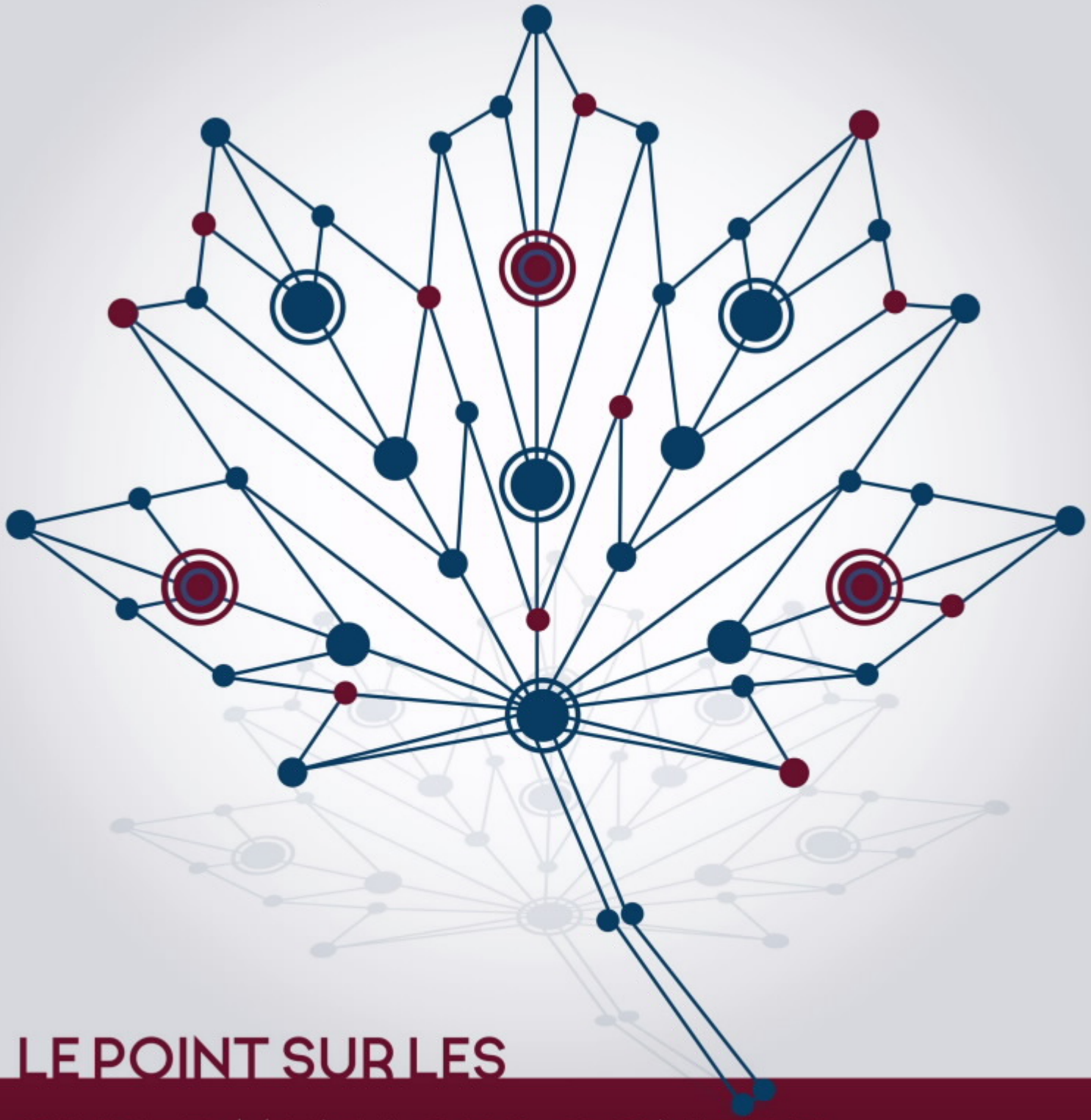
Centre de la sécurité des télécommunications
Communications Security Establishment



LE POINT SUR LES CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA EN 2019

Canada

À PROPOS DU CST

Le Centre de la sécurité des télécommunications (CST) est le centre d'excellence en matière de cyberopérations du Canada. À titre de l'un des principaux organismes de sécurité et de renseignement du pays, le CST protège les réseaux informatiques et les renseignements de grande importance du Canada et procède à la collecte de renseignement électromagnétique étranger. Il fournit également de l'assistance aux organismes chargés de l'application de la loi et de la sécurité dans leurs activités légalement autorisées lorsque ces derniers requièrent ses capacités techniques uniques.

En outre, le CST protège les réseaux informatiques et les renseignements électroniques d'importance pour le gouvernement du Canada, afin d'aider à contrer les activités parrainées par des États et les cybermenaces criminelles contre nos systèmes. De plus, les activités de renseignement électromagnétique étranger du CST appuient les processus décisionnels du gouvernement en matière de sécurité nationale et de politique étrangère; elles permettent aux décideurs de mieux comprendre les crises et les événements mondiaux, et de promouvoir les intérêts du Canada dans le monde.

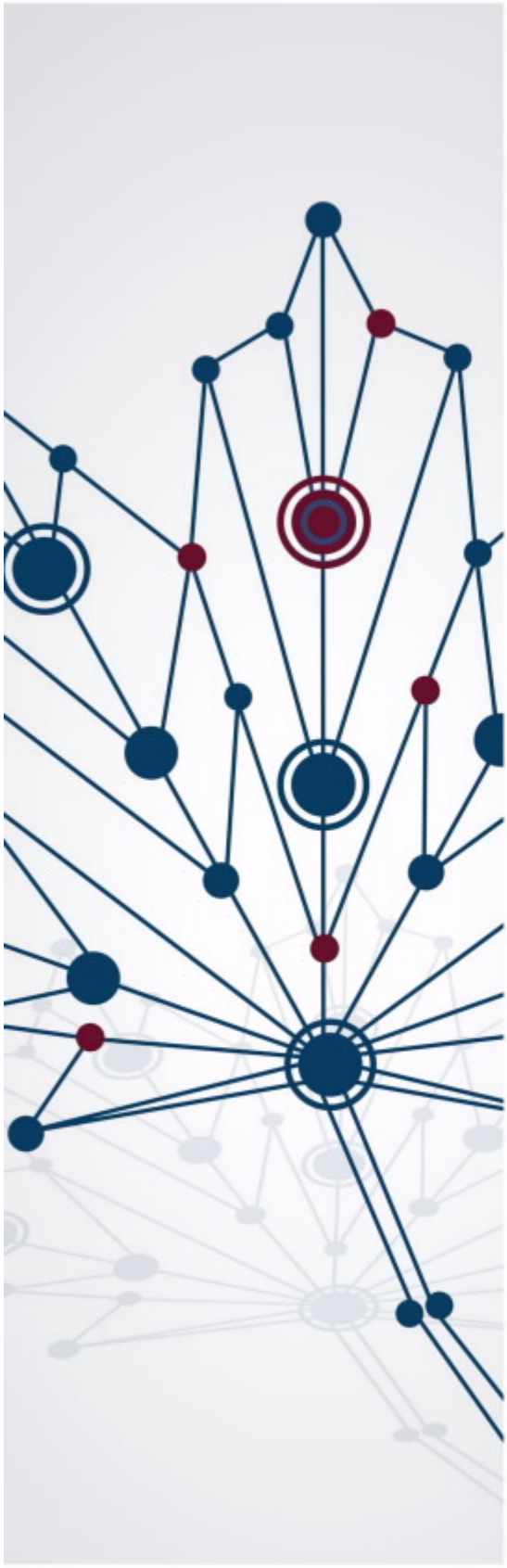
Établi le 1er octobre 2018, le Centre canadien pour la cybersécurité (CCC), qui relève du CST, est un nouvel organisme qui hérite d'un riche passé. Le CCC réunit sous un même toit des spécialistes en sécurité opérationnelle de l'ensemble du gouvernement du Canada. En phase avec la *Stratégie nationale de cybersécurité*, le lancement du CCC marque un tournant vers une approche plus unifiée à la cybersécurité au Canada.

Le CST et le CCC jouent un rôle important dans la protection du Canada et des Canadiens contre le terrorisme basé à l'étranger, l'espionnage étranger, les cybermenaces, l'enlèvement de Canadiens à l'étranger, les attentats visant nos ambassades et d'autres menaces graves émanant d'entités étrangères importantes, en vue d'aider à assurer la prospérité, la sécurité et la stabilité de notre pays.

SOMMAIRE

Ce qu'il faut savoir en 2019 :

- En 2018, des cybermenaces ont ciblé le processus démocratique de la moitié de toutes les démocraties avancées qui tenaient des élections nationales. Le nombre de cybermenaces a donc presque triplé depuis 2015 et nous nous attendons à ce que cette hausse se poursuive en 2019;
- L'ingérence étrangère en ligne, soit les activités d'ingérence menées au moyen de cyberoutils, qui cible les électeurs représente maintenant le type de cybermenace le plus courant contre les processus démocratiques à l'échelle mondiale. Les auteurs de cybermenace manipulent l'information diffusée en ligne, souvent au moyen de cyberoutils, pour influencer l'opinion et le comportement des électeurs;
- Selon nos observations, il est très probable que les électeurs canadiens feront face à une forme quelconque d'activité d'ingérence étrangère en ligne liée aux élections fédérales de 2019. Toutefois, à l'heure actuelle, il est improbable que l'ampleur de cette ingérence étrangère en ligne rivalise avec celle des activités menées par la Russie contre les élections présidentielles de 2016 aux États-Unis;
- Nous estimons que les activités d'ingérence étrangère en ligne contre le Canada s'apparenteront fort probablement aux activités qui ont été menées contre d'autres démocraties avancées au cours des dernières années. Des adversaires étrangers ont tenté d'influencer les idées et les décisions des électeurs en cherchant avant tout à diviser l'opinion sur des enjeux politiques et sociaux, à promouvoir la popularité d'un parti en particulier ou à manipuler les déclarations publiques d'un candidat et ses choix en matière de politiques;
- Depuis la publication du rapport du CST en 2017, les partis politiques, les candidats et leur personnel ont continué d'être la cible de cybermenaces à l'échelle mondiale; toutefois dans une proportion moins élevée que les électeurs. Les auteurs de cybermenace se servent de cyberoutils pour cibler les sites Web, les adresses de courriel, les comptes de médias sociaux, les réseaux et les dispositifs des partis politiques, des candidats et de leur personnel;
- Les cybermenaces ont également continué de cibler des élections dans le monde entier au cours des dernières années. Toutefois, comme nous l'avons noté en 2017, au Canada, les élections fédérales se déroulent encore principalement sur support papier, et Élections Canada a mis en place de nombreuses mesures juridiques, procédurales et liées aux technologies de l'information (TI) qui offrent une protection robuste contre les auteurs de menace qui tentent de modifier secrètement le compte de votes officiel.



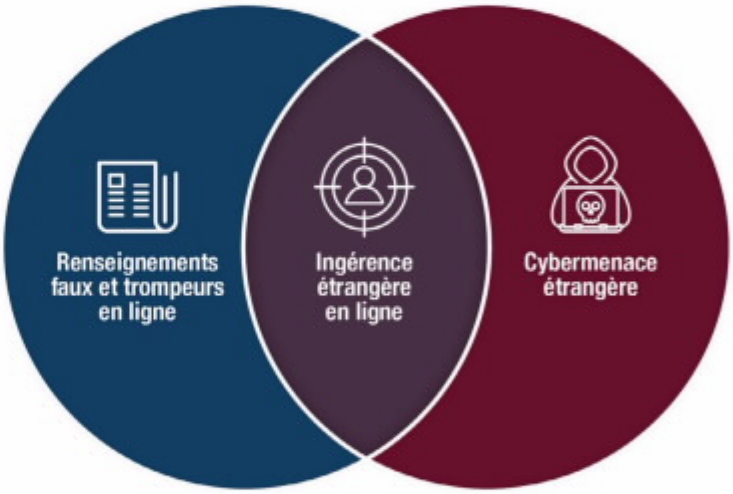
À PROPOS DU PRÉSENT DOCUMENT

Le présent document se veut une mise à jour du rapport que le CST avait publié en 2017. Il vise à informer les Canadiens des cybermenaces qui pèsent sur le processus démocratique du Canada en 2019.

PORTÉE

Le présent rapport traite des cybermenaces qui touchent le processus démocratique. Une cybermenace est une activité menée au moyen de cyberoutils (comme des maliciels ou des courriels de harponnage), qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité du système ou de l'information qu'il contient. Quoiqu'Internet soit truffé de renseignements faux et trompeurs, on parle d'ingérence étrangère en ligne ciblant les électeurs lorsque des auteurs de menace étrangers ont recours à des cyberoutils pour manipuler secrètement l'information diffusée en ligne dans le but d'influencer l'opinion et le comportement des électeurs.

Ingérence étrangère en ligne ciblant les électeurs



SOURCES

Les propos formulés dans la présente sont fondés sur des sources classifiées et non classifiées. Le mandat de renseignement étranger du CST lui procure de précieuses informations sur le comportement des adversaires. En outre, le rôle que joue le CST dans la protection des systèmes d'information du gouvernement du Canada lui confère une perspective unique des tendances observées dans l'environnement de cybermenaces.

LIMITES

Le présent document traite d'une panoplie de cybermenaces contre les activités politiques et électorales à l'échelle nationale et internationale, tout particulièrement dans le contexte des élections fédérales qui auront lieu en 2019 au Canada. La prestation de conseils sur l'atténuation des cybermenaces ne s'inscrit pas dans la portée du présent rapport.

INFORMATION SUPPLÉMENTAIRE

Le site Web du CCC renferme des ressources supplémentaires, comme Les 10 mesures de sécurité des TI et la campagne Pensez cybersécurité.

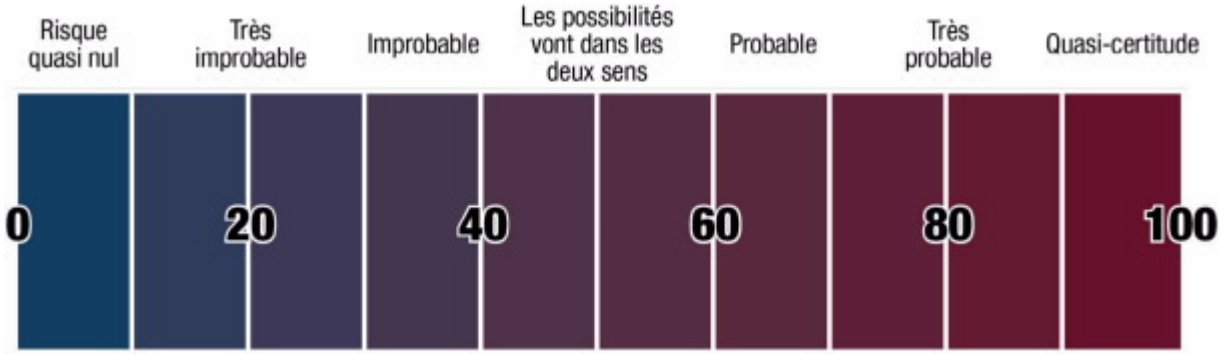
Les lecteurs qui souhaitent en savoir plus sur les cyberoutils et le paysage en évolution des cybermenaces sont priés de consulter l'Évaluation des cybermenaces nationales et l'Introduction à l'environnement de cybermenaces, publiées à l'automne 2018 par le CST.

PROCESSUS D'ÉVALUATION

La présente évaluation est basée sur un processus d'analyse qui comprend l'évaluation de la qualité des renseignements disponibles, l'étude de différentes explications, l'atténuation des biais et l'usage d'un langage probabiliste. Nous employons des termes comme « nous estimons que » ou « selon nos observations » pour communiquer les évaluations analytiques. Des qualificatifs comme « possiblement », « susceptible », « probable » et « très probable » expriment les probabilités.

LEXIQUE DES ESTIMATIONS

Le tableau ci-dessous fait coïncider le lexique des estimations à une échelle de pourcentage approximative. Ces nombres ne proviennent pas d'analyses statistiques, mais sont plutôt basés sur la logique, les renseignements disponibles, des jugements antérieurs et des méthodes qui accroissent la précision des estimations.



La présente évaluation des menaces se fonde sur des renseignements disponibles en date du 1er mars 2019.

LE POINT SUR LES CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA

INTRODUCTION

Le CST a publié son évaluation intitulée Cybermenaces contre le processus démocratique du Canada en juin 2017. Ce rapport examinait les cybermenaces contre les processus démocratiques à l'échelle mondiale. Les principales conclusions de cette évaluation sont toujours valables aujourd'hui :

- Les cybermenaces sont en hausse partout dans le monde, et le Canada ne fait pas exception;
- Un petit nombre d'États-nations sont à l'origine de la majorité des cybermenaces pesant sur les processus démocratiques dans le monde entier;
- Au fédéral, les électeurs, les candidats et les partis politiques sont plus vulnérables, par l'entremise de plateformes de médias en ligne, que les élections comme telles.

Depuis la publication du rapport en juin 2017, les cybermenaces contre les processus démocratiques se sont largement répandues dans le monde entier. Nous estimons que la probabilité que des cybermenaces ciblent le processus démocratique du Canada au cours des élections fédérales de 2019 a augmenté.

La présente mise à jour porte principalement sur les activités de cybermenace entreprises par des adversaires étrangers dans le but de s'ingérer dans le processus démocratique. Nous distinguons les adversaires étrangers des autres auteurs de menace, comme les cybercriminels, qui généralement n'ont pas l'intention de s'ingérer dans le processus démocratique, mais le font accidentellement en tentant d'atteindre d'autres objectifs. Quoiqu'il soit extrêmement difficile de mesurer l'incidence des cybermenaces sur les résultats des élections, la simple impression d'une ingérence étrangère peut saper la confiance dans la démocratie.

En dépit de l'augmentation des cybermenaces contre les processus démocratiques à l'échelle mondiale, le cours des choses s'est quelque peu amélioré depuis la publication de l'évaluation de 2017. Une couverture médiatique et une analyse exhaustives de l'ingérence étrangère en ligne, ainsi que des rapports fréquents sur les cyberincidents majeurs et leur attribution publique par le CST et les alliés, ont permis de mieux faire connaître les menaces éventuelles au public. Par ailleurs, les fournisseurs de services Internet se sont montrés disposés à empêcher que leurs plateformes soient utilisées de manière illégitime pour mener des activités d'ingérence étrangère en ligne.

De plus, en 2018, des accusations ont été portées contre des personnes en Russie qui se seraient ingérées dans les élections présidentielles de 2016 aux États-Unis. On observe ainsi un changement vers une approche qui ne consiste plus uniquement à détecter et à contrer les activités malveillantes, mais aussi à confronter et à poursuivre en justice les auteurs de cybermenace qui ciblent le processus démocratique américain.

POURQUOI CIBLER LE PROCESSUS DÉMOCRATIQUE DU CANADA?

LE CANADA DANS LE MONDE

Le Canada fait partie du G7 et de l'OTAN, et est un membre actif de la communauté internationale. Par conséquent, les choix du gouvernement du Canada en matière de déploiements militaires, d'accords commerciaux et d'investissements, d'échanges diplomatiques, d'aide étrangère ou de politique sur l'immigration intéressent les autres États. La position du Canada peut avoir une influence sur les intérêts fondamentaux d'autres pays, de groupes étrangers et de particuliers. Des adversaires étrangers pourraient utiliser des cyberoutils pour cibler le processus démocratique dans le but de modifier les résultats des élections, d'influencer les choix des responsables des politiques et les relations du gouvernement avec ses partenaires étrangers et nationaux ou de nuire à la réputation du Canada à l'échelle mondiale.

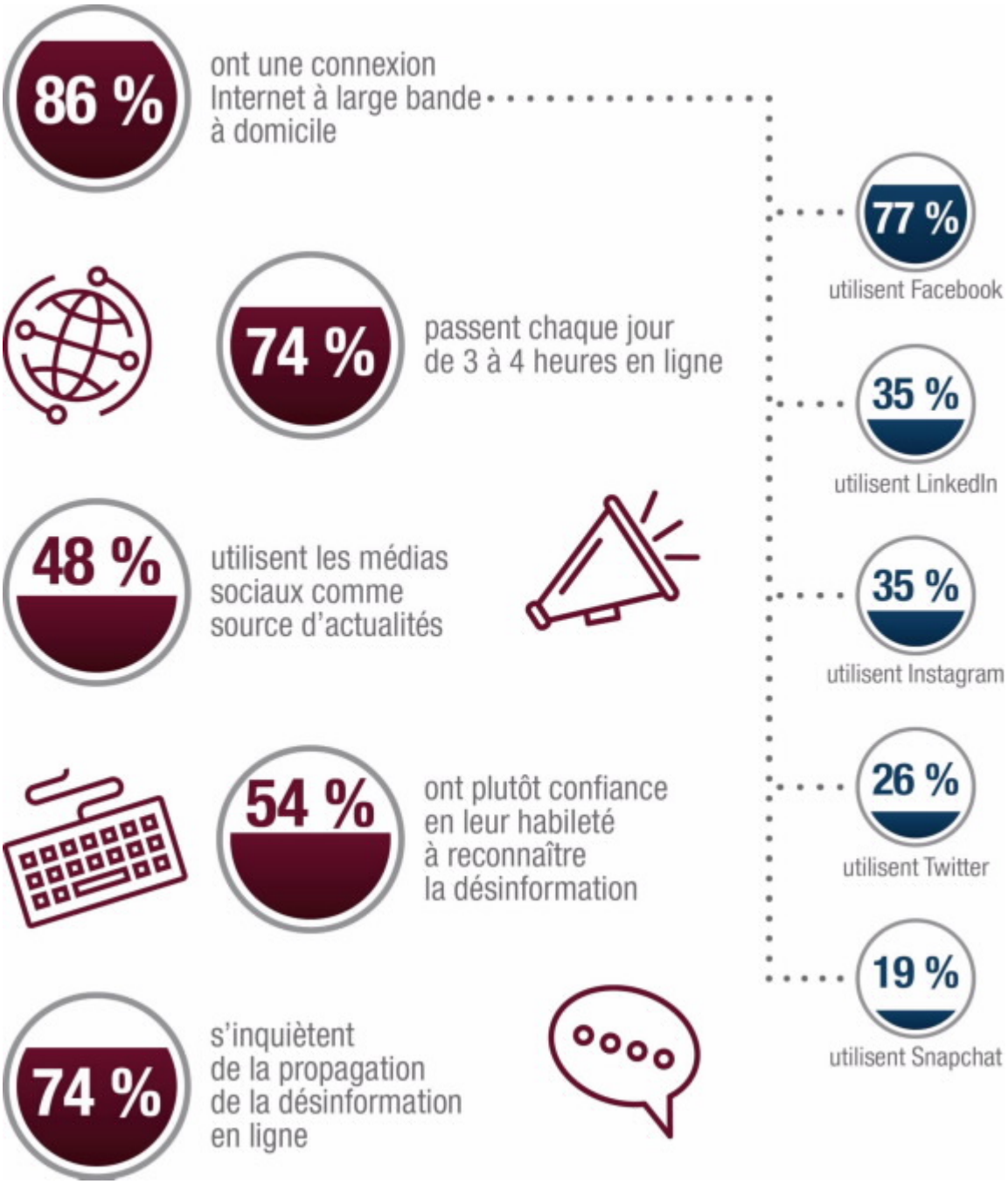
LE CANADA MÈNE DES ACTIVITÉS EN LIGNE TOUT COMME SES ADVERSAIRES ÉTRANGERS

Les Canadiens vivent dans l'une des sociétés les plus branchées au monde. Par conséquent, ils se doivent d'être plus vigilants quant à l'utilisation des cyberoutils que les citoyens de pays moins branchés. La grande majorité des Canadiens font appel aux services offerts par les principaux fournisseurs de services Internet pour obtenir de l'information, communiquer entre eux et former des collectivités[1]. Des adversaires étrangers qui cherchent à s'ingérer dans le processus démocratique du Canada pourraient exploiter cette société hautement branchée en utilisant des cyberoutils pour accentuer leurs activités d'ingérence au Canada.

LES ADVERSAIRES ÉTRANGERS ONT INVESTI DANS LEUR CYBERPUISSANCE

Les cybercapacités font maintenant partie des moyens qu'utilisent les États-nations pour faire avancer leurs intérêts dans le monde entier. De plus en plus, les adversaires étrangers voient la cyberpuissance comme un moyen d'atteindre leurs objectifs stratégiques, qu'il s'agisse d'assurer leur sécurité nationale ou leur prospérité économique ou même de faire avancer les objectifs politiques ou les objectifs idéologiques généraux d'un régime. Pour ces adversaires, les cyberoutils sont des moyens relativement bon marché, dont ils peuvent décliner toute responsabilité, qui s'ajoutent aux activités d'espionnage ou aux mesures militaires ou diplomatiques traditionnelles.

FIGURE 1 : Les Canadiens et Internet *(données tirées de CIRA.CA[2])*



RÉPERCUSSIONS POSSIBLES DES CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE

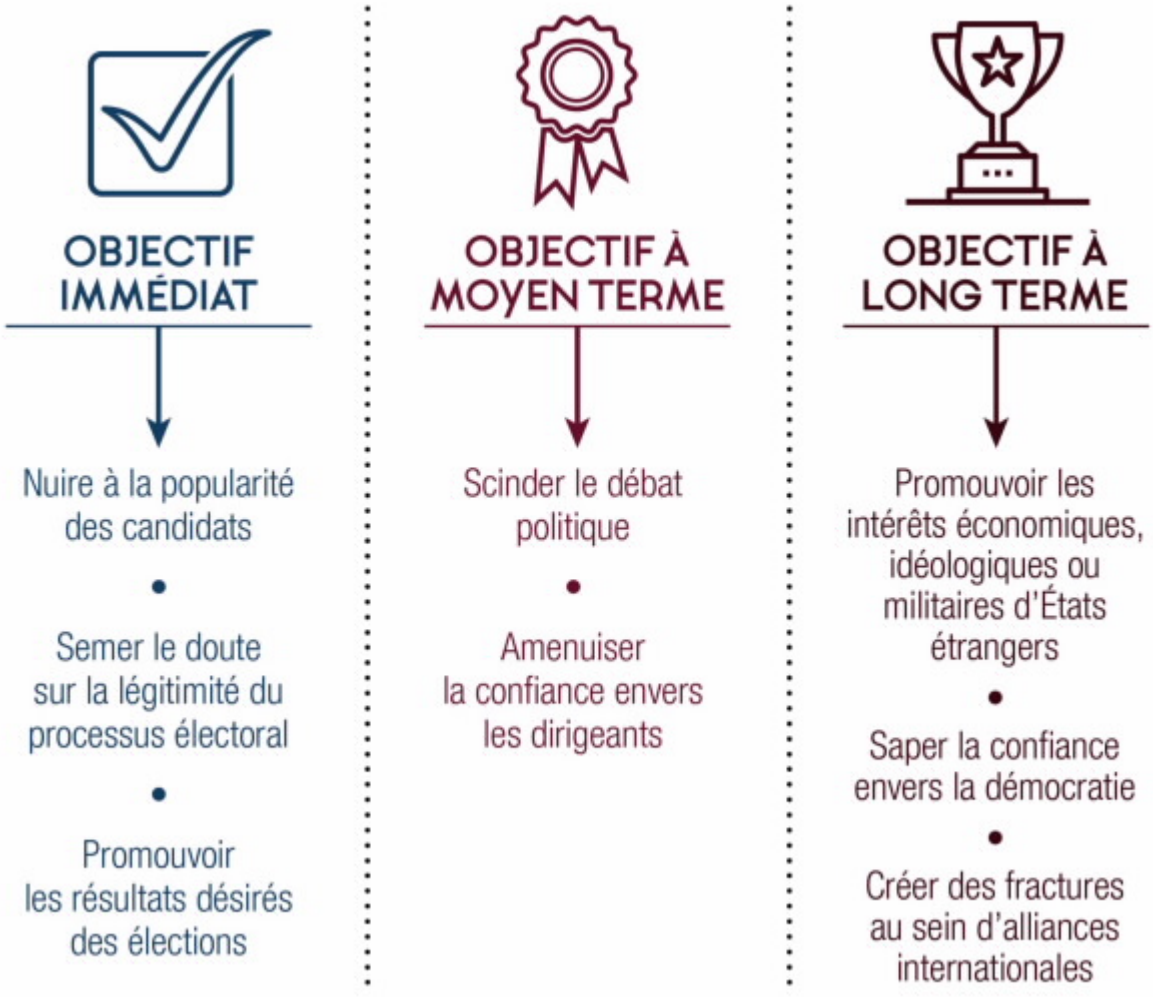
À court terme, les cybermenaces peuvent notamment avoir les conséquences suivantes :

- Dissimuler l'information légitime ou scinder le débat social;
- Nuire à la popularité ou au soutien des candidats;
- Semer le doute sur la légitimité du processus électoral;
- Promouvoir les résultats désirés des élections;
- Distraire les électeurs des enjeux importants.

Les cybermenaces contre le processus démocratique peuvent aussi avoir des conséquences à moyen et à long terme, dont les suivantes :

- Saper la confiance du public envers le processus démocratique;
- Scinder le débat social;
- Créer des fractures au sein des alliances internationales;
- Amenuiser la confiance envers les dirigeants;
- Dissuader des candidats qualifiés de se présenter aux élections;
- Promouvoir les intérêts économiques, géopolitiques ou idéologiques d'États étrangers.

FIGURE 2 : Pourquoi les États-nations font-ils appel à des cybercapacités pour influencer les processus démocratiques de pays étrangers?



CIBLES PRINCIPALES DU PROCESSUS DÉMOCRATIQUE DU CANADA

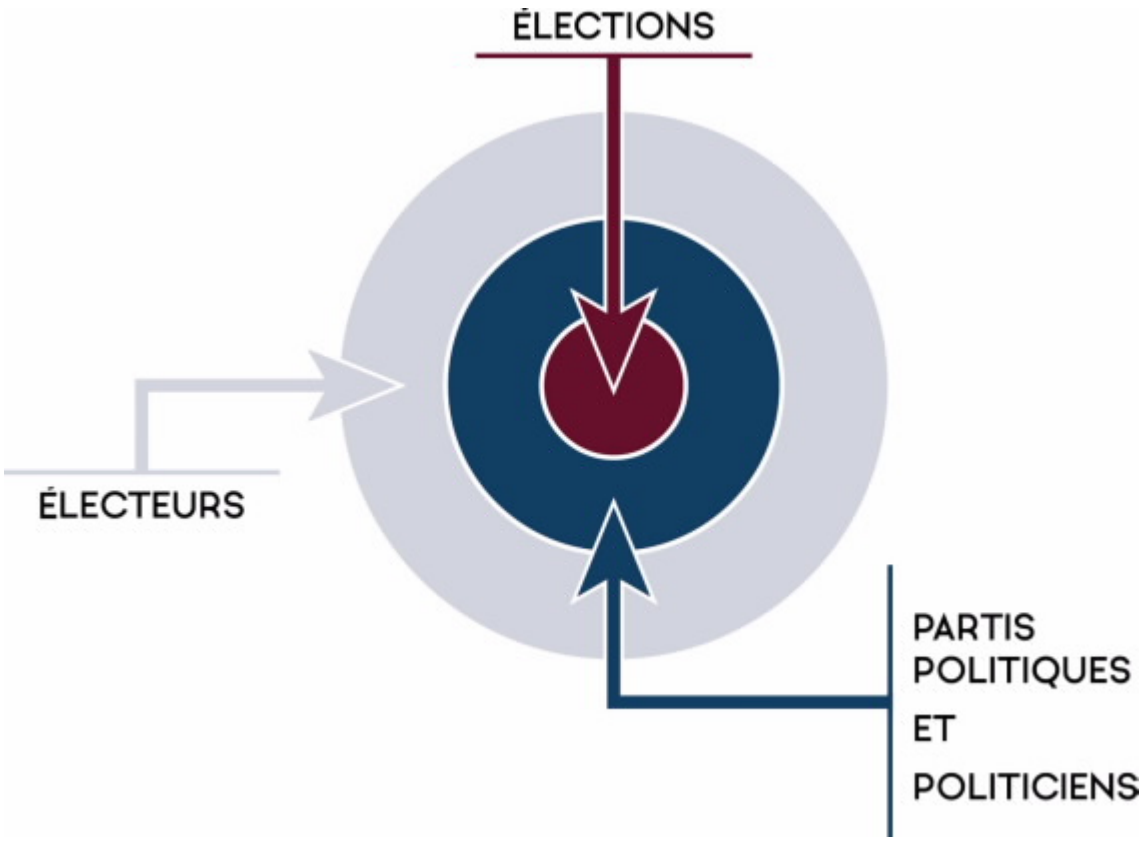
LES CYBERMENACES CONTINUENT DE CIBLER LES TROIS ASPECTS DU PROCESSUS DÉMOCRATIQUE

Les électeurs interagissent avec les partis politiques, les candidats et entre eux au moyen des médias sociaux et traditionnels. Les auteurs de cybermenace manipulent l'information diffusée en ligne, souvent au moyen de cyberoutils dans les médias sociaux, pour influencer l'opinion et le comportement des électeurs. Dans le rapport Cybermenaces contre le processus démocratique du Canada de 2017, nous avions dénommé cette cible « les médias ». Nous avons changé de terme pour mettre davantage l'accent sur la cible comme telle, soit les électeurs, plutôt que sur le moyen de communication.

Les partis politiques, les candidats et leur personnel se disputent l'attention et le soutien des électeurs, surtout au moyen d'Internet qu'ils utilisent pour s'organiser et communiquer avec les électeurs. Les auteurs de cybermenace se servent de cyberoutils pour cibler les sites Web, les adresses de courriel, les comptes de médias sociaux, les réseaux et les dispositifs des partis politiques, des candidats et de leur personnel;

Les élections englobent tous les processus qui entrent en jeu lorsque les Canadiens élisent un député. Pour assurer la réussite du changement de gouvernement, les Canadiens doivent avoir confiance dans la légitimité du processus. Les auteurs de cybermenace pourraient tenter de miner la confiance dans les élections ou d'entraver la participation électorale en modifiant l'information sur les sites Web, les comptes de médias sociaux, les réseaux et les dispositifs qu'utilise Élections Canada.

FIGURE 3 : Processus démocratique du Canada



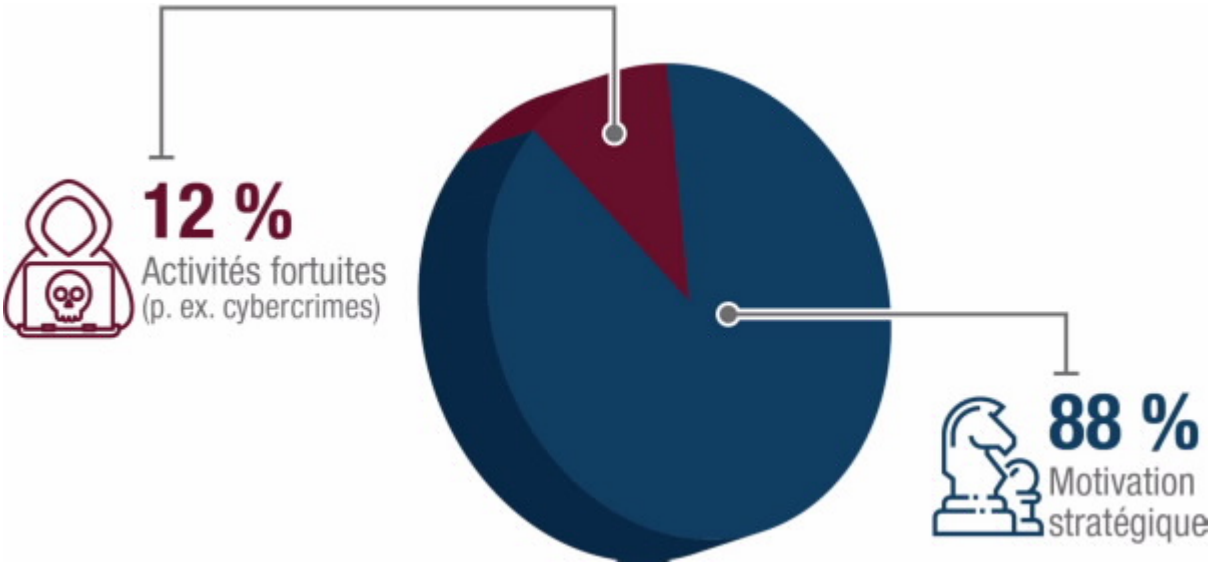
LES TENDANCES MONDIALES ET LA MENACE POUR LE CANADA

DONNÉES DE RÉFÉRENCE MONDIALES SUR LES ÉVÉNEMENTS CONNUS

Depuis la publication de son rapport en 2017, le CST a continué de surveiller les cybermenaces contre les processus démocratiques partout dans le monde. Comme la plupart des activités de cybermenace sont menées secrètement, il est probable que certains incidents soient passés inaperçus. On peut donc supposer que les données du CST sous-estiment le nombre total d'événements.

Comme l'illustre la figure 4 ci-dessous, la grande majorité des cybermenaces qui touchent les processus démocratiques à l'échelle mondiale depuis 2010 est de nature stratégique. Autrement dit, les auteurs de menace ont ciblé un processus démocratique national en particulier dans le but d'en influencer les résultats. Le reste des cybermenaces représentait, en grande partie, des cybercrimes, comme le vol des renseignements personnels des électeurs dans le but de les vendre ou de s'en servir à des fins criminelles.

FIGURE 4 : Cybermenaces contre les processus démocratiques à l'échelle mondiale (2010-2018)

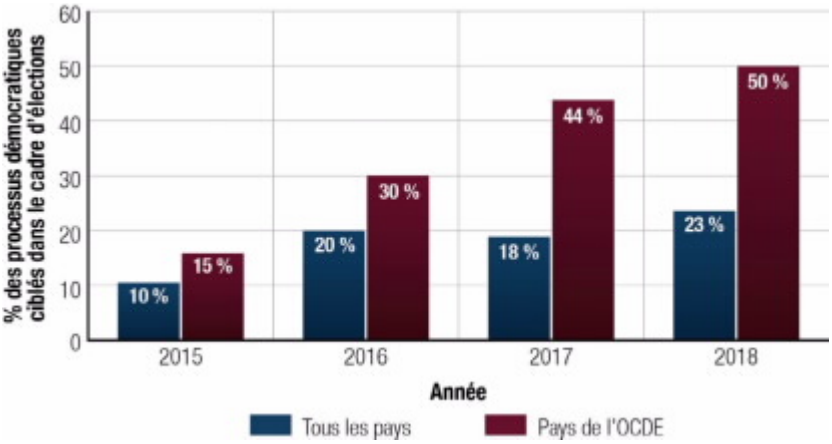


QUATRE GRANDES TENDANCES SE DÉGAGENT DES CYBERMENACES RÉCENTES CONTRE LES PROCESSUS DÉMOCRATIQUES À L'ÉCHELLE MONDIALE

TENDANCE 1 : LES CYBERMENACES CONTRE LES PROCESSUS DÉMOCRATIQUES SONT À LA HAUSSE PARTOUT DANS LE MONDE

La proportion des élections nationales qui ont été ciblées par des cybermenaces étrangères a plus que doublé depuis 2015. Comme l'indique la figure 5 ci-dessous, la proportion des élections ciblées par des cybermenaces **a plus que triplé** dans les démocraties avancées dont l'économique s'apparente à celle du Canada, comme les pays membres de l'Organisation de coopération et de développement économiques (OCDE). En fait, des cybermenaces ont ciblé le processus démocratique de la moitié de tous les pays de l'OCDE qui ont tenu des élections nationales en 2018.

FIGURE 5: Hausse des cybermenaces ciblant les processus démocratiques liés à des élections



Ces données confirment les prévisions que nous avions faites en 2017 selon lesquelles il fallait s'attendre à une hausse des cybermenaces contre les processus démocratiques à l'échelle mondiale. Dans l'Évaluation des cybermenaces nationales 2018, le CST a noté que les cyberoutils sont une solution intéressante pour les adversaires, car :

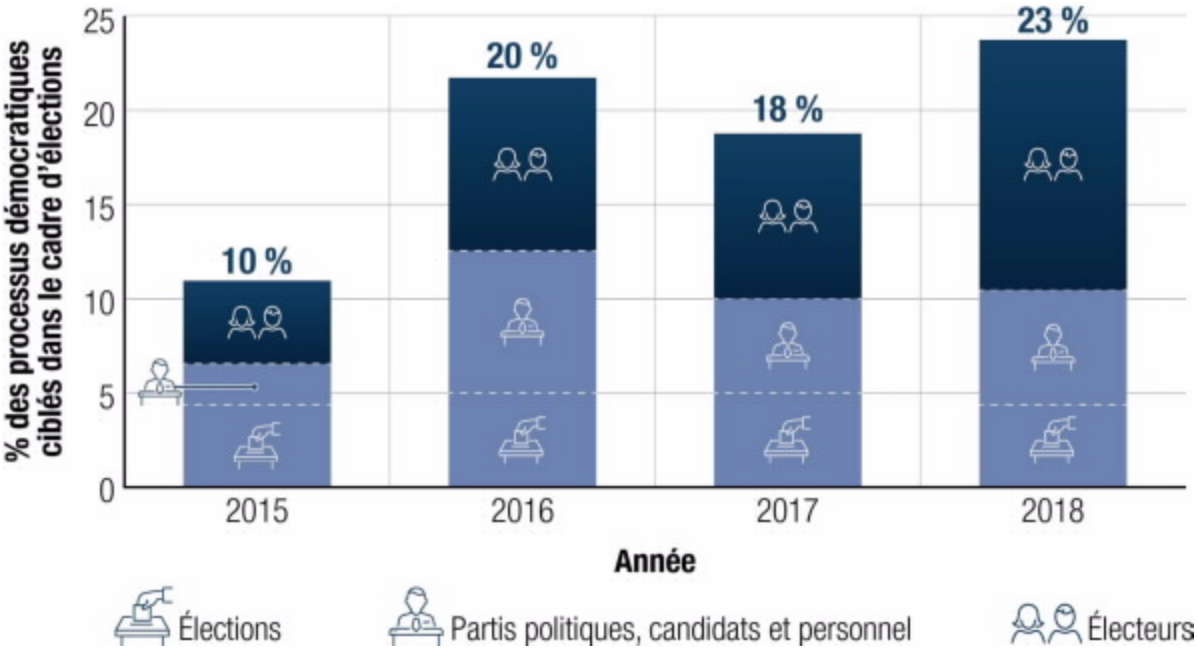
- les États-nations ont continué d'investir dans leurs cyberprogrammes;
- il est toujours difficile de prévenir les cybermenaces et de les attribuer à leurs auteurs;
- il existe une dynamique d'imitation où les cybermenaces réussies inspirent d'autres activités semblables;
- les marchés noirs de la cybercriminalité offrent des cyberoutils abordables et faciles à utiliser.

La hausse des cybermenaces a eu lieu malgré d'importantes tendances compensatoires, comme une plus grande couverture médiatique et une sensibilisation accrue du public, des pratiques de cybersécurité améliorées, l'attribution publique des cybermenaces à leurs auteurs et des mises en accusation contre ces derniers. Selon nos observations, quoique ces tendances aient probablement engendré une augmentation des coûts que doivent assumer les auteurs de cybermenace pour cibler les processus démocratiques, cette hausse n'est toujours pas suffisante pour les convaincre de renoncer à leurs activités.

TENDANCE 2 : LES CYBERMENACES CONTRE LES PROCESSUS DÉMOCRATIQUES CIBLENT DE PLUS EN PLUS LES ÉLECTEURS

La *Charte canadienne des droits et libertés* protège la liberté d'expression qui s'applique à la grande majorité de l'information diffusée en ligne. Cela dit, les adversaires étrangers ont développé des cyberoutils qui leur permettent de manipuler l'information en ligne et de mener des activités d'ingérence à grande échelle et avec précision. Ils se sont d'ailleurs servis de ces méthodes pour s'ingérer dans des processus démocratiques partout dans le monde.

FIGURE 6: Hausse des cybermenaces visant les électeurs à l'échelle mondiale



Comme l'illustre la figure 6, les électeurs, qui représentent actuellement la principale cible des cybermenaces contre les processus démocratiques, ont été visés par plus de la moitié des cybermenaces à l'échelle mondiale en 2018. Ce changement semble avoir pris naissance en 2016, probablement en raison des activités d'ingérence en ligne menées par la Russie contre les élections présidentielles de 2016 aux États-Unis, lesquelles ont été perçues comme une réussite par les auteurs de cybermenace.

La plupart des adversaires étrangers évaluent les coûts et les avantages des activités de cybermenace avant de se mettre à l'œuvre. Ils croient probablement qu'il est plus efficace ou rentable de s'ingérer dans les processus démocratiques en ciblant les électeurs que les élections ou les partis politiques, les candidats et leur personnel.

Parmi les facteurs qui contribuent fort probablement à la hausse du ciblage des électeurs, mentionnons les suivants :

- Internet, dont les médias sociaux, est l'une des principales sources d'information des électeurs[3];
- Les renseignements faux ou trompeurs, souvent diffusés au moyen de cyberoutils, sont parfois difficiles à distinguer des renseignements et des sources fiables[4], des publicités légitimes et d'autres formes de discours protégés[5];
- Les auteurs de cybermenace ont l'impression que le ciblage des électeurs entraîne peu de coûts et peu de risques.

TENDANCE 3 : LES CYBERMENACES CONTRE LES PARTIS POLITIQUES, LES CANDIDATS ET LEUR PERSONNEL PERSISTENT

Les partis politiques, les candidats et leur personnel demeurent des cibles attrayantes pour les auteurs de cybermenace à l'échelle mondiale. Ils représentent d'ailleurs un dixième des cibles des cybermenaces enregistrées contre les processus démocratiques des démocraties avancées (pays de l'OCDE) en 2018. Les auteurs de menace ciblent les partis politiques, les candidats et leur personnel de différentes façons. Ils peuvent voler des renseignements, puis les divulguer au public pour embarrasser ou discréditer un parti politique ou un candidat. Parfois, pour obtenir un effet plus spectaculaire, les auteurs de menace modifient les renseignements avant de les divulguer au public.

Les auteurs de menace peuvent également cibler les partis politiques et les candidats en menant des activités de cyberespionnage pour voler des renseignements personnels dont ils se servent ensuite pour influencer leur victime, par le chantage, la corruption ou la coercition, à agir d'une façon inhabituelle.

Des adversaires étrangers tentent parfois de dérober les bases de données d'un parti politique ou celles sur les électeurs, car ils peuvent en tirer un bon prix dans des parties illicites d'Internet où l'on achète et vend constamment de grandes quantités de renseignements nominatifs personnels. Ils peuvent voler des communications et des documents sensibles liés à une campagne pour les vendre ou les divulguer. Ils peuvent aussi utiliser des maliciels, comme des rançongiciels, pour détruire l'information d'un parti ou perturber les réseaux et les dispositifs de celui-ci.

Une nouvelle technologie a donné lieu à une menace émergente : *la permutation intelligente des visages*, qui permet de créer des vidéos de synthèse souvent impossibles à distinguer des séquences réelles. Les adversaires étrangers peuvent se servir de cette nouvelle technologie pour tenter de discréditer les candidats et d'influencer les électeurs, par exemple en créant une fausse vidéo d'un candidat donnant un discours controversé ou le montrant dans une situation embarrassante.

Les améliorations dans le domaine de l'intelligence artificielle sont susceptibles de renforcer les activités d'ingérence en plus d'en augmenter la précision et d'en améliorer le rapport coût-efficacité. Les technologies en évolution fondées sur l'intelligence artificielle, comme la permutation intelligente des visages, permettront presque certainement aux auteurs de menace de créer, avec plus de souplesse et d'efficacité, du contenu faux ou trompeur visant à influencer les électeurs, et rendront les activités d'ingérence étrangère en ligne plus difficiles à détecter et à atténuer.

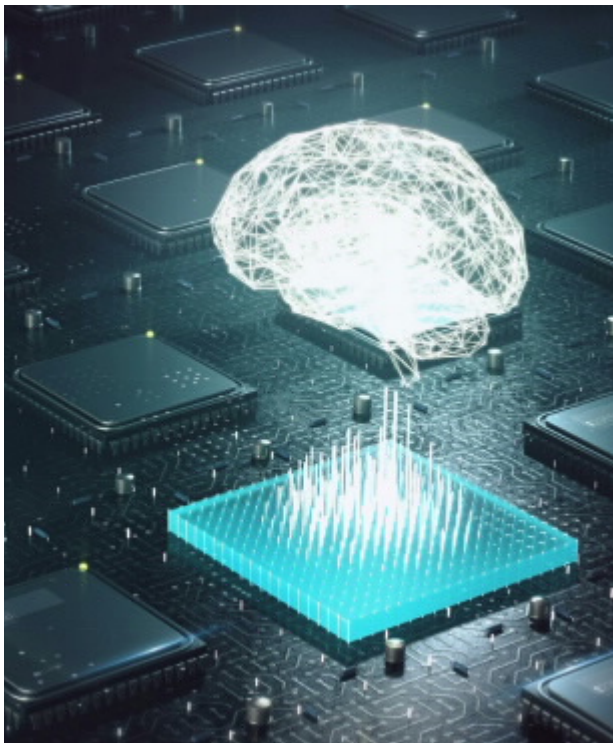


FIGURE 7 : Cybermenaces observées récemment contre les partis politiques à l'échelle mondiale

TENDANCE 4 : LES ÉLECTIONS CONTINUENT D'ÊTRE LA CIBLE DE CYBERMENACES, QUOIQU'ELLES SOIENT MOINS SOUVENT CIBLÉES QUE LES ÉLECTEURS, LES PARTIS POLITIQUES, LES CANDIDATS ET LEUR PERSONNEL

Les cybermenaces continuent de cibler les processus électoraux. Toutefois, en 2018, les élections représentaient un peu moins d'un cinquième de toutes les cibles de cybermenaces contre les processus démocratiques à l'échelle mondiale. En général, les auteurs de cybermenace pourraient tenter de perturber l'admissibilité des électeurs, le jour du scrutin, le compte et l'enregistrement des votes, et la communication des résultats au public.

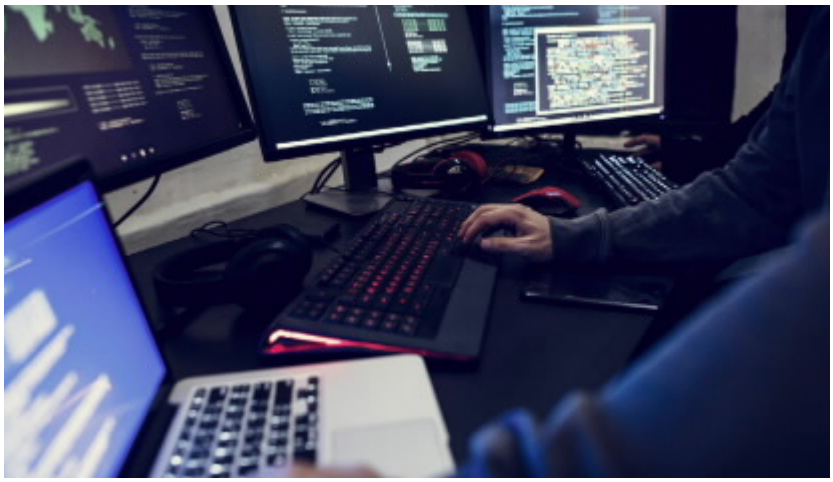
À l'heure actuelle, la cybermenace la plus courante vise les sites Web des organismes électoraux ou met en cause le vol de bases de données sur les électeurs. Dans de tels cas, les adversaires étrangers tentent généralement de semer le doute sur la validité des résultats des élections, plutôt que de modifier secrètement les résultats.

Les cybermenaces touchent très rarement les systèmes TI que les organismes électoraux utilisent pour enregistrer, stocker et transmettre les données sur les élections, comme le compte de votes. Ce type d'activité représentait moins de quatre pour cent de toutes les cybermenaces contre les élections à l'échelle mondiale en 2018. D'ailleurs, les auteurs de cybermenace estiment fort probablement qu'il est difficile de modifier le compte de votes lors d'élections nationales, voire impossible lorsqu'il s'agit de bulletins de vote papier comptés à la main, comme dans le cas des élections fédérales au Canada.

CYBERESPIONNAGE CONTRE DES PARTIS POLITIQUES EN AUSTRALIE

Un auteur de cybermenace a compromis des systèmes d'information du Parlement d'Australie et de trois grands partis politiques australiens en février 2019, alors que l'Australie tiendra des élections nationales plus tard dans l'année. Le premier ministre australien a indiqué ce qui suit : « des spécialistes en cybersécurité australiens sont d'avis qu'un auteur parrainé par un État et disposant de moyens sophistiqués est responsable de cette activité malveillante. » Cette situation fait ressortir le fait que l'information liée aux institutions démocratiques, dont les partis politiques, constitue une cible attrayante pour les auteurs de cybermenace parrainés par des États dans une année électorale.[6]

LE CONTEXTE CANADIEN



L'INFLUENCE ET L'INGÉRENCE ÉTRANGÈRES EN DEHORS DES PÉRIODES D'ÉLECTIONS

Depuis les élections fédérales de 2015, les dirigeants politiques et le public canadiens ont été ciblés par des activités d'ingérence étrangère. Par exemple :

- plus d'un adversaire étranger a manipulé les médias sociaux au moyen de cyberoutils pour propager sur Twitter des renseignements faux ou trompeurs sur le Canada, tout probablement pour créer un clivage entre les Canadiens ou miner les objectifs du Canada en matière de politique étrangère;
- des médias parrainés par des États étrangers ont déprécié des ministres du cabinet du Canada[7];
- un adversaire étranger a manipulé de l'information sur les médias sociaux pour amplifier et promouvoir des points de vue qui critiquent grandement des lois du gouvernement du Canada imposant des sanctions et interdisant l'entrée au pays de représentants de gouvernements étrangers accusés d'avoir violé les droits de la personne[8].

TECHNIQUES EMPLOYÉES PAR LES ADVERSAIRES ÉTRANGERS POUR MENER DES ACTIVITÉS D'INGÉRENCE SUR TWITTER

Des adversaires étrangers s'approprient les comptes d'autres utilisateurs ou créent des identités fictives sur Twitter auxquelles ils associent de nouveaux comptes qui publient des gazouillis sur des sujets populaires ou controversés dans le but d'attirer des abonnés et d'établir leur crédibilité pour ainsi diffuser à un plus vaste public des renseignements faux et trompeurs et d'autres contenus visant à influencer l'opinion. Ces comptes semblent ordinaires et acquièrent généralement des amis et des abonnés en diffusant de l'information sur les sports ou les divertissements. Ils changent cependant de cap en envoyant des messages politiques sur des thèmes canadiens après la tenue d'événements internationaux auxquels participe le Canada.

PRÉVISIONS D'ACTIVITÉS D'INGÉRENCE ÉTRANGÈRE PENDANT LES ÉLECTIONS DE 2019

Nous estimons que, s'ils sont motivés par un objectif stratégique, un nombre croissant d'adversaires étrangers possèdent les cyberoutils, la capacité organisationnelle et une compréhension suffisante du paysage politique canadien pour mener des activités d'ingérence en ligne contre les électeurs canadiens au cours des élections fédérales de 2019.

Toutefois, même si un adversaire étranger cherche à s'ingérer dans le processus démocratique du Canada pour atteindre un objectif stratégique, nous considérons qu'il est actuellement improbable que des activités d'ingérence étrangère en ligne de l'ampleur de celles que la Russie a menées contre les élections présidentielles américaines en 2016 visent le Canada en 2019. Néanmoins, selon nos observations, il est très probable que les électeurs canadiens feront face à une forme quelconque d'activités d'ingérence étrangère en ligne avant et pendant les élections fédérales de 2019.

FAUX REPORTAGES SUR LES TROUPES CANADIENNES

En 2016, de faux renseignements sont apparus dans les médias sociaux sur « l'échec d'un raid canadien » contre les positions séparatistes russes en Ukraine, qui aurait entraîné la mort de 11 militaires canadiens. Les utilisateurs ont diffusé une version anglaise de ce reportage fictif plus de 3 000 fois sur Facebook. En mai 2018, un faux reportage semblable sur la mort de trois soldats canadiens, dont le véhicule aurait frappé une mine terrestre en Ukraine, avait circulé sur des sites Web sympathiques à la Russie[9]. Les auteurs de ces faux reportages tentaient probablement de donner l'impression que les troupes canadiennes – qui occupent des postes de non-combattants en Ukraine – sont imprudentes et leurs opérations inefficaces.

Selon nos observations, il est très probable que les activités d'ingérence étrangère en ligne contre le Canada s'apparenteront aux campagnes d'ingérence qui ont été menées en ligne contre d'autres démocraties avancées au cours des dernières années. Au moyen de cyberoutils ou de plateformes de médias sociaux, des adversaires étrangers ont tenté d'influencer les idées et les décisions des électeurs en cherchant avant tout à diviser l'opinion sur des enjeux politiques et sociaux, à promouvoir la popularité d'un parti en particulier ou à influencer les déclarations publiques d'un candidat et ses choix en matière de politiques.

Au Canada, les élections fédérales se déroulent sur support papier et Élections Canada a d'ailleurs mis en place de nombreuses mesures juridiques, procédurales et liées aux TI qui offrent une protection très robuste contre les auteurs de menace qui tentent de modifier secrètement le compte de votes officiel.

Toutefois, il est probable que des adversaires tenteront de défigurer un site Web ou de voler des renseignements personnels dont ils pourraient se servir pour faire de la désinformation auprès des Canadiens dans le but de troubler ou de perturber le processus électoral. De telles activités viseraient à semer le doute dans l'esprit des électeurs au sujet de la légitimité des élections. Elles pourraient même carrément dissuader certains électeurs à participer au processus démocratique.

INTERNET RESEARCH AGENCY

L'Internet Research Agency (IRA) de la Russie continue de créer des sites Web illégitimes pour y afficher des renseignements faux et trompeurs qu'il fait passer pour des blogues personnels ou du journalisme électronique indépendant. Des comptes de réseaux de zombies unissent leurs efforts pour diffuser et promouvoir automatiquement l'information (souvent le titre d'un nouvel article contenant un hyperlien) sur diverses plateformes de médias sociaux. Ces renseignements faux et trompeurs, qui font l'objet d'une promotion secrète, se retrouvent dans les fils d'actualité d'utilisateurs véritables dont la plupart en ignorent probablement l'origine malveillante et l'intention trompeuse. Au moyen de comptes inventés ou de réseaux de zombies, des employés de l'IRA entrent en contact avec des utilisateurs véritables pour défendre l'authenticité de l'information.

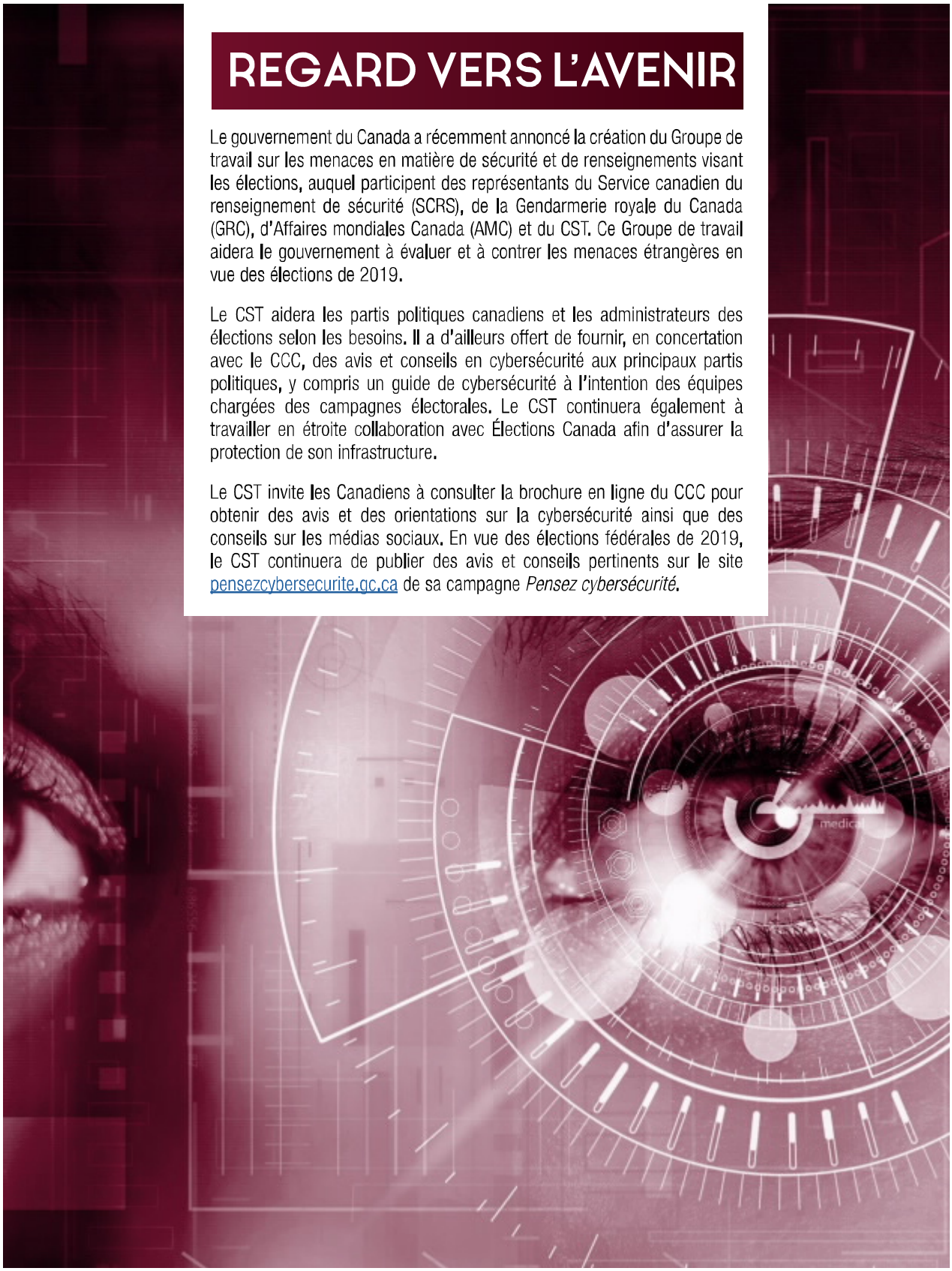
Le site Web ReportSecret.com lié à l'IRA a automatiquement diffusé et amplifié illicitement des articles sur des thèmes canadiens dans Twitter. Une campagne, menée en septembre 2017, a tenté de provoquer au Canada les mêmes dissensions politiques qui touchent la ligue nationale de football des États-Unis en faisant la promotion de titres d'articles comme « La Ligne canadienne de football proteste contre SON PROPRE hymne national! » et « Les joueurs canadiens de la LNH ENVISAGENT de s'agenouiller pendant l'hymne national des États-Unis ».

REGARD VERS L'AVENIR

Le gouvernement du Canada a récemment annoncé la création du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections, auquel participent des représentants du Service canadien du renseignement de sécurité (SCRS), de la Gendarmerie royale du Canada (GRC), d'Affaires mondiales Canada (AMC) et du CST. Ce Groupe de travail aidera le gouvernement à évaluer et à contrer les menaces étrangères en vue des élections de 2019.

Le CST aidera les partis politiques canadiens et les administrateurs des élections selon les besoins. Il a d'ailleurs offert de fournir, en concertation avec le CCC, des avis et conseils en cybersécurité aux principaux partis politiques, y compris un guide de cybersécurité à l'intention des équipes chargées des campagnes électorales. Le CST continuera également à travailler en étroite collaboration avec Élections Canada afin d'assurer la protection de son infrastructure.

Le CST invite les Canadiens à consulter la brochure en ligne du CCC pour obtenir des avis et des orientations sur la cybersécurité ainsi que des conseils sur les médias sociaux. En vue des élections fédérales de 2019, le CST continuera de publier des avis et conseils pertinents sur le site pensezcybersecurite.gc.ca de sa campagne *Pensez cybersécurité*.



NOTES EN FIN D'OUVRAGE

1. La plupart des Canadiens lisent les actualités en ligne quotidiennement, mais les consultent aussi à partir d'autres sources, comme la télévision, la radio et les journaux imprimés, Reuters Institute for the Study of Journalism, 2018 (consulté en février 2019), et Pew Research Center, 11 janvier 2018 (consulté en février 2019)

2. Autorité canadienne pour les enregistrements Internet, 22 mars 2018 (consulté en février 2019)

3. Pew Research Center, Newspapers Fact Sheet, 13 juin 2018 (consulté en janvier 2019), et Reuters Institute for the Study of Journalism, 2018 (consulté en février 2019)

4. Autorité canadienne pour les enregistrements Internet, 22 mars 2018 (consulté en février 2019)

5. Rosenbach, Eric et Katherine Manfred, Belfer Center for Science and International Affairs, Harvard Kennedy School, octobre 2018 (consulté en février 2019)

6. Worthington, Brett. ABC News. 17 février 2019. Consulté en février 2019; et Tarabay, Jamie. The New York Times. 18 février 2019 (consulté en février 2019)

7. Fisher, Matthew, National Post, 14 mai 2017 (consulté en février 2019)

8. Atlantic Council Digital Forensic Research Lab, Medium, 19 octobre 2017 (consulté en février 2019)

9. Ling, Justin, The Walrus, 22 novembre 2018 (consulté en février 2019)