



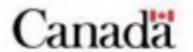
Government of Canada / Gouvernement du Canada

Non classifié



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

L'ingérence étrangère :
Une menace pour la sécurité nationale du Canada



Non
classifié

But

Offrir aux partis politiques des informations exhaustives et à jour sur l'ingérence étrangère.

Objectifs

Donner un aperçu de ce qui suit :

- le GTMSRE et la préparation à l'élection partielle;
- la menace d'ingérence étrangère;
- pourquoi le Canada est visé et quelles sont les cibles;
- qui sont les principaux auteurs de menace;
- les possibilités d'ingérence étrangère connues;
- les cyberactivités liées à la menace;
- les risques de violence et d'extrémisme violent;
- la façon de se protéger.

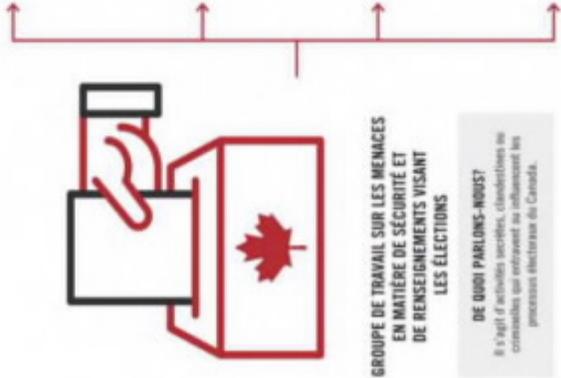


Canada

Non classifié



ACTIVITÉS	MANDAT/RÔLE	
<ul style="list-style-type: none"> • Fournir des renseignements et des cyber-évaluations sur les intentions, activités et capacités des acteurs étrangers de menaces. • Protéger les opérations et les réseaux du gouvernement liés aux élections à l'aide de mesures de cybersécurité. • Fournir des conseils et une orientation en matière de cybersécurité aux partis politiques, aux provinces et aux autres institutions qui participent aux processus démocratiques. 	<p>Sécurité de la technologie de l'information</p> <ul style="list-style-type: none"> • Fournir des conseils, de l'orientation et des services pour aider à assurer la protection de l'information électronique et des systèmes importants. <p>Renseignements étrangers</p> <ul style="list-style-type: none"> • Recueillir des renseignements étrangers destinés au gouvernement du Canada sur les acteurs de menaces. <p>Soutien au Service canadien du renseignement de sécurité (SCRS) et à la Gendarmerie royale du Canada (GRC)</p> <ul style="list-style-type: none"> • Fournir de l'assistance pour les opérations techniques. 	 <p>CST Centre de la sécurité des télécommunications</p>
<ul style="list-style-type: none"> • Fournir des conseils relatifs de menaces et des rapports de renseignement à Elections Canada et au commissaire aux élections fédérales. • Fournir aux décideurs du gouvernement du Canada une évaluation des attitudes et des capacités utilisées pour mener des activités hostiles à l'État. 	<p>Renseignements et réduction des menaces</p> <ul style="list-style-type: none"> • Recueillir des renseignements sur les activités influencées par l'étranger qui posent un enjeu au Canada, sont clandestines ou trompeuses, ou représentent une menace pour la sécurité. • Continuer de telles activités par des mesures de réduction des menaces. <p>Évaluation des renseignements</p> <ul style="list-style-type: none"> • Fournir des conseils, des rapports de renseignement et des évaluations de renseignements au gouvernement du Canada sur les activités influencées par l'étranger. 	 <p>SCRS Service canadien du renseignement de sécurité</p>
<ul style="list-style-type: none"> • Effectuer des recherches sur les campagnes de désinformation ciblant le Canada et menées par des acteurs étrangers. • Réviser compte des tendances, des menaces et des incidents menaçants. • Coordonner l'attribution des incidents. 	<p>Mécanisme de réponse rapide du G7</p> <ul style="list-style-type: none"> • 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. 	 <p>AMC Affaires multinationales Canada</p>
<ul style="list-style-type: none"> • Appuyer 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'appartenance de la loi et de réglementation. 	<p>Sécurité nationale</p> <ul style="list-style-type: none"> • Principale organisation chargée de prévenir, de détecter et de réprimer les menaces criminelles liées à la sécurité nationale au Canada et à l'étranger. • Appuyer sur les actes criminels liés au terrorisme, à l'espionnage, aux cyberattaques et aux activités influencées par l'étranger. • Consulter, pour Elections Canada, le principal organe d'enquête si une activité criminelle est suspectée. 	 <p>GRC Gendarmerie royale du Canada</p>





Élection partielle dans Toronto-St. Paul's

Non
classifié



- Activation du GTMSRE en prévision de l'élection fédérale partielle.
- Surveillance collective des activités liées à la menace.
- Mécanismes internes permettant de faire rapport et de communiquer des informations (Comité des sous-ministres chargé des interventions en matière de renseignement et Comité de coordination sur la sécurité électorale des sous-ministres).
- Activation d'une ligne prioritaire — disponible en tout temps — tout au long de la période de l'élection partielle à l'intention des partis politiques.
- Publication d'un rapport non classifié après l'élection.

Canada



Qu'est-ce que l'ingérence étrangère?

Non
classifié

Le gouvernement du Canada définit **l'ingérence étrangère** comme toute activité malveillante entreprise par un État ou un mandataire d'un État pour favoriser l'atteinte de ses propres objectifs stratégiques au détriment des intérêts nationaux au Canada. Cette définition englobe les activités qui se situent en deçà du seuil du conflit armé, mais qui sont tout de même clandestines, trompeuses, menaçantes ou illégales.

Quel est l'objectif?

Des États étrangers mènent des activités d'ingérence étrangère au Canada pour :

- obtenir un avantage sur le plan stratégique, militaire et économique et dans la collecte de renseignements;
- protéger leur régime;
- décrédibiliser les institutions démocratiques.

L'ingérence étrangère se **distingue des activités d'influence normales**, qui sont légitimes et légales, qui font partie intégrante des relations internationales conventionnelles et qui sont régies par des règles.



Canada



Risque de violence ou d'extrémisme violent

Non
classifié

- Les répercussions sur le Canada des tendances et des incidents observés ailleurs dans le monde surviennent plus rapidement et sont plus importantes qu'auparavant.
- Les auteurs de menace sont animés par tout un éventail de motifs de mécontentement qui sont amplifiés par la mésinformation et la désinformation.
- Les discours menaçants à l'égard des personnalités publiques ont été normalisés et il est bien établi que les menaces adressées aux parlementaires atteignent des sommets pendant les cycles électoraux.
- De multiples facteurs influent sur le risque que des manifestations débouchent sur des actes de violence : caractéristiques démographiques, influence d'idéologues, candidats, historique de la circonscription, etc.



Canada

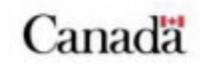


Pourquoi vise-t-on Canada?

Non classifié

Voici quelques caractéristiques qui font du Canada une cible attrayante :

- il a signé plusieurs ententes multilatérales et bilatérales relatives à la défense et au commerce;
- il regorge de ressources naturelles;
- il est un leader dans de nombreux secteurs;
- il comprend une riche diversité et un multiculturalisme important;
- il jouit d'une société ouverte.



For Public Release



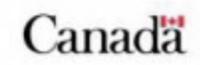
Les élus et les fonctionnaires, cibles d'ingérence étrangère

Non classifié

- Par « élus », on entend notamment :
 - les députés fédéraux;
 - les députés provinciaux;
 - les représentants municipaux;
 - les représentants de gouvernements autochtones.



- Les fonctionnaires, le personnel politique et ministériel et tout personne qui exerce une influence sur les processus de prise de décision d'intérêt publique.
- Les candidats aux élections et leur personnel.





GTMSRE

Que veulent les auteur d'ingérence étrangère?

Non
classifié

- Forcer leurs cibles à **soutenir ou à discréditer des positions politiques précises.**
- Se servir de leurs cibles pour **avoir accès à des décideurs ou à d'autres cibles de grande valeur.**
- Obtenir de leurs cibles des **informations privilégiées** qui les aideraient à atteindre leurs objectifs, notamment :
 - des informations au sujet des politiques et des plans du gouvernement;
 - des informations au sujet de personnes occupant des postes de pouvoir;
 - des informations au sujet des protocoles de sécurité.

For Public Release



Canada



Qui sont les principaux acteurs d'ingérence étrangère?

Non classifié

Voici certains des principaux États étrangers qui mènent des activités d'ingérence étrangère contre le Canada pour servir leurs intérêts stratégiques :



République populaire de Chine (RPC)



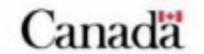
Gouvernement de l'Inde



Russie



Gouvernement du Pakistan





GTMSRE

Possibilités d'ingérence étrangère connues

Non classifié



Financement

- 43^e élection générale – 2019
- 44^e élection générale – 2021



Groupes communautaires

- Grande région de Vancouver, 43^e élection générale – 2019



Nomination de candidats

- Don Valley-Nord



Mesures coercitives

- Don Valley-Nord



Mésinformation et désinformation

- 44^e élection générale, fin août 2021
- Steveston-Richmond-Est, C.-B. et projet de loi C-282
- Député de Wellington-Halton Hills, 4 au 13 mai 2023
- Spamouflage





Cybermenaces pour les parlementaires

Non classifié

Cyberattaques et piratage

- **Tactiques et techniques**
 - Rançongiciels
 - Attaque par déni de service distribué
 - Cyberespionnage
 - Piratage psychologique (p. ex. harponnage, pixel-balise).
- **Cibles**
 - Bases de données (partis ou électeurs)
 - Réseaux et ressources d'organisations
 - Comptes de courriel
- **Objectifs**
 - Accéder à des informations sensibles ou les manipuler
 - Perturber les activités et les campagnes des partis
 - Entacher la réputation

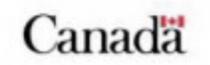
Usurpation d'identité dans les médias sociaux

- **Tactiques et techniques**
 - Piratage psychologique (p. ex. harponnage, soutien technique frauduleux)
 - Compromission d'authentifiants
 - Hypertrucage
 - Vandalisme de comptes et de sites Web.
- **Cibles**
 - Comptes et sites Web officiels des partis
 - Comptes des candidats
 - Comptes administratifs des partis
- **Objectifs**

- Discréditer or embarrasser les cibles.
- Influencer l'opinion publique

Campagnes d'information

- **Tactiques et techniques**
 - Mésinformation, désinformation, malinformation
 - Opérations de piratage et de fuite d'informations
 - Chantage (p. ex. extorsion sexuelle)
- **Cibles**
 - Population canadienne
 - Membres du parti
 - Candidats
- **Objectifs**
 - Entacher la réputation
 - Influencer l'opinion publique et les résultats de l'élection
 - Exercer une contrainte ou un contrôle sur des candidats



For Public Release



GTMSRE

Comment se protéger

Non
classifié

- Méfiez-vous des interactions sociales inusitées et notez-les.
- Méfiez-vous des demandes inappropriées liées à l'argent, à des dons suspects, à des voyages gratuits, à des avantages personnels ou à des cadeaux.
- Suivez les protocoles de sécurité de l'information.
- Faites preuve de rigueur dans vos communications et vos partenariats.
- Suivez les pratiques exemplaires en matière de mot de passe et utilisez l'authentification multifactorielle lorsque possible.
- Tenez à jour vos mobiles, vos ordinateurs et vos applications.
- Protégez vos comptes de médias sociaux.
- Soyez vigilants pour éviter les attaques par hameçonnage et harponnage.
- Conservez vos données en sécurité et adoptez des procédures de sauvegarde.
- Organisez un système de surveillance des médias sociaux et du Web pour mettre au jour et consigner les fausses nouvelles et les hypertrucages liés à votre image et à vos organismes.
- Méfiez-vous des points de connexion Wi-Fi gratuits ou non protégés.



Canada



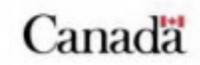
GTMSRE

Comment signaler un incident?

Non classifié

- Si vous ou votre famille êtes en danger immédiat, composer le 911 ou communiquez avec le service de police local.
- Pour signaler de possibles menaces non-immédiates pour la sécurité nationale ou encore des activités suspectes, communiquez avec le SCRS au 613-993-9620 ou au 1-800-267-7685. Vous pouvez aussi remplir le [formulaire Web](#).
- Communiquez avec le Centre canadien pour la cybersécurité du Centre de la sécurité des télécommunications pour obtenir du soutien spécialisé en matière de cybersécurité : composez le **1-833-CYBER-88** ou écrivez à contact@cyber.gc.ca.
- Centre de coordination des opérations de protection de la Gendarmerie royale du Canada : par téléphone au 1-833-226-7622 ou par courriel à protective_policing@rcmp-grc.gc.ca.

For Public Release





GTMSRE

Supplément d'information pour les parlementaires

Non
classifié

- [L'ingérence étrangère et vous](#)
- [Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales](#)
- [Conseils en matière de cybersécurité pour les intervenants politiques](#)
- [Cinq moyens pratiques pour protéger votre campagne](#)
- [Fiche de renseignements relative aux campagnes politiques canadiennes : Protégez vos activités en ligne](#)
- [Parlementaires : Signalez les faux comptes de médias sociaux](#)
- [Considérations liées à la cybersécurité à l'intention des organismes et des administrateurs électoraux \(cours 612\)](#)
- [La cybersécurité à l'intention des décideurs et du personnel des TI travaillant pour un parti politique \(cours 616\)](#)
- Consultez aussi la page sur les [cybermenaces contre les élections](#) ainsi que la [mise à jour sur les cybermenaces contre le processus démocratique du Canada](#) pour en savoir plus.



Canada



GTMSRE

Non classifié

For Public Release

Des questions ?



Le présent document est la propriété du gouvernement du Canada. Il ne peut être modifié, distribué à d'autres que ses destinataires initiaux, diffusé au-delà du public cible, produit, reproduit ni publié, en tout ou en partie, sans l'autorisation expresse du SCRS, compte tenu du rôle de président du GTMSRE joué par ce dernier en 2023-2024.

