadre de leurs lettres de mandat respectives. En second lieu, le Service de protection parlementaire offre aux nouveaux parlementaires des séances d'information sur la sécurité qui couvrent diverses menaces, y compris l'ingérence étrangère. En outre, le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections a offert des séances d'information aux représentants des partis politiques pendant la période électorale alors que le Bureau du Conseil privé informe tous les nouveaux ministres et secrétaires parlementaires, au moment de leur nomination, de l'éventail des menaces à la sécurité, y compris l'ingérence étrangère.

14 Contrer une menace en évolution

M. Judd a recommandé que le Canada « surveille les développements internationaux en portant une attention particulière à toute évolution des tactiques des acteurs malveillants et des contre-mesures défensives prises par les pays cibles (mesures juridiques, réglementaires et opérationnelles) ». Le gouvernement a poursuivi la collaboration internationale dans divers forums, y compris par l'entremise du Mécanisme de réponse rapide, en réunissant les pays du G7 pour cerner les menaces étrangères et y répondre. L'Appel de Paris pour la confiance et la sécurité dans le cyberespace (Appel de Paris), qui a été lancé en novembre 2018, invite les États, le secteur privé et les organisations de la société civile à travailler ensemble pour renforcer la sécurité dans le cyberespace, lutter contre la désinformation et faire face aux nouvelles menaces qui se dessinent. Dans le cadre de l'Appel de Paris, le Canada et d'autres groupes mettent en commun l'information et les pratiques exemplaires relatives à plusieurs formes d'ingérence électorale étrangère. Des ateliers ont été organisés débouchant sur la publication du document L'approche multipartite : Recueil sur la défense des processus électoraux en 2021.

En réponse à la recommandation n° 4 de M. Judd, le gouvernement a offert des séances d'information aux partis politiques à l'approche de l'élection fédérale de 2021 et leur a fourni de l'information à propos des problèmes auxquels ils pourraient faire face pendant la campagne.

M. Rosenberg a souligné « la nécessité de collaborer avec des partenaires externes au Canada et dans le reste du monde, issus du milieu universitaire, de l'industrie et de la société civile, afin de soutenir l'intégrité de l'information pendant les élections. Ces partenaires externes jouent plusieurs rôles importants. Ils ont des points de vue sur l'évolution de l'environnement des menaces qui peuvent être différents de ceux des organismes de sécurité nationale. Ils ont un rôle de sensibilisation du public. Ils peuvent également alerter le public sur les tentatives d'ingérence avant et pendant la campagne ». À cette fin, le gouvernement du Canada s'est employé à doter les Canadiennes et les Canadiens, et en particulier les jeunes, des compétences nécessaires pour s'y retrouver dans l'information présentée en ligne. Depuis janvier 2020, l'Initiative de citoyenneté numérique a investi plus de 15 millions de dollars dans 96 projets menés par des organisations de la société civile et du milieu universitaire afin de renforcer la résilience citoyenne face à la désinformation. L'engagement du gouvernement à l'égard de l'Initiative de citoyenneté numérique s'est encore affermi à l'occasion de l'Énoncé économique de l'automne 2022 avec un investissement de 31 millions de dollars sur quatre ans, soit plus du double du financement annuel du programme.

Le 6 mars 2023, le gouvernement du Canada a annoncé un investissement de 5,5 millions de dollars pour renforcer la capacité des partenaires de la société civile à fournir des renseignements importants sur la dynamique de l'écosystème d'information du Canada, en renforçant la résilience et la littératie numérique du gouvernement, de l'industrie, de la société civile et des citoyennes et citoyens.

Lacunes potentielles et prochaines étapes

Le rapport de 2019 du CPSNR a recommandé (recommandation n° 1f) que la stratégie canadienne pour contrer l'ingérence étrangère et renforcer la résilience institutionnelle et publique « [comprenne] une approche à l'intention des ministres et des hauts dirigeants afin qu'ils nouent le dialogue avec les institutions fondamentales et la population ». Au moment où il examinera le Protocole à la suite de la publication du rapport de M. Rosenberg, le gouvernement envisagera l'instauration d'un processus par lequel les ministres et les hauts fonctionnaires, y compris les membres du Groupe d'experts dans le cadre du Protocole public en cas d'incident électoral majeur, communiqueront avec les intervenants et les communautés. Ce dialogue permettrait d'être à l'écoute des points de vue sur les pratiques exemplaires d'atténuation de l'incidence de l'ingérence étrangère et de la désinformation sur les institutions canadiennes.

Le gouvernement continuera également à travailler avec ses partenaires canadiens afin de poursuivre les travaux amorcés dans le cadre de l'Appel de Paris pour veiller à ce que tous aient accès à l'expertise la plus récente en vue de protéger l'intégrité des processus électoraux canadiens.

Dans son rapport, M. Rosenberg formulait aussi des recommandations en vue de tenir des séances d'information pour les représentants des partis politiques dans des lieux sécurisés à Ottawa (n° 12) et de fixer à l'avance les séances d'information au cours de la période électorale tout en prévoyant une certaine souplesse pour faire face aux situations d'urgence (n° 13). Ces recommandations seront mises en œuvre. Le rapport proposait aussi de prévoir à l'intention des parlementaires et de leur personnel un programme de séances d'information non classifiées sur l'ingérence étrangère et les mesures à prendre afin de s'en protéger (n° 14). Des séances d'information seront offertes aux parlementaires et à leur personnel à la suite de leur assermentation ainsi que sur une base régulière à l'avenir.

Conclusion et prochaines étapes

Le gouvernement du Canada a mis en œuvre au cours des dernières années un certain nombre de mesures pour contrer l'ingérence étrangère dans tous les aspects de la société, notamment dans les processus démocratiques. Ces mesures donnaient suite, en tout ou en partie, à plusieurs recommandations formulées par le CPSNR, M. Judd et M. Rosenberg. Le présent plan précise d'autres mesures visant à donner suite aux recommandations en suspens et à éliminer les lacunes qui pourraient subsister.

Ce travail comprend l'amélioration de la transparence et une communication plus efficace avec les Canadiennes et les Canadiens à propos de la menace d'ingérence étrangère et des mesures particulières prises par le gouvernement pour l'atténuer. Cela comprend l'examen des lois existantes, comme la *Loi sur le SCRS*, le *Code criminel*, la *Loi sur la protection de l'information* et la *Loi électorale du Canada*. Cela comprend également l'amélioration de la sécurité des hauts fonctionnaires et l'exploration d'améliorations possibles au Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections et à la Directive du Cabinet.

Toute démarche qui sera entreprise tiendra soigneusement compte des travaux continus du CPSNR, de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement et du rapporteur spécial indépendant, le très honorable David Johnston, afin de veiller à ce que les Canadiennes et les Canadiens continuent d'accorder leur confiance à leurs institutions démocratiques et à leurs processus électoraux.

Annexe A – Tableau des recommandations et des mesures connexes

	Recommandation	Mesures clés et prochaines étapes
Rapport annuel 2019 du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR)		
1	Le gouvernement du Canada élabore une stratégie exhaustive pour lutter contre l'ingérence étrangère et renforcer la résilience des institutions et de la population. Basée sur l'examen et les conclusions du Comité, la stratégie devrait :	Les ministères et organismes collaborent au sein d'un cadre de gouvernance efficace pour déceler et contrer les activités d'ingérence étrangère. Le nouveau Bureau national de lutte contre l'ingérence étrangère jouera un rôle de premier plan pour faire en sorte que les efforts pangouvernementaux pour lutter contre l'ingérence étrangère sont efficaces et sont orientés vers le même objectif. À partir des conclusions et des recommandations de l'examen de l'ingérence étrangère par le rapporteur spécial indépendant, ainsi que des examens en cours du CPSNR et de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), le gouvernement prendra des mesures supplémentaires.
	a) définir les risques et les préjudices à court et à long terme pour les institutions et les droits et libertés des Canadiens que fait peser la menace de l'ingérence étrangère;	Les ministères et organismes ont élaboré des évaluations exhaustives des menaces et des risques liés à l'ingérence étrangère. Il s'agit d'une analyse permanente qui tient compte de l'évolution de la menace et des mesures prises pour la contrer. Les ministères et organismes ont collaboré avec des intervenants de divers secteurs pour échanger de l'information sur les menaces et aider à cerner les risques. Il reste des défis à relever pour mesurer et décrire concrètement les préjudices liés à l'ingérence étrangère dans certains secteurs d'intérêt stratégique. Le gouvernement tirera parti du nouveau Bureau national de lutte contre l'ingérence étrangère et des programmes universitaires et d'autres programmes de sensibilisation pour inciter les intervenants à évaluer davantage les répercussions à court et à long terme de l'ingérence étrangère au Canada.
	b) examiner et prendre en main la vaste étendue des vulnérabilités institutionnelles auxquelles s'attaquent les États étrangers	Les ministères et organismes ont élaboré des évaluations exhaustives des menaces et des risques liés à l'ingérence étrangère.

18 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
	hostiles, y compris les champs ne faisant expressément pas partie de l'examen du Comité;	Les outils utilisés par les acteurs étatiques étrangers pour mener des activités d'ingérence continuent d'évoluer et nécessitent des évaluations continues des risques. Les ministères et organismes continueront de collaborer avec les intervenants pour évaluer les vulnérabilités dans les secteurs stratégiques. Le budget de 2023 propose un financement de 48,9 millions de dollars sur trois ans à la Gendarmerie royale du Canada (GRC) pour protéger les Canadiennes et les Canadiens contre le harcèlement et l'intimidation, augmenter sa capacité d'enquête et s'engager de manière plus proactive avec les communautés qui sont plus à risque d'être ciblées.
	c) évaluer la validité des lois en vigueur liées à l'ingérence étrangère, comme la *Loi sur la protection de l'information* et la *Loi sur le Service canadien du renseignement de sécurité*, et permettre la proposition de modifications au besoin	Au cours des dernières années, les ministères et organismes ont effectué une analyse stratégique et juridique afin de cerner les lacunes et d'élaborer des options pour les combler. S'appuyant sur les travaux en cours du rapporteur spécial indépendant et sur les examens du CPSNR et de l'OSSNR, le ministre de la Sécurité publique s'efforcera de consulter et d'apporter des changements à la *Loi sur le Service canadien du renseignement de sécurité*, à la *Loi sur la protection de l'information* et au *Code criminel*.
	d) élaborer des mécanismes opérationnels et stratégiques pratiques et pangouvernementaux pour cerner les activités des États hostiles et y réagir;	La création du Bureau national de lutte contre l'ingérence étrangère renforce la gouvernance actuelle de la sécurité nationale et la capacité du gouvernement à lutter efficacement contre les activités d'ingérence étrangère. Le budget de 2023 prévoit un financement de 13,5 millions de dollars sur cinq ans et 3,1 millions de dollars par la suite à Sécurité publique Canada pour mettre sur pied le Bureau national de lutte contre l'ingérence étrangère. Le budget de 2023 propose en outre un financement de 48,9 millions de dollars sur trois ans à la GRC pour protéger les Canadiennes et les Canadiens contre le

19 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
		harcèlement et l'intimidation, augmenter sa capacité d'enquête et s'engager de manière plus proactive avec les communautés qui sont plus à risque d'être ciblées. Les ministères et organismes collaborent au sein d'un cadre de gouvernance efficace pour déceler et contrer les activités d'ingérence étrangère. Au cours des dernières années, des mesures ont été prises pour renforcer le cadre de gouvernance de la sécurité nationale afin de garantir que le conseiller à la sécurité nationale et au renseignement (CSNR) continue de s'informer activement des menaces existantes et des mesures d'atténuation, y compris celles liées à l'ingérence étrangère. Le budget de 2022 a octroyé 2 millions de dollars par année pour permettre à l'Unité de protection de la démocratie du Bureau du Conseil privé de coordonner, d'élaborer et de mettre en œuvre des mesures pangouvernementales conçues pour lutter contre la désinformation et protéger les institutions et les processus démocratiques du Canada. Cela comprend l'élaboration d'une approche pansociétale pour protéger la démocratie canadienne, la mise en œuvre d'une trousse d'outils de lutte contre la désinformation et la formation des parlementaires et des fonctionnaires sur la mésinformation et la désinformation, en s'appuyant sur le modèle RESIST du Royaume-Uni. Cela comprend également l'élaboration d'options pour renforcer la gouvernance interministérielle, en tenant compte des comités existants. Le gouvernement du Canada a annoncé un investissement de 5,5 millions de dollars pour renforcer la capacité des partenaires de la société civile et de recherche à fournir des renseignements importants sur l'écosystème canadien de l'information, notamment en ce qui concerne la désinformation et les activités des acteurs étatiques.

20 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
	e) mettre en place des mécanismes réguliers de collaboration avec les paliers infranationaux du gouvernement et les organismes d'application de la loi, y compris fournir les cotes de sécurité nécessaires;	Au cours des dernières années, la GRC, le Service canadien du renseignement de sécurité (SCRS), le Centre canadien pour la cybersécurité et Sécurité publique Canada ont collaboré avec leurs collègues provinciaux, territoriaux et municipaux ainsi qu'avec les propriétaires et les exploitants d'infrastructures essentielles afin de mieux faire connaître les menaces d'ingérence étrangère et de renforcer leur résilience. Un engagement soutenu, régulier et coordonné avec les partenaires est essentiel pour détecter les menaces, renforcer la résilience et contrer efficacement les activités d'ingérence étrangère. Le nouveau Bureau national de lutte contre l'ingérence étrangère travaillera en vue d'élargir les mécanismes d'information avec les autorités provinciales, territoriales, municipales et autochtones. L'Unité de protection de la démocratie du Bureau du Conseil privé collaborera également davantage avec les provinces et les territoires.
	f) comprendre une approche à l'intention des ministres et des hauts dirigeants afin qu'ils nouent le dialogue avec les institutions fondamentales et la population;	Les ministères et organismes ont accru leurs capacités à mener des activités de sensibilisation, ce qui comprend la mobilisation des intervenants par le SCRS (industrie, universités, secteur de la recherche et du développement, collectivités canadiennes, société civile), les activités de sensibilisation du Centre de la sécurité des télécommunications (CST) et du Centre canadien pour la cybersécurité (industrie, petites entreprises, infrastructures essentielles privées) et les efforts de sensibilisation communautaire de la GRC. La communication et la sensibilisation sont des éléments clés de la stratégie gouvernementale pour lutter contre l'ingérence étrangère. Les efforts se poursuivront pour mobiliser de manière efficace et cohérente les partenaires de tous les ordres de gouvernement. Le gouvernement prendra avantage du nouveau Bureau national de lutte contre l'ingérence étrangère et du prochain rapport

21 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
		annuel du SCRS pour améliorer la communication avec la population canadienne. Le financement récemment annoncé en vue de renforcer la capacité des partenaires de la société à contrer la désinformation, y compris celle provenant de sources étrangères, aidera également à accroître la résilience. De nouvelles séances d'information seront offertes aux députés et aux sénateurs et le Bureau travaillera en vue d'étendre l'offre de séances aux partenaires externes au gouvernement fédéral. Le gouvernement examinera la possibilité de mettre en œuvre un processus par lequel les ministres et les hauts fonctionnaires, y compris les membres du Groupe d'experts dans le cadre du Protocole public en cas d'incident électoral majeur, communiqueront avec les intervenants et les communautés. Cette mobilisation permettrait de recueillir des avis sur les pratiques exemplaires afin d'atténuer les répercussions de l'ingérence étrangère et de la désinformation sur les institutions canadiennes.
	g) orienter la coopération avec les alliés au sujet de l'ingérence étrangère.	Les ministères et organismes participent avec leurs homologues internationaux à des efforts de collaboration et à des partenariats visant à contrer l'ingérence étrangère. Le Bureau national de lutte contre l'ingérence étrangère assurera la cohérence de ces efforts interministériels et veillera à ce qu'ils cadrent avec les objectifs de la politique étrangère du Canada. Le ministre de la Sécurité publique coopère également avec les alliés du Canada en tant que représentant du Canada à la réunion ministérielle des cinq pays, où les ministres de la Sécurité du Groupe des cinq se réunissent pour collaborer sur diverses questions de sécurité nationale, notamment l'ingérence étrangère, discuter de leurs approches respectives concernant des enjeux communs et coordonner une réponse cohérente du Groupe des cinq.

22 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
2	Le gouvernement du Canada appuie cette stratégie exhaustive grâce à une direction et une coordination centrales durables. Pour donner un exemple d'entité de coordination centrale visant à agir sur l'ingérence étrangère, le Comité renvoie à la nomination et au mandat du coordonnateur de la lutte nationale contre l'ingérence étrangère de l'Australie.	Le premier ministre a annoncé la création du Bureau national de lutte contre l'ingérence étrangère. Le budget de 2023 prévoit un financement de 13,5 millions de dollars sur cinq ans et 3,1 millions de dollars par la suite à Sécurité publique Canada pour mettre sur pied le Bureau national de lutte contre l'ingérence étrangère. Le budget de 2022 a octroyé 2 millions de dollars par année pour permettre au Bureau du Conseil privé de coordonner, d'élaborer et de mettre en œuvre des mesures pangouvernementales conçues pour lutter contre la désinformation et protéger la démocratie canadienne.
Rapport spécial du CPSNR sur les allégations entourant la visite officielle du premier ministre Trudeau en Inde en février 2018		
1	1.A. Dans l'intérêt de la sécurité nationale, il faudrait informer les députés de la Chambre des communes et les sénateurs des risques que représentent l'ingérence étrangère et l'extrémisme au Canada au moment de leur assermentation, et un suivi en ce sens devrait être effectué régulièrement par la suite.	Le Service de protection parlementaire offre des séances d'information aux nouveaux parlementaires. Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections offre des séances d'information aux représentants des partis politiques pendant la période électorale. La Division des opérations de la sécurité du Bureau du Conseil privé informe tous les nouveaux ministres et secrétaires parlementaires de l'éventail des menaces à la sécurité, ce qui comprend l'ingérence étrangère. Le SCRS offre également des séances d'information aux parlementaires sur demande. Des séances d'information seront offertes aux députés et aux sénateurs à la suite de leur assermentation ainsi que sur une base régulière à l'avenir.
	1.B. De plus, il faudrait rappeler aux ministres du Cabinet les attentes énoncées dans le document du gouvernement *Pour un gouvernement ouvert et responsable*, notamment le fait que l'on s'attend à ce que les ministres fassent preuve de discernement	Les obligations et attentes concernant les ministres et leurs activités sont rendues publiques dans le cadre de l'application de *Pour un gouvernement ouvert et responsable*.

23 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
	quant aux personnes qu'ils rencontrent et avec lesquelles ils établissent des liens et à ce qu'ils fassent clairement la distinction entre les messages officiels et les messages privés dans les médias. Il faudrait aussi leur rappeler que conformément à la *Loi sur les conflits d'intérêts*, les titulaires d'une charge publique doivent toujours accorder la priorité à l'intérêt public avant leurs intérêts personnels.	
2	Le ministre de la Sécurité publique et de la Protection civile devrait envisager de modifier *** afin d'y inclure un rôle officiel pour le conseiller à la sécurité nationale et au renseignement (CSNR). Le Comité estime qu'il est légitime que le CSNR formule des conseils en sa qualité de coordonnateur de la communauté de la sécurité et du renseignement et de conseiller auprès du premier ministre.	Des mesures ont été prises pour renforcer davantage le cadre de gouvernance de la sécurité nationale afin de s'assurer que le conseiller à la sécurité nationale et au renseignement auprès du premier ministre se tient au courant des menaces continues et des mesures d'atténuation, y compris celles liées à l'ingérence étrangère.
Rapport sur l'évaluation du Protocole public en cas d'incident électoral majeur pour 2019 (Rapport Judd)		
1	Mettre en œuvre le Protocole pour la prochaine élection en se fondant sur le même modèle et la même composition. Préparer les membres du groupe bien en amont du scrutin, en commençant par les nouveaux membres. Le seuil élevé des critères à remplir et la prise de décisions par consensus devraient être maintenus, ainsi que l'appui et la participation des mêmes ministères et agences. Cette recommandation se fonde sur le fait que ce modèle a déjà été accepté par les parties concernées et qu'il est possible d'assurer une certaine cohérence dans la composition du groupe. Une stratégie médias devrait également être élaborée.	La Directive du Cabinet sur le Protocole public en cas d'incident électoral majeur a été mise à jour avant l'élection fédérale de 2021. Le même cadre général a été conservé et certains changements ont été apportés à la lumière de l'évaluation de M. Judd. Bien que la stratégie médiatique du gouvernement n'ait pas été aussi complète pour les élections de 2021 que pour celles de 2019 compte tenu de la situation minoritaire du gouvernement, une stratégie de communication plus proactive sera élaborée par le Bureau du Conseil privé pour les élections futures et s'appuiera sur les recommandations formulées par M. Rosenberg.
2	Le Protocole devrait s'appliquer durant la période préélectorale, reconnaissant que ça pourrait ne pas être possible dans le cas d'une élection déclenchée par un vote de censure.	Cette recommandation n'a pas été mise en œuvre, car les ministres ont déjà les responsabilités et les pouvoirs nécessaires pour gérer toute préoccupation concernant l'ingérence étrangère susceptible de survenir entre les élections. La responsabilité

24 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
		ministérielle est un principe fondamental de la démocratie parlementaire canadienne. En s'appuyant sur les recommandations de M. Rosenberg, le gouvernement générera des occasions de communiquer avec les Canadiennes et les Canadiens au sujet des menaces qui pèsent sur les institutions démocratiques et les processus électoraux en tout temps, indépendamment du calendrier électoral.
3	Les équipes de soutien du Bureau du Conseil privé (institutions démocratiques, sécurité et renseignement) devraient surveiller les développements internationaux en portant une attention particulière à toute évolution des tactiques des acteurs malveillants et des contre-mesures défensives prises par les pays cibles (mesures juridiques, réglementaires et opérationnelles). Cela peut également comprendre les recherches universitaires et de groupes de réflexion.	Le gouvernement continuera de s'appuyer sur le travail existant des alliés et de tirer des leçons des pratiques exemplaires. Par exemple, le gouvernement pourrait renouer le dialogue avec ses partenaires canadiens pour faire avancer le travail accompli dans le cadre de l'Appel de Paris afin de s'assurer que les alliés du Canada ont accès à l'expertise la plus récente pour protéger les processus électoraux. De plus, le budget de 2022 a prévu des fonds pour coordonner, élaborer et mettre en œuvre des mesures pangouvernementales conçues pour lutter contre la désinformation et protéger la démocratie canadienne. L'Unité de protection de la démocratie entreprend de travaux de recherche sur les menaces qui pèsent sur la démocratie. En mai 2022, le gouvernement a également alloué 13,4 millions de dollars sur cinq ans afin d'approfondir la coordination entre les pays pour cerner les menaces étrangères à la démocratie, notamment la désinformation instiguée par des États, et réagir à ces menaces.
4	Établir immédiatement les mêmes liens avec les partis politiques, surtout en ce qui a trait aux conseils et au soutien concernant la sécurité informatique, car ces derniers représentent des cibles probables et ce, même en dehors des périodes électorales.	Des séances d'information ont été organisées à l'approche des élections de 2021. Le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections prévoit organiser des réunions d'information similaires lors des prochaines élections, en s'appuyant sur les recommandations de M. Rosenberg.

25 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
5	Réaliser une évaluation de la mesure dans laquelle les plateformes de médias sociaux ont été à la hauteur de la Déclaration du Canada sur l'intégrité électorale en ligne. Par la suite, mener des discussions avec les plateformes sur les attentes du gouvernement pour la prochaine élection. Les enseignements tirés de la participation du Canada à l'Appel de Paris pourraient contribuer à façonner d'éventuelles nouvelles ententes.	Un exercice sur les leçons retenues de la Déclaration a été mené à la suite des élections de 2019. Des discussions avec les plateformes ont eu lieu à l'approche des élections de 2021, ce qui a abouti à une déclaration révisée et à trois signataires supplémentaires (TikTok, LinkedIn et YouTube).
Rapport sur l'évaluation du Protocole public en cas d'incident électoral majeur pour 2021 (Rapport Rosenberg)		
1	Les communications publiques sur le Protocole doivent expliquer clairement l'inclusion des acteurs intérieurs et des types d'activités préoccupantes.	Le Bureau du Conseil privé élaborera une stratégie pour mieux communiquer avec les Canadiennes et les Canadiens au sujet du Protocole et de la façon dont il s'inscrit dans la série de mesures visant à contrer l'ingérence étrangère et à protéger les institutions démocratiques.
2	Les préparatifs de la prochaine élection devraient comprendre une évaluation de l'adéquation des capacités de la sécurité ministérielle, de la police de protection de la Gendarmerie royale du Canada et des services de police locaux par rapport au niveau et à la persistance des menaces, et de l'efficacité de la coordination entre ces organes. Il faudrait également revoir la coordination entre les partis politiques et le gouvernement en ce qui concerne les campagnes et les opérations de sécurité.	Le gouvernement évaluera des outils pour améliorer la sécurité et l'information des parlementaires afin de tenir compte de l'évolution du contexte de la menace, des lacunes en matière de sécurité et des préoccupations en matière de sûreté. Cela est conforme à l'engagement de la lettre de mandat selon lequel le ministre de la Sécurité publique doit collaborer avec le ministre des Affaires intergouvernementales, de l'Infrastructure et des Collectivités pour renforcer la sécurité des ministres et des parlementaires.
3	Il convient d'évaluer si des ajustements doivent être apportés au rôle des membres du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections à la lumière du problème croissant de l'ingérence nationale.	En vue d'améliorer continuellement les mesures prises dans le cadre du Plan pour protéger la démocratie canadienne, le gouvernement examinera le mandat et la composition du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections.
4	Il devrait y avoir une annonce, dans l'année qui suit l'élection précédente, au sujet du plan du gouvernement pour préserver l'intégrité des élections au canada, y compris une explication de la raison du Protocole.	Le Bureau du Conseil privé élaborera une stratégie pour mieux communiquer avec les Canadiennes et les Canadiens au sujet du Protocole et de la façon dont il s'inscrit dans la série de mesures visant à contrer l'ingérence étrangère et à protéger les institutions démocratiques.

26 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
5	Le plan et les communications publiques du gouvernement doivent reconnaître que le problème de l'ingérence se pose aussi bien avant le déclenchement des élections que pendant la période d'application de la convention de transition. Il faudrait indiquer plus clairement comment l'ingérence préélectorale sera gérée et par qui et ne pas se limiter à dire qu'elle sera gérée par les voies ministérielles normales.	Le ministre des Affaires intergouvernementales, de l'Infrastructure et des Collectivités, avec l'appui du Bureau du Conseil privé et du ministre de la Sécurité publique, cherchera à accroître les communications avec les Canadiennes et les Canadiens au sujet des menaces qui pèsent sur les institutions démocratiques et les processus électoraux en tout temps, indépendamment du calendrier électoral.
6	Il est recommandé que le gouvernement examine les options permettant de s'assurer que le Groupe d'experts est bien préparé et que, dans la mesure du possible, la continuité au sein du Groupe d'experts est assurée entre les élections.	Le Bureau du Conseil privé veillera à ce que les membres du Groupe d'experts soient constamment prêts à assumer leurs responsabilités en informant les nouveaux membres des rôles et responsabilités du Groupe d'experts dans les trois mois suivant leur nomination.
7	Les séances d'information du groupe d'experts devraient commencer beaucoup plus tôt au cours du mandat et inclure des acteurs non gouvernementaux ayant une expertise en matière d'ingérence et de désinformation.	Le Bureau du Conseil privé veillera à ce que les membres du groupe d'expert soient toujours prêts à assumer leurs responsabilités liées au groupe d'expert en présentant aux nouveaux membres du Groupe d'experts une séance d'information dans les trois mois suivant leur nomination à leur nouveau poste afin d'expliquer les rôles et les responsabilités du groupe. À compter du printemps 2023, des réunions du Groupe d'experts seront tenues régulièrement.
8	Un organe de surveillance devrait avoir la possibilité d'évaluer les décisions des ministres concernant l'utilisation de mesures de réduction de la menace pendant la période d'application de la convention de transition.	Le CPSNR et l'OSSNR peuvent effectuer des examens conformément à leur mandat.
9	Le gouvernement devrait envisager de modifier l'article 6.0 pour prévoir que, à moins de motifs impérieux liés à la sécurité nationale et à l'intérêt public, une annonce sera faite si les critères sont remplis.	Pour donner suite au rapport de M. Rosenberg, le gouvernement examine la Directive du Cabinet et étudie les changements possibles.
10	Le gouvernement devrait envisager de supprimer la quatrième phrase du dernier paragraphe de l'article 6.0 et de préciser que l'incidence réelle ou potentielle est l'un des nombreux facteurs que le Groupe d'experts prend en compte dans l'exercice de son	Pour donner suite au rapport de M. Rosenberg, le gouvernement examine la Directive du Cabinet et étudie les changements possibles.

27 Contrer une menace en évolution

	Recommandation	Mesures clés et prochaines étapes
	jugement pour déterminer si les critères ont été remplis.	
11	Il convient d'étudier plus avant la question de savoir si le Protocole doit être modifié pour prévoir la possibilité qu'une annonce soit faite même si les critères établis à l'article 6.0 ne sont pas remplis.	Pour donner suite au rapport de M. Rosenberg, le gouvernement examine la Directive du Cabinet et étudie les changements possibles.
12	Il faudrait tenter d'organiser des séances d'information pour les représentants des partis politiques dans des lieux sécurisés du centre-ville d'Ottawa.	Pendant les périodes électorales, le Bureau du Conseil privé veillera à ce que les séances d'information à l'intention des représentants des partis politiques aient lieu dans des endroits sécurisés du centre-ville d'Ottawa.
13	L'heure de la tenue des séances d'information des représentants des partis politiques devrait être fixée à l'avance, en prévoyant une certaine souplesse pour faire face aux situations urgentes.	Pendant les périodes électorales, le Bureau du Conseil privé veillera à ce qu'un calendrier de séances d'information soit fourni aux représentants des partis politiques dès que possible après la délivrance du bref.
14	Les organismes de sécurité nationale devraient élaborer un programme de séances d'information non classifiées pour sensibiliser les députés et les sénateurs à l'ingérence étrangère et à l'ingérence dans les élections, ainsi qu'aux mesures qu'ils peuvent prendre pour se protéger et protéger leurs informations en ligne.	De nouvelles séances d'information seront offertes aux parlementaires et leur personnel.
15	Le Protocole doit être maintenu sous réserve des modifications mentionnées dans le présent rapport.	La Directive du Cabinet demeure en vigueur et, par conséquent, le Protocole sera en place pour les prochaines élections fédérales. Les modifications seront considérées comme indiqué dans le présent document.
16	Les communications publiques sur le Protocole doivent mettre l'accent sur l'ensemble des activités qui se déroulent pendant la période d'application de la convention de transition, plutôt que de se concentrer sur l'annonce faite par le Groupe d'experts.	Le Bureau du Conseil privé élaborera une stratégie pour mieux communiquer avec les Canadiennes et les Canadiens au sujet du Protocole et de la façon dont il s'inscrit dans la série de mesures visant à contrer l'ingérence étrangère et à protéger les institutions démocratiques.

Table of Initiatives – Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions

Initiative	Lead
Communicating with Canadians About Foreign Interference and Protecting Canada's Democracy	
Undertake more robust and frequent communications with Canadians on foreign interference and efforts taken to protect Canadian democracy	PSC, RCMP, PCO
Adopting emerging communications best practices to strengthen the capacity of the Government of Canada to help combat disinformation based on the RESIST model	PSC, PCO
Use CSIS' upcoming Annual Report as an opportunity to bolster ongoing communications related to foreign interference with Canadians	CSIS, PCO, PSC
Explore expanding briefing mechanisms on foreign interference to provinces, territories, municipalities and Indigenous officials	PCO, PSC
Strengthen capacity of civil society partners to counter disinformation	PCO, PCH
Ensure Panel members (as part of the Critical Election Incident Public Protocol) are in a constant state of readiness to assume their Panel-related responsibilities	PCO
Effective Governance and Strong Legal Frameworks	
Creation of the National Counter-Foreign Interference Coordinator within Public Safety	PSC
Public consultations on the implementation of a Foreign Influence Transparency registry	PSC
Explore modernizing the *CSIS Act* to allow CSIS to better operate in the digital world by: • Effectively collecting and using digital data • Enabling intelligence sharing with non-government partners to help counter threats • Enabling intelligence collection and conducting activities to counter foreign threats not envisioned when *CSIS Act* came into force • Examining how the Public Order Emergency Commissions final report recommendations can information legislative changes to the *CSIS Act* • Developing a consultation and communications plan to address how Canadian interests and Charter rights will be respected while still enabling necessary legislative reform	PSC, CSIS, DOJ, PCO
Undertake analysis to determine if further amendments or new offences to facilitate the prosecution of foreign interference activities are required under the *Security of Information Act* and the *Criminal Code*	PSC, RCMP, PCO, DOJ, PPSC

Initiative	Lead
Examine whether potential amendments to the *Canada Elections Act* are required to counter foreign interference	PCO
Risks, Vulnerabilities, and Security	
Protect Canadians from harassment and intimidation, increase investigative capacity, and engage more proactive with at-risk communities through Budget 2023 investments	RCMP, PSC
Continue to engage with stakeholders in academia and other outreach programs to assess short and long-term impacts of foreign interference in Canada	PSC
Continue to update assessments as threat of foreign interference evolves	PSC, PCO, CSIS, CSE, RCMP
Undertake a comprehensive analysis of security and tools to align with the threat environment, including foreign interference, threats and protective measures available to Ministers, other Parliamentarians and senior officials	PSC, PCO
Develop further enhancements to the Plan to Protect Canada's Democracy, including: • An examination of making the Security and Intelligence Threats to Elections (SITE) Task Force a permanent entity with a mandate to conduct regular reporting on foreign interference activities • Reviewing the Cabinet Directive on the Critical Election Incident Public Protocol based on the recommendations suggested by Mr. Morris Rosenberg in his evaluation of the Protocol following the 2021 general elections	PCO, others
Engagement to Raise Awareness and Improve Resilience to Foreign Interference	
Strengthen the capacity of civil society partners to provide insight into Canada's information ecosystem, strengthen resilience and digital literacy of the government, industry, civil society and citizens	PCO, PCH, others
Establish a process for Ministers and senior officials, including Panel members, to engage with stakeholders and communities to seek views on best practices to mitigate the impact of foreign interference and disinformation on Canada's institutions	PSC, PCO
Continue working with Canadian partners to further the work accomplished through the Paris Call to ensure broad access to the most current expertise to protect Canada's electoral processes	PCO
Develop briefings for political party representatives in secure locations in Ottawa, with flexibility in scheduling that can adapt/react to urgent situations that may arise during election periods	PCO
Provide briefings to Members of Parliament and the Senate to increase awareness on the threat of foreign interference. This includes the development of a program for unclassified briefings for Parliamentarians and their staff on foreign interference including ways to protect themselves following their swearing-in and ongoing basis going forward	PCO

Membres proposés du Groupe de coordination de direction pour la protection de la démocratie

Participantes et Participants	Équipe
Bureau du Conseil privé	
	Unité pour la protection de la démocratie, Institutions démocratiques
	Affaires intergouvernementales – Politique stratégique et portefeuille social
	Politiques, Unité pour la protection de la démocratie, Institutions démocratiques
	Recherche, Unité pour la protection de la démocratie, Institutions démocratiques
	Engagement et opérations, Unité pour la protection de la démocratie, Institutions démocratiques
BCP – Sécurité et renseignements	
BCP – Groupe de travail sur l'ingérence étrangère	
Patrimoine canadien	
	Initiative de citoyenneté numérique
	Politique stratégique et intégration horizontale
Sécurité publique	
	Lutte contre la radicalisation menant à la violence
	Centre canadien d'engagement Communautaire et prévention de la violence
SP – Politique de Sécurité nationale	

Participantes et Participants	Équipe
Affaires mondiales Canada	
	Centre pour la politique numérique internationale
	Groupe de travail sur l'établissement d'un centre pour la démocratie
	Bureau des droits de la personne, des libertés et de l'inclusion – Démocratie, inclusion et liberté de religion
Innovation, Sciences et Développement économique Canada	
	Direction des conseils en matière de politiques de S-T
	Direction de la politique sur la vie privée et la protection des données
Secrétariat du Conseil du Trésor du Canada	
	Direction de l'intégration de l'ensemble des politiques
	Gouvernement ouvert et Portails
Department of Justice Canada – Ministère de la Justice Canada	
	Direction de la mise en œuvre des politiques
Relations Couronne-Autochtones et Affaires du Nord Canada	
	Direction des politiques stratégiques
Services aux Autochtones Canada	
	Direction des politiques stratégiques
Immigration, Réfugiés et Citoyenneté Canada	
	Élaboration des politiques et développement du savoir
	Groupe de travail anti-racisme

Participantes et Participants	Équipe
Environnement et Changement climatique Canada	
	Justice environnementale et ACS plus
Santé Canada	
	Direction de la coordination et de la planification des politiques
Agence de la santé publique du Canada	
	Direction de la Sécurité et du renseignement en santé publique
Femmes et Égalité des genres Canada	
	Politiques stratégiques et des programmes
Gendarmerie royale du Canada	
Service canadien du renseignement de sécurité	
Centre de la sécurité des télécommunications	

Plan de travail de haut niveau 2023-2024 – Protection de la démocratie canadienne

Printemps 2023

- **Mettre en place le Groupe de coordination de direction pour la protection de la démocratie (mai 2023)**
- Rapport intérimaire du rapporteur indépendant spécial (23 mai 2023)
- Rencontre du groupe de recherche pour la protection de la démocratie (juin 2023)
- Inventaire des mesures gouvernementales pour protéger la démocratie canadienne

Été 2023

- Rencontres du groupe de recherche pour la protection de la démocratie (juillet et septembre 2023)
- **Rencontre du Groupe de coordination de direction pour la protection de la démocratie (août 2023)**
- Inventaire des mesures gouvernementales pour protéger la démocratie canadienne (continuation)
- Débuter le processus de rédaction d'une « réponse gouvernementale intégrée » pour protéger la démocratie canadienne

Automne 2023

- Rencontre du groupe de recherche pour la protection de la démocratie (octobre 2023)
- Rapport final du rapporteur indépendant spécial (fin octobre 2023)
- **Rencontre du Groupe de coordination de direction pour la protection de la démocratie (novembre 2023)**
- Tableronde ministérielle possible sur l'ingérence étrangère (novembre 2023)
- Rédaction de réponses du gouvernement aux rapports d'études de PROC et ETHI (à confirmer)
- Proposition d'une « réponse gouvernementale intégrée » pour protéger la démocratie canadienne
- Lancement du « Countering Disinformation Guidebook » pour les practitiens en communications

Hiver 2024

- Rencontre du groupe de recherche pour la protection de la démocratie (janvier 2024)
- **Rencontre du Groupe de coordination de direction pour la protection de la démocratie (février 2024)**
- Rédaction de demandes de budget (si nécessaire)