ISSN 2564-1395
CAT D95-10F-PDF

CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA

MISE À JOUR DE JUILLET 2021

Centre de la sécurité des télécommunications
Communications Security Establishment

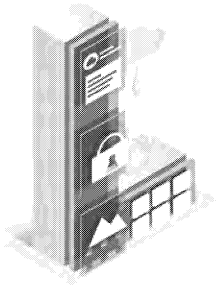
Canada

Centre de la sécurité des télécommunications
1929, chemin Ogilvie
Ottawa, ON K1J 8K6
cse-cst.gc.ca

ISSN 2564-1395
CAT D95-10F-PDF

L'évaluation *Cybermenaces contre le processus démocratique du Canada* est un document ponctuel publié environ aux deux ans.

À PROPOS DU CST



LE Centre de la sécurité des télécommunications (CST) est le centre canadien d'excellence en matière de cyberopérations. Le CST est l'un des principaux organismes de sécurité et de renseignement du Canada. Il 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 fédéraux chargés de l'application de la loi et de la sécurité dans leurs activités légalement autorisées lorsqu'ils requièrent l'expertise technique unique du CST.

En outre, le CST protège les réseaux informatiques et l'information électronique 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. Les activités de renseignement électromagnétique étranger du CST appuient les processus décisionnels du gouvernement en matière d'affaires internationales, de défense et de sécurité, car elles permettent aux décisionnaires de mieux comprendre les crises et événements mondiaux et de promouvoir les intérêts du Canada dans le monde.

Relevant du CST, le Centre canadien pour la cybersécurité (CCC) embauche des spécialistes de la cybersécurité dignes de confiance et s'est vu confier un mandat précis et axé sur la collaboration avec le gouvernement, le secteur privé et le milieu universitaire afin d'assurer la sécurité du Canada en ligne.

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

SOMMAIRE

ES auteurs de cybermenace continuent de s'en prendre aux processus démocratiques de partout dans le monde. La présente évaluation se penchera sur les tendances mondiales entourant les cybermenaces contre les processus démocratiques (qui comprennent les électeurs, les partis politiques et les élections) et examinera la menace qui pèse sur le Canada, particulièrement les répercussions de la pandémie de COVID-19.

PRINCIPALES CONCLUSIONS

TENDANCES MONDIALES

- Les processus démocratiques restent une cible populaire. Après avoir connu une hausse de 2015 à 2017, la proportion des processus ciblés par des auteurs de cybermenace est restée relativement stable depuis 2017.
- Nous estimons que la grande majorité des cybermenaces ayant touché des processus démocratiques de 2015 à 2020 peuvent être attribuées à des auteurs de cybermenace parrainés par des États. Ces derniers ciblent des processus démocratiques pour servir leurs objectifs stratégiques (c'est-à-dire des objectifs politiques, économiques et géopolitiques).
- La Russie, la Chine et l'Iran sont fort probablement responsables de la plupart des activités de cybermenace parrainées par des États et menées contre des processus démocratiques partout dans le monde.
- Souvent, les auteurs de cybermenace ciblent une combinaison d'électeurs, de partis politiques et d'infrastructures électorales. Nous estimons que les auteurs de cybermenace perçoivent probablement qu'il est plus efficace de diriger leurs efforts sur plusieurs cibles liées à un processus démocratique que de se concentrer que sur un seul groupe.
- De 2015 à 2020, les cybermenaces visaient plus souvent les électeurs que les partis politiques et les élections, tant les activités d'influence étrangère en ligne que les activités de cybermenace plus traditionnelles comme le vol d'information ou le déni d'accès à des sites Web importants. D'après nous, les auteurs de cybermenace estiment probablement que le ciblage des électeurs est une façon efficace et relativement facile de s'ingérer dans les processus démocratiques.
- Nous sommes d'avis que les changements apportés aux processus démocratiques partout dans le monde en raison de la pandémie de COVID-19, comme le transfert d'une partie du processus en ligne ou l'intégration de nouvelles technologies au scrutin, augmentent presque assurément l'exposition des processus démocratiques aux cybermenaces. Plus important encore, les auteurs de cybermenace peuvent exploiter et amplifier les faussetés sur la pandémie de COVID-19 pour miner la confiance dans les élections.

CONSÉQUENCES POUR LE CANADA

- Nous sommes d'avis que comparativement à ceux d'autres pays, le processus démocratique du Canada n'est pas une cible prioritaire pour les auteurs de cybermenace parrainés par des États. Toutefois, nous croyons que l'électorat canadien devra fort probablement composer avec une forme quelconque d'ingérence étrangère en ligne (par exemple des activités de cybermenace par des auteurs étrangers ou de l'influence étrangère en ligne) avant ou pendant la prochaine élection fédérale. Il est peu probable que cette ingérence soit de l'ampleur de celle vécue aux États-Unis.
- Si l'élection fédérale devait avoir lieu pendant la pandémie, Élections Canada a dressé un plan pour protéger la santé et la sécurité de tous les participants au processus électoral. Toute modification au processus électoral peut entraîner une hausse de la cybermenace, mais nous estimons que les modifications prévues n'occasionneront pas une intensification considérable de la cybermenace qui pèse sur le processus démocratique du Canada.

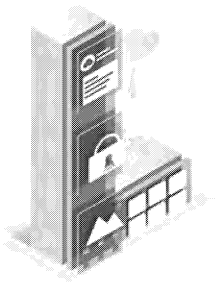
TABLE DES MATIÈRES

LISTE DES FIGURES

PORTÉE

Le présent rapport traite des cybermenaces qui touchent le processus démocratique, composé des électeurs, des partis politiques et des élections. Une cybermenace est une activité menée au moyen de cyberoutils (comme des maliciels ou des courriels de harponnage) et 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. Ce type d'activité est mené par des auteurs parrainés par des États, des cybercriminels, des hacktivistes, des personnes ayant des motivations politiques et des amateurs de sensations fortes. L'Internet est truffé d'information fausse et trompeuse, mais la présente évaluation se penche principalement sur les **activités d'influence étrangère en ligne** ciblant les électeurs. Ce genre d'activité d'influence se produit lorsque des auteurs de menace étrangers manipulent secrètement l'information diffusée en ligne, souvent au moyen de cyberoutils, pour influencer l'opinion et le comportement des électeurs. Nous définissons l'ingérence étrangère comme une activité secrète, trompeuse ou coercitive menée par un auteur étranger contre un processus démocratique pour servir des objectifs stratégiques. L'**ingérence étrangère** en ligne comprend à la fois les cybermenaces menées par des auteurs étrangers et des activités d'influence étrangère en ligne. Ces définitions sont propres à notre contexte des cybermenaces contre le processus démocratique du Canada; des expressions semblables peuvent être employées différemment par d'autres établissements fédéraux canadiens.

À PROPOS DU PRÉSENT DOCUMENT



Le présent document est une mise à jour des rapports du CST *Cybermenaces contre le processus démocratique du Canada* de 2017 et *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019*. Il vise à informer les Canadiens et Canadiennes des cybermenaces qui pèsent sur le processus démocratique.

SOURCES

Les propos formulés dans le présent document sont fondés sur des sources classifiées et non classifiées. Le volet du mandat du CST touchant le renseignement étranger procure à l'organisme de précieuses informations sur le comportement des adversaires. Le fait de défendre les systèmes d'information du gouvernement du Canada place le CST dans une position unique pour observer l'évolution du contexte des cybermenaces.

RESTRICTIONS

Le présent document traite d'une panoplie de cybermenaces qui pèsent sur les activités politiques et électorales à l'échelle nationale et internationale et repose sur l'information à laquelle nous avions accès. La prestation de conseils sur l'atténuation des menaces ne s'inscrit pas dans la portée du présent rapport.

INFORMATION SUPPLÉMENTAIRE

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 2020* (ECN 2020) et l'*Introduction à l'environnement de cybermenaces*.

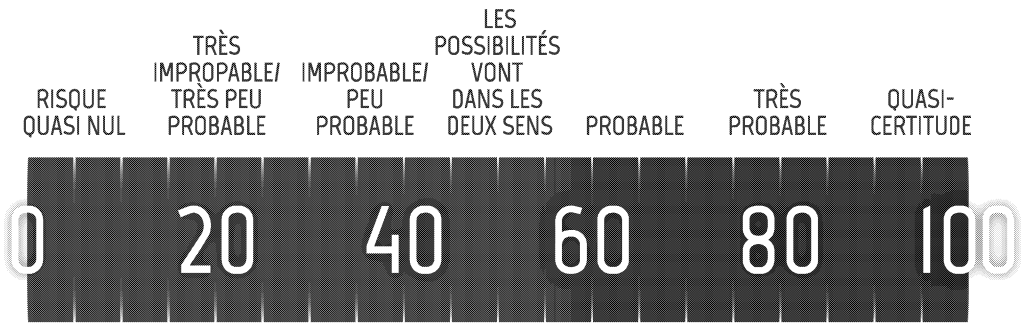
Le CCC offre une foule d'autres ressources en ligne, dont *Pensez cybersécurité*, *Ne mordez pas à l'hameçon : Reconnaître et prévenir les attaques par hameçonnage* et *Pratiques exemplaires en cybersécurité*.

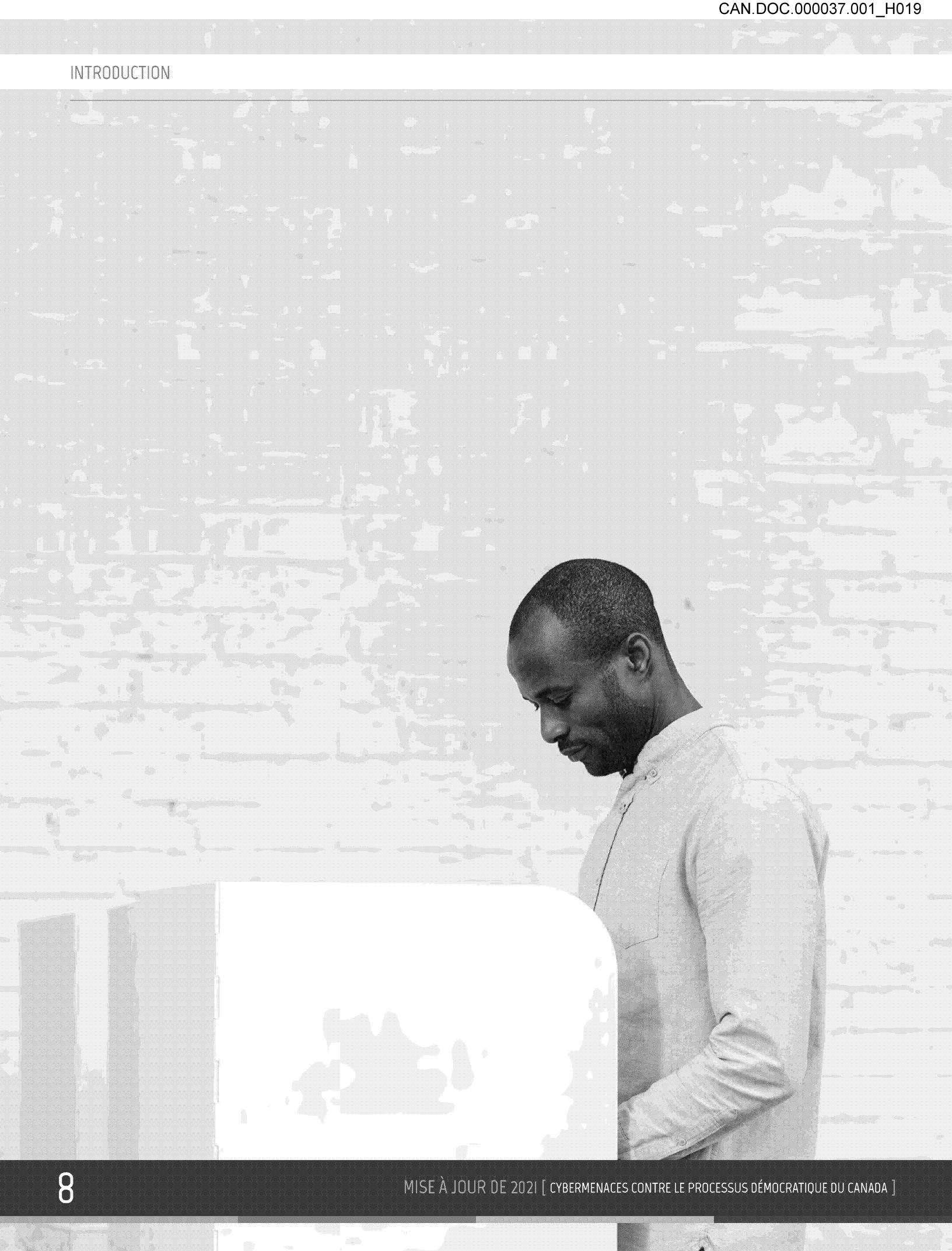
LEXIQUE DES ESTIMATIONS

Nos principaux jugements sont basés sur un processus d'analyse qui comprend l'évaluation de la qualité de l'information disponible, l'étude d'autres explications possibles, la réduction de biais et l'utilisation d'un langage probabiliste. On emploiera des termes tels que « on considère que » ou « selon nos observations » pour communiquer les évaluations analytiques. On utilisera des qualificatifs comme « possiblement », « probable » et « très probable » pour exprimer les probabilités.

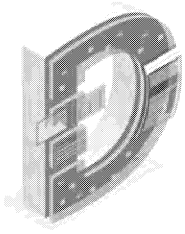
Le présent document est basé sur des renseignements disponibles en date du 12 juillet 2021.

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.





INTRODUCTION



ANS le monde entier, les processus démocratiques continuent de subir les contrecoups de cybermenaces. Un processus démocratique se compose de participants, comme les électeurs et les partis politiques, et d'événements, comme les élections. Les activités de cybermenace sont menées contre ces participants et ces événements par des auteurs parrainés par des États, des cybercriminels, des auteurs ayant des motivations politiques, des hacktivistes et des amateurs de sensations fortes. Nous avons pu observer à quel point les tactiques utilisées par ces auteurs de menace ont évolué au fil du temps, alors que ceux-ci s'adaptent aux nouvelles occasions et aux nouveaux outils qui leur permettent d'ébranler plus facilement le processus démocratique.

Le fait de s'attaquer aux processus demeure en grande partie une activité stratégique. Les auteurs de cybermenace parrainés par des États ayant des liens avec la Russie, la Chine et l'Iran sont ceux, d'après les observations, qui ont dirigé le plus grand nombre d'activités de cybermenace à l'endroit des processus démographiques à travers le monde.

La pandémie de COVID-19 a entraîné d'importants changements relatifs au fonctionnement des processus démocratiques dans le monde, y compris au Canada. Dans plusieurs pays, les campagnes électorales des partis politiques et de leurs candidats se font presque exclusivement en ligne. Les employés des organismes chargés des élections ont été contraints de planifier et de se préparer pour les élections en travaillant de la maison. Le déroulement du vote a dû également être adapté pour assurer la santé des électeurs et du personnel des bureaux de scrutin et pour veiller à ce que tous les membres admissibles de la société puissent voter en toute sécurité. Malgré tout, on considère que les changements aux procédures électorales liés à la COVID-19 ont eu très peu de répercussions sur les cybermenaces observées à l'endroit des élections.

Toutefois, ces mêmes changements, dont la popularité croissante du vote par la poste ou les retards de diffusion des résultats, ont entraîné la propagation de faussetés et de théories du complot qui remettent en question la légitimité du résultat du vote. Tout cela se produit à un moment où l'écosystème informationnel en ligne est déjà truffé de contenus mensongers et trompeurs. Des auteurs, qui se trouvent au pays ou à l'étranger, créent et partagent de fausses allégations pour en tirer des avantages politiques ou géopolitiques ou encore pour manipuler ou nuire à un public cible ou à la société. D'autres partagent ces contenus parce qu'ils pensent qu'ils sont vrais. Il devient de plus en plus difficile de déterminer qui partage la fausse information et pourquoi. Dans un tel contexte, il est plus facile pour les auteurs étrangers hostiles d'effectuer des activités d'influence en ligne, d'alimenter les divisions au sein de la société et de miner la confiance dans les institutions démocratiques.

Les auteurs de menace ont de nombreuses occasions de s'en prendre aux processus démocratiques, mais il est important de souligner les progrès importants accomplis ces dernières années pour protéger la démocratie à travers le monde, entre autres les efforts déployés par les gouvernements, des organisations non gouvernementales, des organismes de recherche, la société civile, les médias traditionnels, les médias sociaux et des entreprises spécialisées dans la technologie afin d'améliorer les pratiques de cybersécurité, de sensibiliser et d'intervenir rapidement en cas d'incidents. Par exemple, le Canada a mis en œuvre une vaste gamme de mesures, y compris des dispositions législatives (p. ex. la *Loi sur la modernisation des élections*), des accords avec des entreprises de médias sociaux, ainsi que plusieurs initiatives permettant d'améliorer les mécanismes de communication et de partage de l'information entre Élections Canada, les organismes canadiens de la sécurité et du renseignement, d'autres ministères, les partis politiques et les électeurs.

Dans la présente évaluation, nous examinons les cybermenaces qui sont dirigées contre les processus démocratiques à travers le monde et analysons ce que cela implique pour le Canada, en apportant une attention spéciale aux impacts de la COVID-19. Nous décrivons d'abord la raison pour laquelle le Canada pourrait devenir la cible d'un adversaire. Nous discutons des conséquences possibles d'une cyberactivité contre les processus démocratiques, et nous donnons un aperçu des impacts de la pandémie de COVID-19 sur cette menace. Par la suite, nous décrivons plus en détail les cybermenaces qui planent sur les électeurs, les partis politiques et les élections à travers le monde. Enfin, nous discutons des tendances mondiales relatives aux cyberactivités menées contre les processus démocratiques et ce que cela signifie concrètement dans le contexte canadien.

POURQUOI CIBLER LE PROCESSUS DÉMOCRATIQUE DU CANADA?

LE CANADA DANS LE MONDE

Le Canada joue un rôle actif au sein de la communauté internationale en participant à d'importants forums multilatéraux, notamment l'Organisation du Traité de l'Atlantique Nord (OTAN), l'Organisation de coopération et de développement économiques (OCDE), le Groupe des 20 (G20) et le Groupe des 7 (G7).[1] Les choix du gouvernement du Canada en matière de politique étrangère, de déploiements militaires, d'accords commerciaux et d'investissements, de relations diplomatiques, d'aide internationale ou de politique sur l'immigration intéressent les autres États. La position du Canada sur une question peut avoir une influence sur les intérêts fondamentaux d'autres pays, de groupes étrangers et de particuliers. Des auteurs de menace pourraient utiliser des cyberoutils pour cibler le processus démocratique du Canada dans le but de modifier les résultats des élections, d'influencer les choix des décideurs 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 LES AUTEURS DE MENACE

Selon les dernières estimations, environ 94 % des Canadiens utilisaient Internet en 2021.[2] La grande majorité des Canadiens utilisent les services des grandes sociétés Internet, comme Facebook ou Google, pour obtenir de l'information, communiquer entre eux et bâtir des communautés. Lorsque les Canadiens communiquent ensemble et accèdent à de l'information en ligne, ils s'exposent aux auteurs de cybermenace et aux outils que ceux-ci utilisent pour s'immiscer dans le processus démocratique. Les auteurs de menace qui veulent perturber ce processus peuvent tirer profit non seulement des Canadiens vivant dans une société toujours plus branchée, mais aussi des services en ligne qu'ils utilisent régulièrement. Les cybercriminels qui essaient de faire de l'argent et les amateurs de sensations fortes qui cherchent à relever un défi ou à obtenir de la notoriété peuvent aussi cibler les processus démocratiques du Canada. Bien que ces activités n'aient pas une orientation stratégique, elles ont quand même une incidence sur le fonctionnement des processus démocratiques et la perception des électeurs en ce qui a trait à la sécurité, à la légitimité et à l'impartialité des résultats.

DES CYBEROUTILS ET DES SERVICES AMÉLIORÉS À LA PORTÉE DES AUTEURS DE MENACE

Dans l'*ECN 2020*, nous avons observé que le développement des marchés commerciaux pour les cyberoutils et les talents a permis de réduire le temps nécessaire aux États pour établir des cybercapacités et d'augmenter le nombre d'États qui se sont dotés de cyberprogrammes. Alors que de plus en plus d'États ont accès à des cyberoutils, ceux qui voulaient cibler les processus démocratiques sans disposer des capacités nécessaires pour le faire peuvent maintenant entreprendre ce type de cyberactivité plus facilement. La prolifération de cyberprogrammes soutenus par les États rend les choses plus difficiles lorsque vient le moment de repérer les activités de cybermenace, de les attribuer à leurs auteurs et de se défendre contre celles-ci de façon plus générale.

À cela s'ajoute un vaste marché illicite offrant des outils et des services qui permettent aux cybercriminels de réduire considérablement leur temps de préparation et de mener des activités plus complexes et sophistiquées.[A] De nombreux marchés en ligne permettent aux marchands de vendre des cyberoutils et des services spécialisés à des acheteurs qui s'en servent à des fins de cybercriminalité, comme la défiguration de sites Web, le cyberespionnage, les attaques par déni de service distribué (DDoS) et les attaques par rançongiciel.[B] N'importe lequel de ces outils peut être utilisé contre des processus démocratiques pour obtenir un gain financier, envoyer un message politique ou essayer d'influencer une élection.

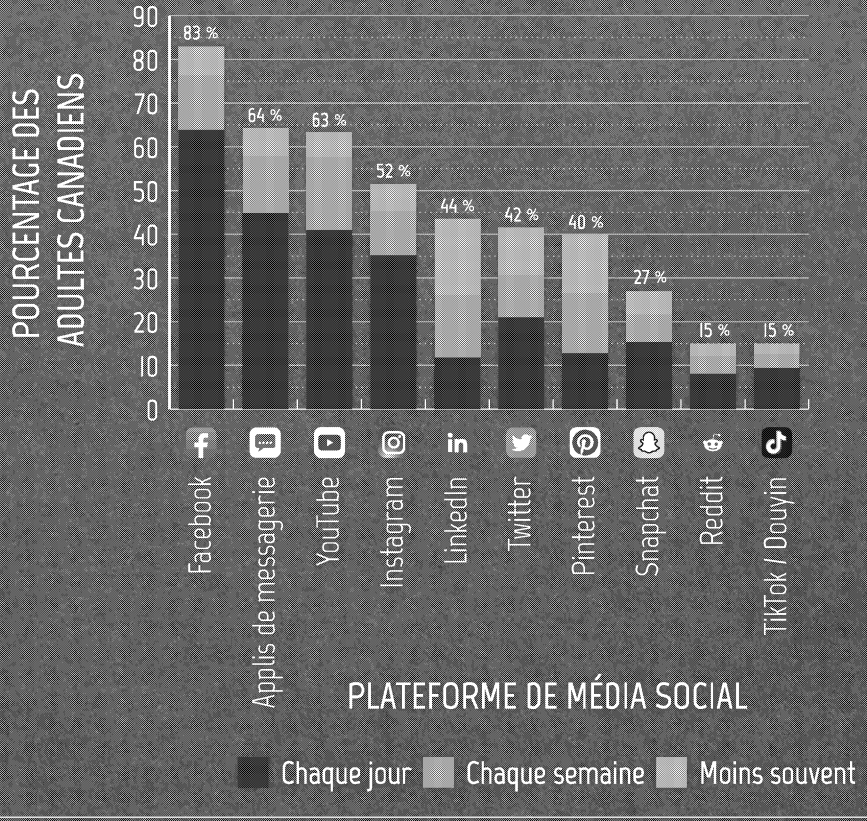
HYPERTRUCAGE : AU-DELÀ DES IMAGES ET DE LA VIDÉO

Cette technologie en évolution, fondée sur l'intelligence artificielle (IA) et utilisée par des auteurs de cybermenace pour créer du contenu en ligne faux ou trompeur, est devenue bon marché et facile d'accès.[3] L'*ECN 2020* traitait des vidéos synthétisées par hypertrucage et expliquait comment l'utilisation de ce procédé permettait de créer des vidéos synthétiques d'événements ou de personnalités publiques ayant l'air vraies. Alors que des entreprises spécialisées dans la technologie ont investi des ressources pour faire progresser la détection automatique de vidéos hypertruquées, d'autres personnes ont mis au point d'autres formes de supports générés par IA en évolution rapide plus difficiles à détecter, comme l'écriture générée par IA (p. ex. le texte hypertruqué) et le son hypertruqué.[4] Les auteurs de menace peuvent utiliser le texte hypertruqué pour s'immiscer dans le processus électoral, notamment en ciblant les électeurs au moyen de la désinformation, en recourant à l'hameçonnage contre les candidats et leur personnel et en faisant une mauvaise utilisation des processus gouvernementaux en ligne.[5] Le texte hypertruqué passe maintenant le plus souvent inaperçu chez les humains. En effet, dans le cadre d'une étude réalisée en 2019, on a demandé à des individus de classer des commentaires selon qu'ils provenaient d'un humain ou d'un robot; les résultats du classement n'étaient pas meilleurs que si les commentaires avaient été divisés au hasard.[6] Les auteurs de menace peuvent aussi cibler les électeurs au moyen de matériel audio généré par IA qui imite la tonalité, l'accentuation et les idiosyncrasies des candidats ou du personnel des bureaux de scrutin.

A Pour obtenir de plus amples renseignements sur ces tendances, consultez l'*ECN 2020* du CST.

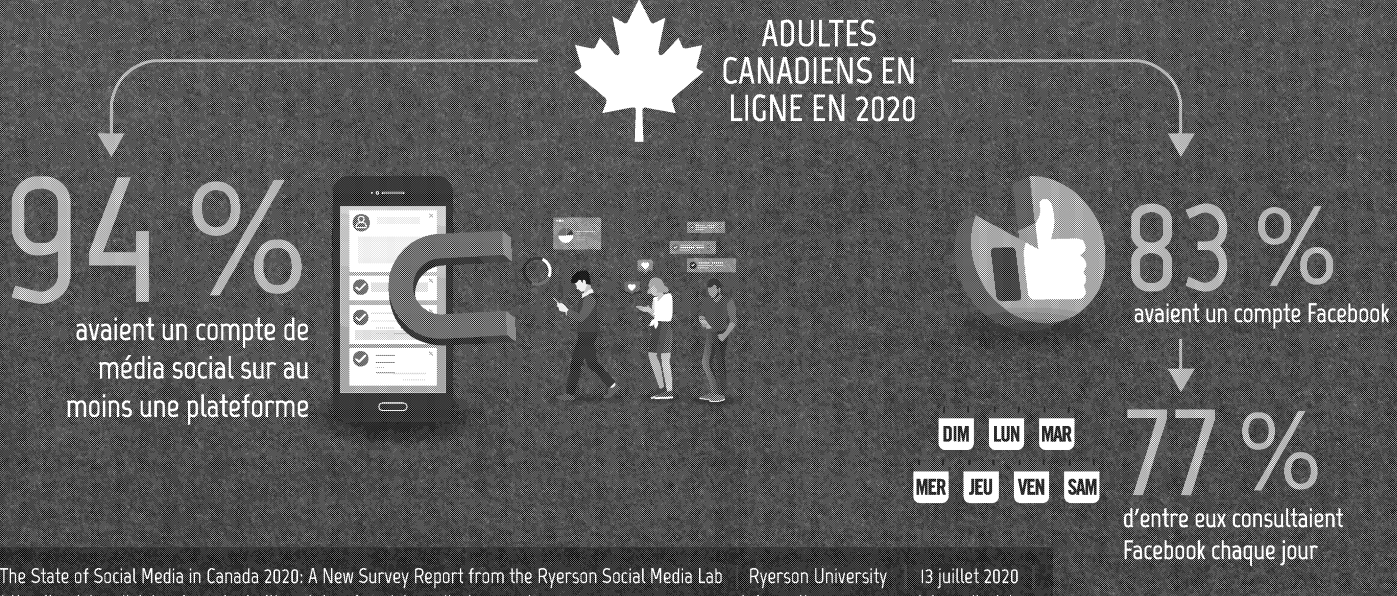
B Pour connaître la définition de ces tactiques et cyberoutils courants et d'autres, consultez l'*Introduction à l'environnement de cybermenaces* du CST.

FIGURE 01 | FRÉQUENCE D'UTILISATION DES MÉDIAS SOCIAUX PAR DES ADULTES EN 2020



Google détenait toujours 91,83 % du marché des moteurs de recherche au Canada en janvier 2021.*

* Search Engine Market Share Canada Global Stats consulté en février 2021 https://gs.statcounter.com/search-engine-market-share/all/canada



The State of Social Media in Canada 2020: A New Survey Report from the Ryerson Social Media Lab Ryerson University 13 juillet 2020
https://socialmedialab.ca/2020/07/13/the-state-of-social-media-in-canada-2020-a-new-survey-report-from-the-ryerson-social-media-lab

EFFETS DES CYBERACTIVITÉS MENÉES CONTRE LES PROCESSUS DÉMOCRATIQUES

Les activités de cybermenace menées contre les processus démocratiques à travers le monde peuvent avoir des effets à court, à moyen et à long termes. Dans certains cas, la perception d'une activité de cybermenace réussie contre les processus démocratiques pourrait miner la confiance du public dans les institutions démocratiques, et ce, même si la cyberactivité ne s'est jamais concrétisée ou n'a eu aucune conséquence sérieuse. Par exemple, l'appareil du renseignement des États-Unis a constaté que durant l'élection présidentielle américaine de 2020, certains auteurs étrangers ont diffusé de fausses allégations ou ont multiplié des allégations concernant de présumées compromissions de modes de scrutin pour miner la confiance dans le processus électoral et mettre en doute les résultats.[7] De nombreuses allégations de fraude électorale ont ébranlé cette élection et ont persisté même après avoir été démenties.[8] Ces allégations ont fragilisé, de façon durable, la confiance dans les processus démocratiques aux États-Unis.[9]

Lorsqu'une activité de cybermenace contre des partis politiques ou l'infrastructure des élections est combinée à des activités d'influence étrangère en ligne, les impacts qui en découlent peuvent être plus importants. Par exemple, les auteurs de cybermenace peuvent voler des renseignements sensibles concernant un candidat et diffuser ces renseignements dans les médias sociaux pour faire baisser la cote de popularité de ce candidat.

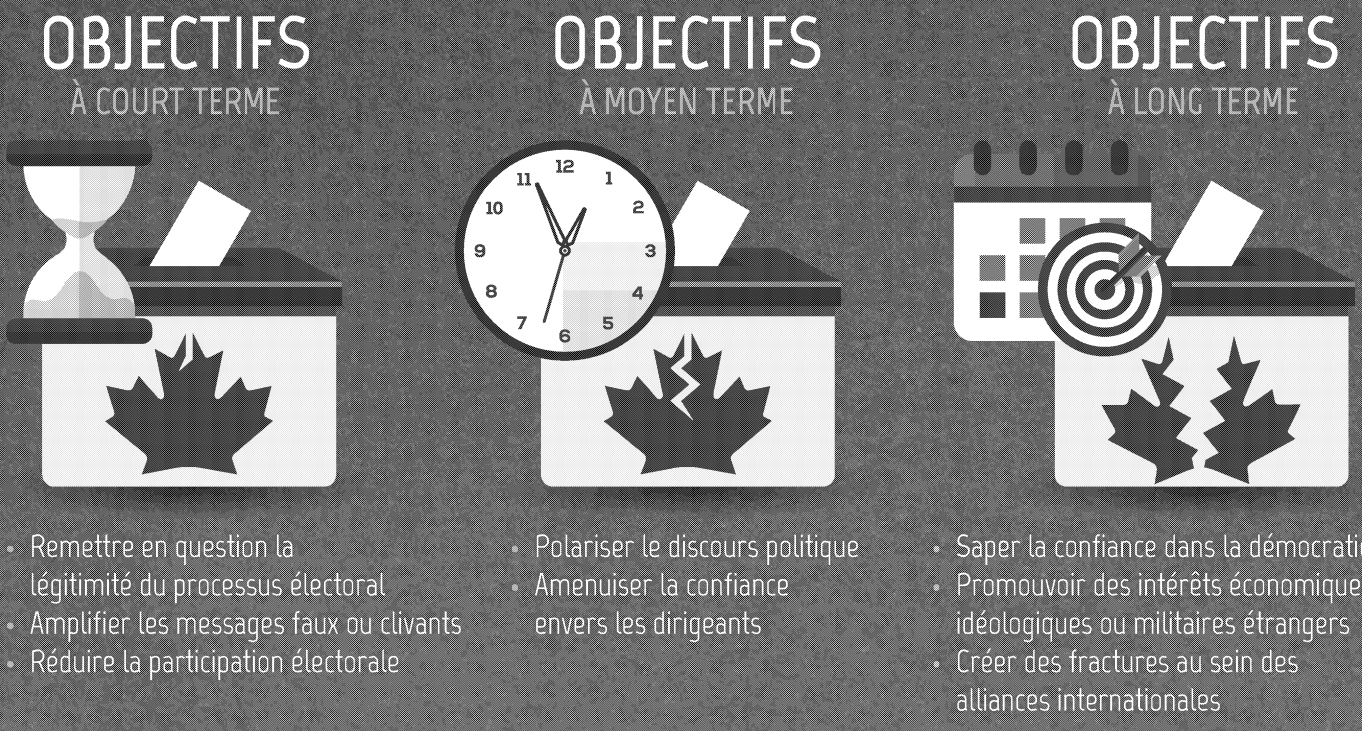
À court terme, les cybermenaces peuvent notamment avoir les conséquences suivantes :

- mettre en évidence un message faux ou clivant;
- dissimuler l'information légitime;
- nuire à la popularité ou au soutien des candidats;
- semer le doute sur la légitimité du processus électoral et les résultats;
- favoriser les résultats désirés pour les élections;
- détourner l'attention des électeurs des enjeux importants;
- limiter la participation électorale.

Les conséquences à moyen et à long termes sont les suivantes :

- saper la confiance du public envers le processus démocratique;
- diminuer la confiance envers le journalisme et les médias;
- créer des fractures au sein des alliances internationales;
- augmenter la division et diminuer la cohésion sociale;
- amenuiser la confiance envers les dirigeants;
- promouvoir les intérêts économiques, géopolitiques ou idéologiques d'États étrangers hostiles.

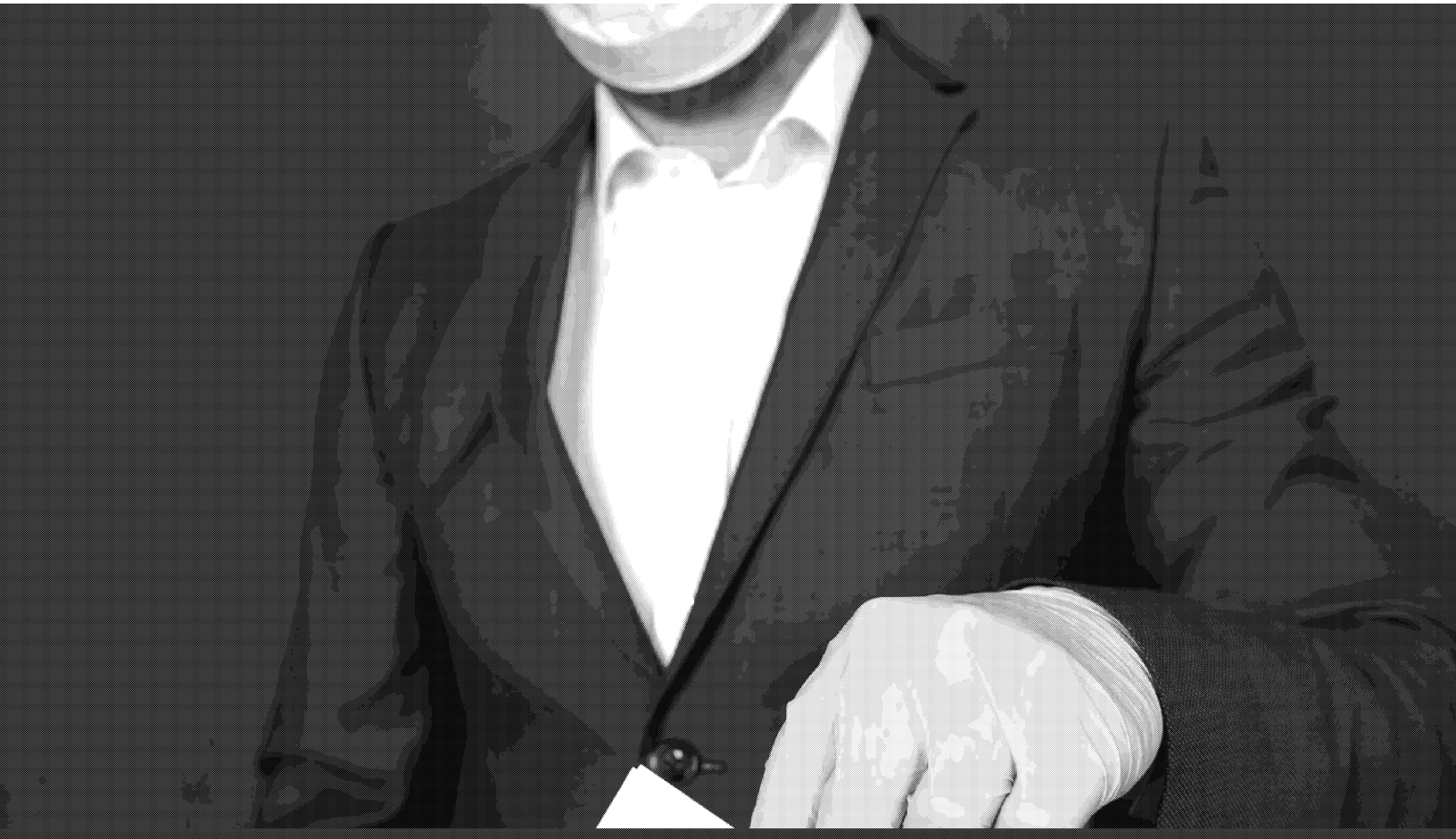
FIGURE 02 | OBJECTIFS À COURT, À MOYEN ET À LONG TERMES DES AUTEURS DE CYBERMENACE PARRAINÉS PAR DES ÉTATS



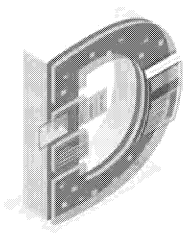
IMPACTS DE LA PANDÉMIE DE COVID-19 SUR LES PROCESSUS DÉMOCRATIQUES

En 2020, au moins 40 pays et territoires à travers le monde ont dû reporter des élections et des référendums à l'échelle nationale en raison de la pandémie de COVID-19 alors qu'au moins 79 élections et référendums à l'échelle nationale se sont quand même tenus pendant la pandémie.[10] La majorité des États ont mis en place des mesures sanitaires et de distanciation, et beaucoup ont proposé différents moyens de vote pour permettre aux gens en isolement volontaire ou à ceux dont la santé est plus fragile de voter en toute sécurité et de réduire l'achalandage dans les bureaux de scrutin. Par exemple, des États ont élargi le vote par la poste, ont autorisé le vote par téléphone, ont prolongé les heures de vote et augmenté le nombre de bureaux de scrutin.[11]

Dans l'ensemble, les modifications apportées aux procédures électorales en raison de la COVID-19 semblent avoir eu une incidence limitée sur la cybermenace qui pèse sur les élections. Elles ont créé de nouvelles possibilités pour les auteurs de cybermenace, mais d'après nos observations, ces derniers n'ont pas vraiment changé la fréquence de leurs activités. Même si les auteurs de menace peuvent tenter de brouiller la communication sur les modifications apportées aux procédures de vote ou cibler des campagnes électorales en ligne, nous estimons que les meilleures occasions qui s'offrent à eux sont les messages liés à la COVID-19 qu'ils peuvent utiliser pour miner la confiance de la population dans les élections.[12] Ces messages servent entre autres à établir un lien entre la fraude électorale et le vote par la poste et exagèrent les risques pour la santé publique que représentent les votes en personne.[13]



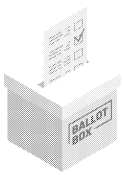
CIBLES PRINCIPALES DU PROCESSUS DÉMOCRATIQUE



ANS le rapport intitulé *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019*, nous avons déterminé trois cibles principales au sein du processus démocratique : les électeurs, les partis politiques et les élections. La section qui suit fournit des détails supplémentaires sur les menaces auxquelles fait face chaque cible et sur l'évolution de celles-ci au cours des dernières années, plus particulièrement dans le contexte de la pandémie de COVID-19.

Les électeurs interagissent avec les partis politiques, les candidats et les autres électeurs au moyen des médias sociaux. Ils accèdent également à de l'information sur les processus de vote en ligne. Les auteurs de cybermenace manipulent l'information diffusée en ligne pour influencer l'opinion et le comportement des électeurs.

Les partis politiques se disputent l'attention et le soutien des électeurs, surtout au moyen d'Internet qu'ils utilisent pour s'organiser et communiquer avec ces derniers. Cette dépendance est encore plus marquée pendant la pandémie de COVID-19 alors que les campagnes en personne et les événements de collecte de fonds se butent à des restrictions liées à la COVID-19. Les auteurs de cybermenace se servent de cyberoutils pour cibler les sites Web, les comptes de courriel et de médias sociaux, les réseaux et les dispositifs des partis politiques, des candidats et de leur personnel. Ils ciblent également les experts-conseils, les maisons de sondage et les sociétés de recherche engagés par des partis politiques.



Les élections englobent tous les processus qui s'enclenchent lorsque des personnes votent pour les représentants du gouvernement : l'inscription des électeurs, le vote, le dépouillement du scrutin et le dévoilement du résultat au public. Les électeurs 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'utilisent les organismes d'administration électorale.

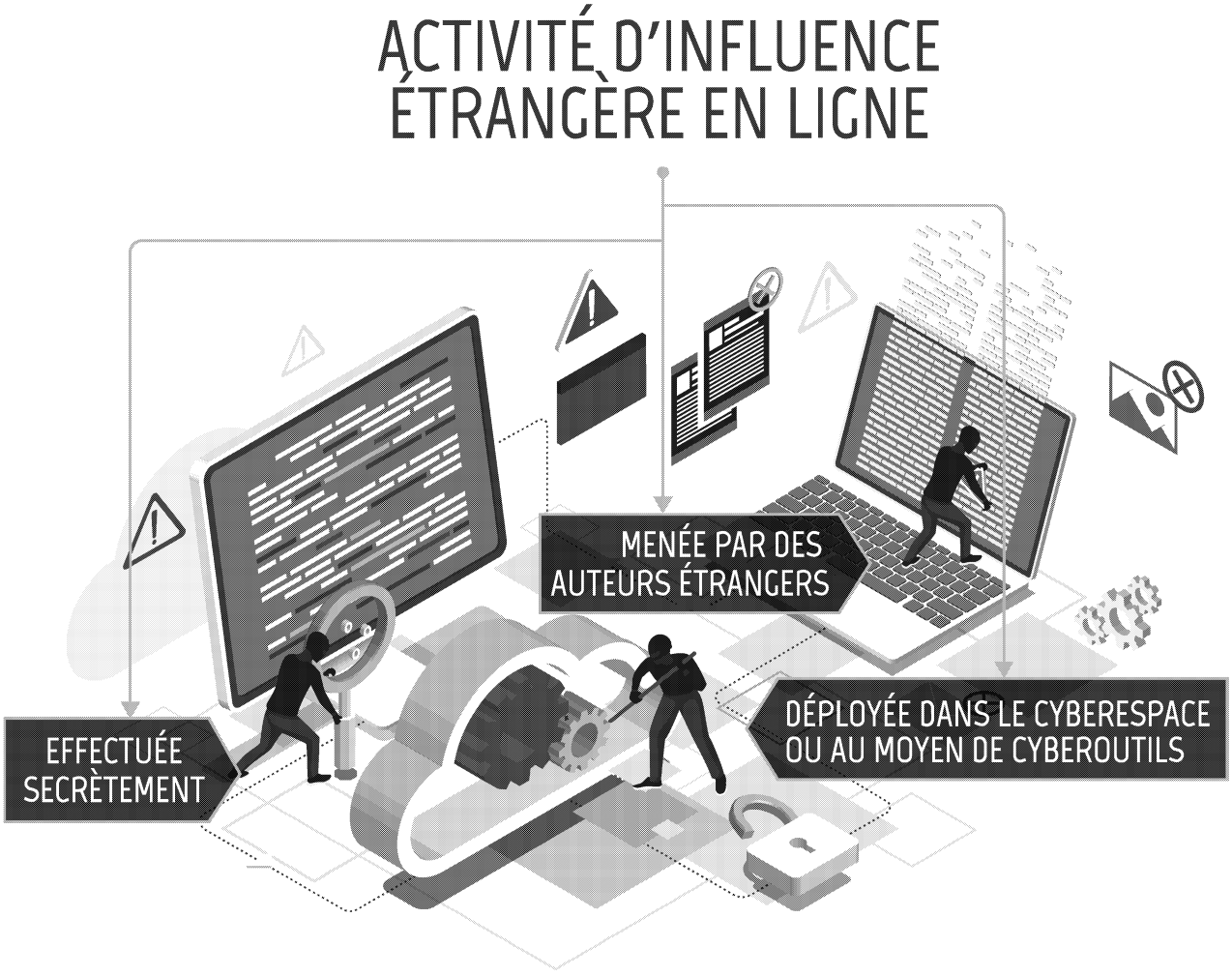
CIBLER LES ÉLECTEURS

Nous estimons que l'influence étrangère en ligne est la cybermenace la plus importante qui pèse sur les électeurs; elle se produit lorsque des auteurs étrangers créent, diffusent ou amplifient discrètement des informations fausses et trompeuses en ligne afin d'influencer les croyances ou les comportements des électeurs. Les auteurs de cybermenace ciblent également les bases de données contenant des renseignements sur les électeurs que détiennent les partis politiques et les organismes d'administration électorale, ainsi que les sites Web que consultent les électeurs pour obtenir l'information dont ils ont besoin pour voter.

L'influence étrangère en ligne est devenue un outil courant pour les adversaires. Ils y ont recours pour servir leurs intérêts fondamentaux, comme la sécurité nationale, la prospérité économique et des objectifs idéologiques.[C] Les campagnes d'influence en ligne peuvent avoir pour objectif :

- d'avoir un impact sur le débat public;
- d'influencer les choix des décideurs politiques;
- de compromettre les relations gouvernementales et la réputation des politiciens;
- de délégitimiser le concept de la démocratie ainsi que d'autres valeurs, comme les droits de la personne et la liberté;
- d'aggraver la friction actuelle dans les sociétés démocratiques.

FIGURE 03 | TROIS COMPOSANTES D'UNE ACTIVITÉ D'INFLUENCE ÉTRANGÈRE EN LIGNE



C Pour obtenir de plus amples renseignements, consultez l'*ECN 2020* du CST

L'INFLUENCE ÉTRANGÈRE ET L'ÉCOSYSTÈME INFORMATIONNEL INTÉRIEUR

Les électeurs doivent composer avec un écosystème informationnel en ligne rempli d'informations fausses et trompeuses. Ces informations peuvent provenir de sources étrangères ou intérieures. Il est souvent difficile de déterminer la provenance de l'information qui circule sur Internet et de savoir qui la diffuse et pourquoi. Bien que cela dépasse la portée de la présente évaluation, des renseignements faux ou inexacts diffusés par des auteurs nationaux (avec des intentions malveillantes ou non) peuvent avoir un effet négatif sur les électeurs et contribuer à la réalisation des objectifs des auteurs de menace étrangers, comme le fait de miner la confiance des électeurs dans les processus électoraux et de diviser davantage l'électorat.

TYPES DE FAUSSE INFORMATION : DÉSINFORMATION ET MÉSINFORMATION

La désinformation est une fausse information qui a été délibérément conçue et diffusée pour causer des préjudices[14], notamment la modification de documents officiels pour faire de fausses allégations qui paraissent légitimes ou la création d'un contenu qui semble officiel, comme un hypertrucage. **La mésinformation** est une fausse information répandue sans vouloir causer de préjudices.[15] Concrètement, il est souvent difficile de faire la différence entre la mésinformation et la désinformation.

Les médias sociaux augmentent la portée des messages des auteurs nationaux qui comptent de nombreux abonnés, comme les influenceurs, les personnes ayant des comptes vérifiés ou les personnalités publiques. Une fausse information répandue par des personnalités importantes, notamment lorsqu'il s'agit de messages visant à miner la confiance envers les institutions et les processus démocratiques, peut se propager davantage et avoir une plus grande incidence sur les électeurs que lorsque des auteurs étrangers cherchent à faire la même chose de façon discrète. La portée disproportionnée de personnalités publiques a été étudiée dans le contexte de la COVID-19. En effet, des chercheurs du Reuters Institute ont constaté que même si la mésinformation liée à la COVID-19 provenant de grandes personnalités publiques comptait pour à peine 20 % des allégations de mésinformation étudiées, elles représentaient 69 % de la mobilisation dans les médias sociaux.[16]

Certains gouvernements et partis politiques se servent de la désinformation ou manipulent l'écosystème informationnel en ligne pour influencer les électeurs.[17] Par exemple, pendant la campagne électorale de 2021 en Ouganda, Facebook a retiré un réseau de faux comptes et de comptes en double liés au gouvernement ougandais qui étaient utilisés pour augmenter la popularité des messages.[18] Dans les jours qui ont suivi, le gouvernement a interdit les médias sociaux et a fermé l'accès à Internet en Ouganda.[19] Les gouvernements restreignent de plus en plus l'accès à Internet durant les élections pour limiter l'accès à l'information, étouffer l'opposition et contenir la liberté d'expression.[20]

INFLUENCE EN LIGNE CONTRE COMPENSATION FINANCIÈRE

Des entreprises privées sont de plus en plus nombreuses à offrir des services d'influence en ligne à des gouvernements et à des auteurs politiques.[21] Une étude menée à Oxford en 2020 a cerné 48 cas où des entreprises privées se livraient à de la désinformation pour le compte d'un auteur politique. Depuis 2018, les mêmes chercheurs ont trouvé plus de 65 entreprises offrant la désinformation en tant que service.[22] Pour y arriver, celles-ci ont recours au trollage, à des comptes automatisés, à des comptes gérés par des humains et à l'IA.[23] Les gouvernements et les auteurs politiques qui embauchent des entreprises pour mener des campagnes d'influence en ligne en leur nom font appel non seulement à des sociétés de leur pays, mais aussi à des firmes basées à l'étranger.[24] Par exemple, entre 2019 et 2020, la firme Archimedes Group, basée en Israël, a mené des campagnes d'influence en ligne contre des élections qui se sont déroulées en Afrique, en Amérique latine et en Asie du Sud-Est.[25]

ÉTUDE DE CAS : QANON ET L'INFLUENCE ÉTRANGÈRE EN LIGNE

QAnon est un mouvement peu structuré basé sur des théories conspirationnistes réfutées. Le volume et la fréquence du contenu de ces théories sont en hausse depuis la fin de 2017.[26] Principalement établies aux États-Unis, les théories de QAnon ont maintenant des adeptes dans plus de 25 pays, dont le Canada, qui est d'ailleurs l'un des quatre principaux pays à partir desquels du contenu de QAnon est publié dans les médias sociaux.[27] Des groupes parrainés par la Russie et l'Iran ont diffusé du contenu relatif à QAnon.[28] Des comptes de médias sociaux et de nouvelles ayant des liens avec la Russie ont fait la promotion de QAnon à ses débuts.[29] Sur Twitter, des comptes qui seraient contrôlés par des auteurs de cybermenace russes ont publié en 2019 un nombre élevé de gazouillis en lien avec QAnon.[30] Dans une moindre mesure, des auteurs iraniens ont fait référence à QAnon et au contenu de ses théories dans le cadre de leur activité d'influence en ligne, notamment lors d'activités qui ont eu lieu pendant l'élection américaine de 2020.[31]

Des auteurs de cybermenace parrainés par des États, dont la Russie et l'Iran, ont profité de groupes et de mouvements nationaux dans certains pays et se sont servis des messages et de la portée de ces groupes pour mieux influencer les électeurs.[32] Par exemple, des auteurs de cybermenace parrainés par des États ont fait la promotion de contenus et de messages liés au mouvement QAnon dans le but de toucher l'électorat aux États-Unis. Ils se sont également fait passer pour des groupes nationaux américains pour envoyer des messages menaçants à des électeurs.[33]

Des intellectuels et des journalistes de pays donnés ont également été embauchés à leur insu par des auteurs de cybermenace étrangers pour rédiger des articles présentant un certain angle politique qui sont ensuite utilisés dans des campagnes plus générales d'influence étrangère.[34] Cette situation ne fait que brouiller davantage la distinction entre les auteurs d'un pays et ceux de l'étranger. S'allier à des sources légitimes pour qu'elles soutiennent des points de vue spécifiques donne de la crédibilité aux messages véhiculés par des campagnes d'influence étrangère en ligne.

Cette façon de faire brouille davantage la distinction entre les auteurs d'un pays et ceux de l'étranger et donne de la crédibilité aux points de vue soutenus par des campagnes d'influence en s'alliant à des sources légitimes pour promouvoir des messages spécifiques.

INTERNET, PLATEFORMES DE MÉDIAS SOCIAUX ET ÉLECTEURS

Les électeurs du monde entier obtiennent de grandes quantités d'informations en ligne, souvent par le biais des médias sociaux.[35] Les plateformes de médias sociaux sont toutefois un environnement propice à la création et à la diffusion de fausses informations. Elles reposent sur des algorithmes d'apprentissage profond pour proposer du contenu aux utilisateurs et privilégient souvent des messages ayant suscité un engouement (par exemple, par le biais de partages, de mentions j'aime ou de commentaires), contribuant ainsi à l'amplification du contenu provocant.[36] Par conséquent, les électeurs sont inondés d'informations trompeuses, fausses et provocatrices. Dans le contexte de la COVID-19 et des élections, certaines plateformes de médias sociaux ont adopté les mesures suivantes pour essayer de contrer la diffusion de fausses informations :

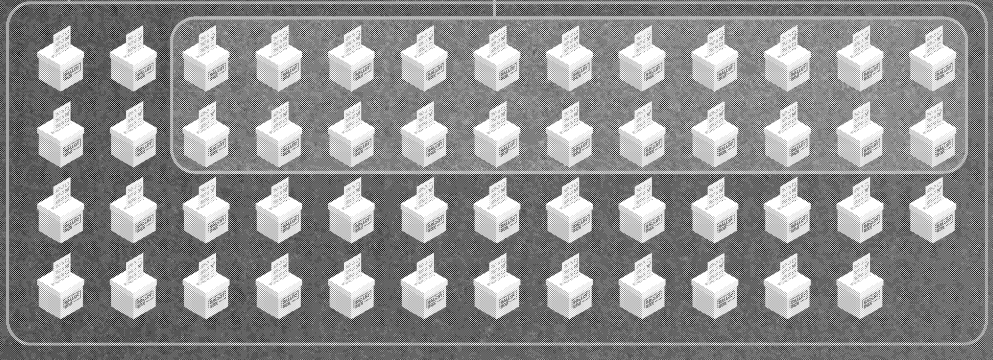
- déclasser le contenu douteux (c.-à-d. le contenu qui contrevient presque aux lignes directrices communautaires);
- fermer les comptes non authentiques;
- embaucher du personnel pour filtrer les publications et enquêter sur les cas de malfaisance;
- collaborer avec des organismes de vérification des faits et de recherche;
- signaler ou déclasser le contenu trompeur;
- diriger les utilisateurs vers des sources fiables.[37]

Certaines plateformes de médias sociaux, adaptées à des groupes d'utilisateurs précis, jouent un rôle essentiel dans la diffusion de contenus haineux et radicaux.[38] Bien que des sites comme 4chan, 8chan, Gab et Parler n'ont pas la portée des médias sociaux plus populaires, ils permettent quand même à des personnes aux vues similaires de se rassembler pour interagir et entretenir des opinions radicales qui peuvent ensuite être propagées sur l'ensemble de la toile.[39] Le retrait des contenus radicaux et faux d'un nombre croissant de plateformes conventionnelles peut aussi inciter des individus intéressés à ce type d'information à passer d'une communauté ouverte, comme Twitter, à des groupes marginaux, comme Gab, qui se targuent de permettre aux utilisateurs de publier ce qu'ils veulent.[40] Des auteurs étrangers hostiles se sont servis de telles plateformes pour mener des activités d'influence étrangère en ligne. Par exemple, durant l'élection américaine de 2020, des auteurs russes ont ciblé des utilisateurs américains d'extrême droite sur Gab et Parler avec une activité d'influence étrangère en ligne visant à promouvoir le président Trump et à dénigrer le candidat Biden.[41]

Certaines plateformes sont utilisées principalement par des communautés spécifiques et peuvent servir à censurer ou promouvoir des messages au sein de ces communautés. Par exemple, WeChat, une application de Chine offrant de multiples fonctionnalités et qui est utilisée par des milliards de personnes à travers le monde, a intensifié les divisions et a diffusé de la désinformation ou de la propagande en s'adressant spécifiquement à la diaspora chinoise qui utilise la plateforme.[42]

FIGURE 04 | CAMPAGNES POLITIQUES PENDANT LA PANDÉMIE DE COVID-19

Un examen des élections nationales tenues dans **51** pays pendant la pandémie de COVID-19 en 2020 a révélé que **22** de ces pays avaient adopté des mesures liées à la COVID-19 qui limitaient les possibilités de rassemblement public et qui avaient donc des répercussions sur les campagnes électorales. Dans de nombreux pays, les candidats ont réagi en faisant campagne en ligne.*



INFLUENCE ÉTRANGÈRE EN LIGNE SUR PLATEFORMES CHIFFRÉES

Les applications de messagerie chiffrée, comme WhatsApp, Signa et Telegram, compliquent le suivi et le freinage de la propagation de fausses informations. C'est d'ailleurs pour cette raison que de nombreux groupes chassés de plateformes d'applications conventionnelles se tournent vers des applications de messagerie chiffrée.[43] Par exemple, après l'expulsion de groupes américains d'extrême droite de plusieurs plateformes conventionnelles et la fermeture de la plateforme Parler en raison des mesures prises par Apple, Google et Amazon, beaucoup d'utilisateurs d'extrême droite se sont tournés vers des applications de messagerie chiffrée comme Signal, CloutHub, MeWe, Telegram et Rumble.[44] De plus, de par le caractère fermé de ces applications, la plupart des utilisateurs communiquent avec des gens qu'ils jugent dignes de foi. La transmission d'information à de grands groupes augmente également le risque qu'une fausse information soit interprétée comme un fait. Pendant la pandémie de COVID-19, les applications de messagerie chiffrée sont aussi devenues une courroie de transmission majeure pour tout ce qui touche la mésinformation, les fraudes et les canulars liés au domaine médical.[45]

LA COVID-19 ET LA CYBERMENACE QUI PLANE SUR LES ÉLECTEURS

La pandémie de COVID-19 offre de nouvelles occasions d'influence étrangère en ligne visant à saper la confiance des électeurs dans les processus électoraux et à baisser le taux de participation aux élections.[46] Beaucoup de pays ont étendu l'accès au scrutin postal et ont opté pour d'autres méthodes de vote afin de réduire l'affluence aux urnes et de protéger les électeurs à risque. Toutefois, cela ouvre la voie aux auteurs de cybermenace pour créer ou amplifier des informations fausses faisant un lien entre le vote par la poste ou d'autres nouvelles modalités de vote et la fraude électorale. Les auteurs étrangers hostiles peuvent également créer et amplifier les messages pour fausser la perception qu'ont les électeurs du risque de contracter la COVID-19 aux urnes dans le but de baisser le taux de participation. Même si elles n'affectent pas le taux de participation, l'omniprésence de ces propos et la perception selon laquelle la COVID-19 fait diminuer la participation au vote risquent de miner la confiance des électeurs à l'égard des résultats. Enfin, les changements apportés aux procédures de vote, comme d'augmenter le nombre de jours prévus pour le scrutin et d'accroître l'utilisation du vote par la poste, peuvent retarder la diffusion des résultats. Un tel retard permet aux auteurs de menace de faire de la désinformation, par exemple en donnant de faux résultats, avant que les organismes d'administration électorale aient l'occasion de diffuser l'information exacte.

CIBLER LES PARTIS POLITIQUES

Les auteurs de cybermenace ciblent les partis politiques, les candidats et leur personnel de différentes façons pour :

- perturber l'engagement auprès du public pour obtenir un gain financier, pour nuire à un parti politique ou à un candidat, ou pour obtenir de la publicité;
- voler de l'information sensible ou exclusive, notamment celle contenue dans des bases de données;
- entraver les procédures des partis politiques entreprises en ligne.

Nous estimons que les cybercriminels continueront presque assurément de tirer profit de la présence en ligne des partis politiques ou des politiciens pour en tirer des gains financiers, que ce soit en détournant des sites Web ou des comptes de partis

FIGURE 05 | COMMENT LES CANDIDATS SE SONT ADAPTÉS À LA PANDÉMIE DE COVID-19

* Erik Asplund, et al. Elections and COVID-19: How election campaigns took place in 2020 International Institute for Democracy and Electoral Assistance 2 février 2021
https://www.idea.int/news-media/news/elections-and-covid-19-how-election-campaigns-took-place-2020

politiques ou de politiciens ou en créant de faux sites Web, comptes, courriels ou autres communications conçus pour avoir l'air officiels. Les cybercriminels peuvent utiliser un rançongiciel ou y aller d'attaques DDoS pour perturber des événements ou des pages en ligne et tenter de soutirer de l'argent à des politiciens et à des partis politiques. Selon Cloudflare, une entreprise américaine de services de sécurité de site Web, un nombre considérable d'activités DDoS a été observé contre des sites Web de campagnes politiques américaines en 2020.[47] Les cybercriminels peuvent également compromettre les ressources en ligne de politiciens et de partis politiques d'autres façons. Par exemple, lors de l'élection américaine de 2020, le site Web de la campagne électorale d'un candidat a été compromis par des cybercriminels qui ont tenté de l'utiliser pour percevoir de la cryptomonnaie.[48] De plus, certains cybercriminels tirent profit des événements dans l'actualité, dont les élections, pour cibler leurs victimes en leur envoyant des courriels d'hameçonnage sur des sujets d'intérêt pour inciter les destinataires à ouvrir des pièces jointes malveillantes ou à cliquer sur des liens malveillants.[49] Lorsqu'il est question de leurres liés aux élections, les victimes sont des membres de partis politiques, des candidats, leur personnel, des électeurs ou d'autres personnes qui s'intéressent aux élections.

Les auteurs parrainés par des États s'intéressent également aux réseaux, aux sites Web et aux comptes de courriel et de médias sociaux de partis politiques, de candidats et de leur personnel. Le fait de perturber la campagne d'un candidat ou d'un parti politique peut avoir une incidence sur l'appui que reçoit ce parti ou miner la confiance dans l'équité du processus électoral. Les hacktivistes, les auteurs ayant une motivation politique et les amateurs de sensations fortes ont également ciblé des sites Web et des événements de partis politiques et de candidats pour diffuser leurs propres messages et pour obtenir de la publicité.[50]

En outre, l'information sensible liée à un parti politique ou à un candidat ainsi que les bases de données des partis politiques renfermant des renseignements personnels sont attrayantes tant pour les cybercriminels que pour les auteurs parrainés par des États. Les maisons de sondage, les sociétés de recherche et les experts-conseils embauchés par des partis politiques ou des candidats détiennent également de l'information intéressante pour les auteurs de cybermenace. Les bases de données volées peuvent servir à des cyberactivités futures, notamment des activités motivées par l'appât du gain ainsi que des campagnes menées à des fins stratégiques par des auteurs de cybermenace parrainés par des États. L'information sensible volée de comptes compromis peut être divulguée dans le but de ternir la réputation d'un candidat ou être utilisée comme forme d'extorsion. Les auteurs de menace peuvent aussi concentrer leurs activités d'influence étrangère en ligne sur un candidat ou un parti spécifique pour chercher à éloigner les électeurs de ce candidat et à les diriger vers un opposant.

Enfin, certains partis politiques votent en ligne. Dans certains cas, cela permet à un plus grand nombre de membres du parti de voter lors d'une course à la chefferie.[51] Toutefois, lorsqu'il est tenu en ligne, le scrutin est particulièrement vulnérable aux auteurs de cybermenace qui pourraient chercher à changer les résultats ou à semer la méfiance au sein d'un parti politique. D'ailleurs, en 2021, un parti politique d'Allemagne qui a tenu sa course à la chefferie en ligne dans le cadre d'une conférence virtuelle a été la cible d'une attaque DDoS. L'attaque a causé l'interruption de la conférence, mais n'a eu aucune incidence sur le scrutin puisqu'il n'était pas hébergé sur le même serveur que la conférence afin de protéger le vote contre toute cybermenace.[52]

LA COVID-19 ET LA CYBERMENACE QUI PLANE SUR LES PARTIS POLITIQUES

En raison de la pandémie de COVID-19, les événements en personne organisés dans le cadre de campagnes électorales, comme les rassemblements politiques, les collectes de fonds ou la sollicitation porte-à-porte, ont été limités, voire interdits dans certains pays. Face à cette situation, certains partis politiques et candidats ont dû s'adapter afin de se conformer aux mesures sanitaires de leur région en envoyant des trousses d'information par la poste, en organisant des rassemblements en auto, en faisant des visites porte-à-porte en respectant la distanciation et en augmentant leur utilisation d'outils en ligne pour mener la campagne ou prendre des décisions à l'interne concernant le parti.[53] Depuis le début de la pandémie, les partis politiques ont tenu des conventions virtuelles, des assemblées publiques locales et des collectes de fonds, et ils se sont tournés vers les appels vidéo en ligne pour solliciter des votes.[54] Les campagnes et les collectes de fonds électorales se faisaient déjà en ligne avant la COVID-19, mais la pandémie a fait augmenter l'utilisation des outils numériques.[55] Ce mouvement vers des solutions en ligne offre davantage de possibilités aux auteurs de cybermenace qui cherchent à cibler les partis et les campagnes politiques dans le but de faire avancer des objectifs stratégiques ou pour obtenir un gain financier. Il affaiblit aussi la résilience des campagnes advenant la compromission des ressources en ligne.

ADAPTER LES CAMPAGNES ÉLECTORALES EN TEMPS DE COVID-19 : CORÉE DU SUD

La Corée du Sud a été l'un des premiers pays à tenir une élection nationale majeure pendant la pandémie de COVID-19. Des restrictions sur la tenue d'événements, la participation à des rassemblements publics et les exigences relatives à la distanciation physique ont empêché l'organisation d'activités habituelles de campagne, comme les rassemblements partisans, les discours publics, les débats, les collectes de fonds et les sollicitations porte-à-porte. Les candidats ont plutôt adopté la technologie en ligne et numérique, ce qui leur a permis de diffuser des messages vidéo par le biais des médias sociaux, de textes et d'applications pour téléphones cellulaires. Certains candidats ont eu recours à la réalité augmentée pour discuter avec les électeurs à distance alors que d'autres ont aussi fait campagne en dehors de l'espace numérique, en faisant du bénévolat en lien avec la COVID-19 et en postant aux électeurs des documents imprimés.[56]

CIBLER LES ÉLECTIONS

Les auteurs de menace qui souhaitent miner les institutions démocratiques ou saboter les résultats des élections peuvent s'en prendre aux processus et à l'infrastructure des élections, falsifier le contenu des sites Web et des comptes de médias sociaux des administrations électorales, voler de l'information comme celle des bases de données d'inscription des électeurs ou compromettre la sécurité des communications et des systèmes essentiels aux élections. Les processus électoraux de partout dans le monde sont composés de quatre grandes étapes et chacune d'elles présente des occasions à saisir pour les auteurs de menace.

Dans plusieurs pays, l'**inscription des électeurs** se fait en ligne.[57] Les auteurs de cybermenace peuvent cibler les registres en ligne des électeurs pour tenter d'y ajouter des dossiers de faux électeurs, effacer ou chiffrer des données, trafiquer le site Web pour empêcher les inscriptions ou publier de l'information trompeuse. Ces activités peuvent semer le doute dans l'esprit des électeurs, ralentir le processus électoral, frustrer les électeurs ou les amener à ne pas voter et influencer le résultat du scrutin. Les données volées sur l'inscription des électeurs peuvent servir pour de futures activités de menace, comme des activités stratégiques liées à l'élection ou encore des cybermenaces n'ayant aucun lien avec l'élection.[D]

Lorsque les électeurs vont **voter** en personne, les responsables vérifient leur identité et confirment qu'ils figurent dans la liste des électeurs inscrits dans les registres de scrutin. De nombreux pays ont adopté des registres électroniques du scrutin pour faciliter la recherche des électeurs. Les registres sont parfois connectés en réseau pour que les différents bureaux de scrutin puissent communiquer entre eux et que les gens puissent choisir où ils veulent voter sans leur permettre de le faire à plus d'un endroit. Toutefois, ces dispositifs connectés et pouvant communiquer à distance sont plus vulnérables aux cybermenaces. Un électeur peut exercer son droit de vote après qu'on a confirmé qu'il figure dans la liste des électeurs inscrits. Cette étape est presque toujours faite sur papier ou par voie électrique. L'Estonie est le seul pays qui a recours au scrutin en ligne pour toutes les circonscriptions lors d'une élection à l'échelle nationale.[58]

Une fois le vote terminé, il faut **compter** les bulletins et **annoncer le résultat** du suffrage. On compte souvent les bulletins électroniquement, mais on peut aussi procéder manuellement. Tous les bureaux de scrutin de toutes les circonscriptions remettent ensuite leurs résultats à un organisme central qui s'occupe de comptabiliser le tout. Ils peuvent les transmettre par téléphone, par télécopieur, par courriel ou par voie électronique. Toutefois, de nombreux États conservent les dossiers papier pour pouvoir valider ou vérifier les résultats ultérieurement. La dernière étape du processus électoral est l'annonce des résultats qui se fait souvent en ligne.

La plupart des organismes d'administration électorale recourent à certaines technologies pour améliorer le processus électoral (p. ex. outils de bureautique et sites Web standards, bases de données d'inscription contenant les données biométriques des électeurs et systèmes de vote Web).[59] Certes, ces solutions peuvent augmenter l'efficacité, la précision et la transparence du processus électoral, mais les auteurs de cybermenace peuvent cibler chacun des composants en ligne ou électroniques. Les institutions responsables des élections prennent diverses mesures pour protéger le processus, entre autres garder certaines parties cruciales du processus sur papier, conserver des copies des bases de données importantes et avoir une solution de rechange pour permettre aux électeurs d'inscrire leur vote advenant la défaillance ou la compromission des technologies utilisées.

Des auteurs de cybermenace ont mené des opérations après certaines élections pour discréditer ou miner le gouvernement élu avant qu'il prenne le pouvoir. Ces opérations ne visent pas nécessairement les électeurs, les partis politiques ou les élections. Souvent, les auteurs ciblent les institutions gouvernementales en général ou même les infrastructures essentielles. Ils peuvent même faire de la désinformation au lendemain d'une élection pour semer le doute sur les résultats du suffrage ou pour tenter d'empêcher le gouvernement élu de prendre le pouvoir.

ÉTUDE DE CAS : MANIFESTATIONS EN LIGNE EN BIÉLORUSSIE

De nombreux pays, dont le Canada, les États-Unis et l'Union européenne, ont qualifié de frauduleuses les élections présidentielles d'août 2020 en Biélorussie.[60] Après l'annonce du suffrage, l'opposition a refusé de concéder la victoire, ce qui a déclenché des manifestations massives.[61] Des hacktivistes biélorusses ont alors employé diverses tactiques, dont la défiguration de sites Web du gouvernement et le ciblage d'institutions gouvernementales, pour pousser le président sortant à démissionner. Ils ont par exemple publié le nom et l'adresse de 1000 agents d'application de la loi qui avaient usé de violence dans leurs interventions contre les manifestants.[62] En août 2020, des hacktivistes étaient responsables d'au moins 15 cyberincidents contre des ressources en ligne de l'État biélorusse.[63]

D Pour obtenir de plus amples informations, consultez l'*ECN 2020* du CST.

LA COVID-19 ET LA CYBERMENACE QUI PLANE SUR LES ÉLECTIONS

Avant la pandémie de COVID-19, de nombreux pays transféraient certains processus électoraux en ligne, comme l'inscription des électeurs, mais rares étaient ceux qui tentaient de mettre en place un système de vote Web à l'échelle nationale. Il est donc peu probable que les États qui n'étaient pas déjà dotés de tels systèmes soient aptes ou enclins à en adopter un dans la foulée de la pandémie.[64]

En raison de la COVID-19, des pays de partout dans le monde ont apporté des ajustements à leurs élections à l'échelle nationale, comme imposer de nouvelles règles d'hygiène et de santé publique, modifier les heures de scrutin et l'échéance des inscriptions et offrir de nouvelles méthodes de vote aux personnes à risque ou en isolement. Si la plupart de ces changements n'entraînent pas en soi de nouvelles menaces liées à la cybersécurité, ils doivent être énoncés clairement aux électeurs pour qu'ils se prévalent de ces changements et qu'ils aient toujours l'assurance que les élections sont libres et justes.[65] Certaines démocraties ont annoncé ces changements par Internet, courriel et texto; des auteurs de cybermenace peuvent cibler ces communications pour les modifier, perturber leur transmission ou diffuser de la fausse information ayant l'air réelle.[66]

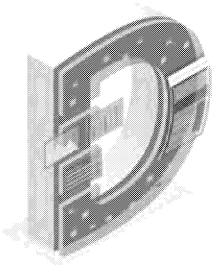
PERTURBATIONS CAUSÉES PAR UNE FORTE DEMANDE

La pandémie peut entraîner une augmentation de la demande pour les diverses ressources en ligne liées au scrutin et aux élections, comme les pages d'information, les bases de données d'inscription des électeurs et les portails de demande de bulletin de vote d'un électeur absent. Les autorités doivent prendre les mesures adéquates pour satisfaire à cette forte demande, sinon les électeurs n'auront peut-être pas accès aux ressources nécessaires pour participer aux élections. C'est d'ailleurs une des inquiétudes qu'avaient manifestées les responsables des élections aux États-Unis à l'approche du scrutin de 2020. Toutefois, aucune panne majeure n'est survenue en raison de l'explosion de la demande.

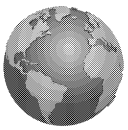
De plus, à l'instar de bien d'autres personnes pendant la pandémie, les employés de certains organismes d'administration électorale ont été forcés de préparer les élections en travaillant à distance. Sauf si elles appliquent les pratiques exemplaires en matière de cybersécurité, les personnes qui travaillent à distance peuvent introduire de nouvelles vulnérabilités, car elles accèdent à des données sensibles liées au travail à partir du réseau Wi-Fi de leur domicile qui est souvent moins bien protégé qu'une infrastructure de TI d'un milieu professionnel.

TENDANCES MONDIALES

DONNÉES DE RÉFÉRENCE MONDIALES SUR LES ÉVÉNEMENTS CONNUS

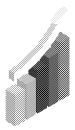


DEPUIS la parution du document *Le point sur les cybermenaces contre le processus démocratique du Canada en 2019*, le CCC a continué de surveiller les cybermenaces menées contre les processus démocratiques partout dans le monde. Comme dans nos rapports précédents, nous supposons que nos sources de données combinées sous-estiment le nombre total d'événements qui ciblent les processus démocratiques à l'échelle mondiale. Nous avons constaté que quatre tendances se dégagent de nos observations réalisées entre 2015 et 2020.



TENDANCE N^{O} 1

Les cybermenaces parrainées par un État visent des États et des régions en particulier.



TENDANCE N^{O} 3

Le ciblage des processus démocratiques est toujours élevé.

TENDANCE N^{O} 2

La plupart des cybermenaces dirigées contre des processus démocratiques appuient des objectifs stratégiques.

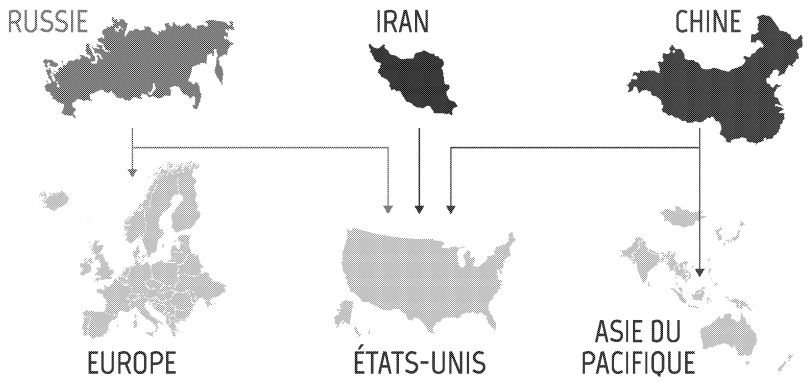
TENDANCE N^{O} 4

Les cyberactivités ont souvent une incidence sur de nombreuses cibles d'un processus démocratique.

TENDANCE Nº 1 LES CYBERMENACES PARRAINÉES PAR UN ÉTAT VISENT DES ÉTATS ET DES RÉGIONS EN PARTICULIER

Nous estimons que les auteurs parrainés par la Russie, la Chine et l'Iran sont responsables de la majorité des cybermenaces lancées contre les processus démocratiques dans le monde. Nous avons constaté que de toutes les cybermenaces menées depuis 2015 par ces pays contre les processus démocratiques, plus de 90 % étaient axées sur des États revêtant une importance stratégique pour eux. Plus précisément, la plupart des activités attribuées à la Russie visaient les processus démocratiques des États-Unis, de l'Ukraine et d'autres États européens. Pour sa part, la Chine ciblait surtout les États-Unis, Taïwan et d'autres pays de l'Asie et du Pacifique. L'Iran, quant à elle, dirigeait la plupart de ses activités contre les États-Unis. Les cibles des cybermenaces parrainées par un État et dirigées contre les processus démocratiques sont dictées par les intérêts des auteurs de menace et les pays qu'ils perçoivent comme une menace pour leurs objectifs régionaux et mondiaux.

FIGURE 06 LES AUTEURS DE CYBERMENACE CIBLENT DES ÉTATS ET DES RÉGIONS D'IMPORTANCE STRATÉGIQUE



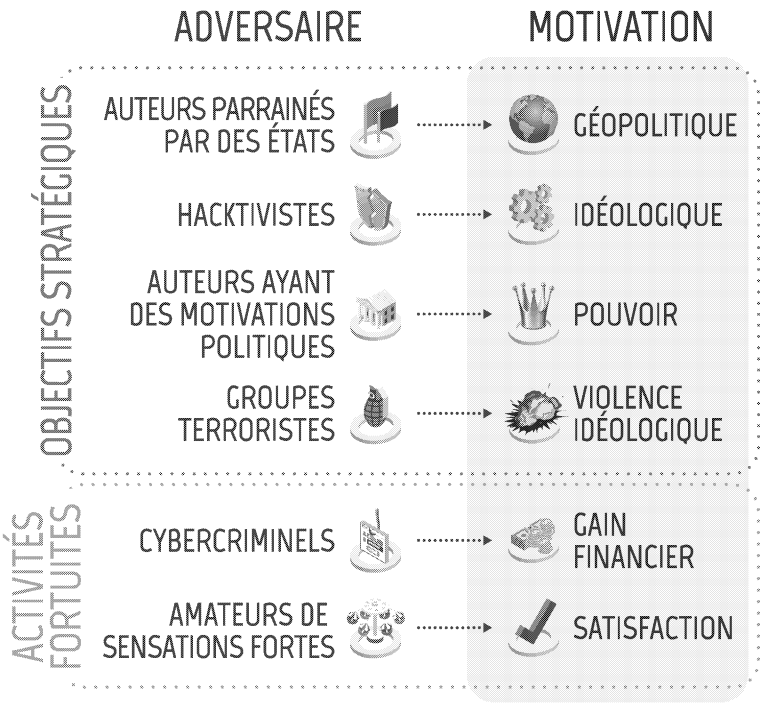
Plus de **90 %**

des activités de cybermenace observées depuis 2015 et menées par la Russie, la Chine et l'Iran visaient des États et des régions revêtant une importance stratégique pour eux.

TENDANCE Nº 2 LA PLUPART DES CYBERMENACES DIRIGÉES CONTRE DES PROCESSUS DÉMOCRATIQUES APPUIENT DES OBJECTIFS STRATÉGIQUES

La vaste majorité des cybermenaces qui ont touché les processus démocratiques dans le monde entre 2015 et 2020 servaient les objectifs stratégiques de leurs auteurs. D'après nos observations, les auteurs de menace parrainés par un État ont mené 76 % des activités contre les processus démocratiques que nous avons pu attribuer à leurs responsables. Étant donné qu'une telle opération est relativement facile à mener et peut rapporter gros, nous estimons que les auteurs de menace parrainés par un État accordent fort probablement un plus grand intérêt pour les processus démocratiques que les autres auteurs de menace. Les activités fortuites désignent des cyberactivités qui ont eu une incidence sur un processus démocratique, mais qui ne servaient pas un objectif stratégique. Les cybercriminels étaient responsables de la plus grande partie des activités fortuites et de 8 % de toutes les cyberactivités observées contre les processus démocratiques que nous avons attribuées à leurs auteurs.

FIGURE 07 ACTIVITÉS SERVANT DES OBJECTIFS STRATÉGIQUES ET ACTIVITÉS FORTUITES



TENDANCE Nº 3 LE CIBLAGE DES PROCESSUS DÉMOCRATIQUES EST TOUJOURS ÉLEVÉ

Comme nous l'avons constaté dans nos rapports précédents, le nombre de cybermenaces contre les processus démocratiques reste élevé. Nous avons remarqué une augmentation marquée de la proportion d'élections ciblées par des cybermenaces entre 2015 et 2017. Toutefois, les proportions sont restées relativement stables de 2017 à 2020 pour ce qui est des activités contre les processus démocratiques liés à des élections dans le monde, à des élections dans des pays membres de l'Organisation de coopération et de développement économiques (OCDE) et à des élections dans des pays du G20. Ces chiffres ne tiennent pas compte des cas où des auteurs se sont livrés secrètement à des activités d'influence en ligne dans leur propre pays ou encore des cas où des sociétés de relations publiques ont été embauchées pour mener de telles activités. De telles sociétés ont été embauchées dans au moins 48 pays.[68]

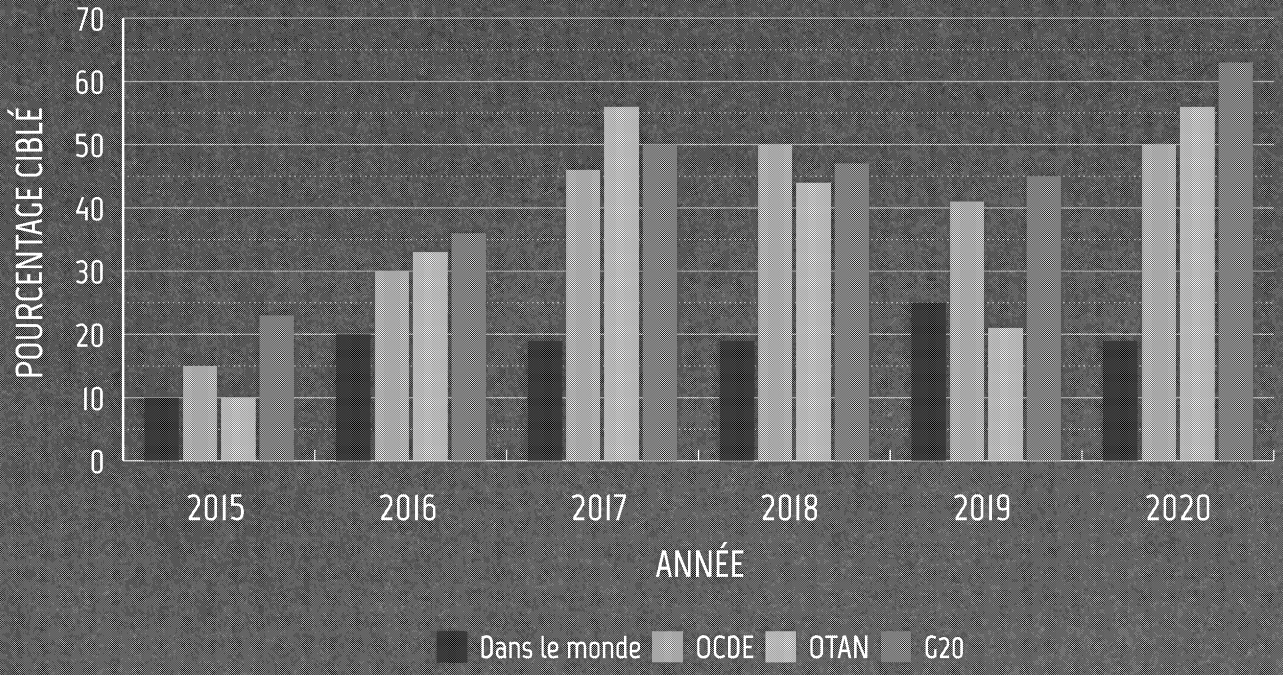
Le pourcentage d'élections prises pour cible chaque année est stable depuis 2017. Toutefois, cette statistique ne tient pas compte des variations dans la quantité d'activités éprouvées par chaque pays – qu'un pays soit victime d'une vaste campagne ou d'un seul événement, il est considéré comme un pays touché.

On observe également des tendances compensatoires qui ont pour effet de diminuer le nombre de cybermenaces contre les processus démocratiques, notamment :

- les efforts déployés par les médias sociaux afin de repérer et de supprimer les comptes exhibant un comportement non authentique coordonné et de signaler le contenu problématique;
- l'approfondissement de la couverture médiatique et de la sensibilisation du public;
- la mobilisation des entités gouvernementales, des organismes non gouvernementaux et de recherche et de la société civile pour contrer le faux contenu;
- l'amélioration des pratiques de cybersécurité;
- l'attribution publique des activités à leurs auteurs et la mise en accusation de ces auteurs.

Aucune étude méthodique n'a encore été menée sur l'efficacité de ces mesures, mais une comparaison des élections américaines de 2016 et de 2020 porte à croire qu'on peut atténuer les efforts déployés par les États hostiles pour influencer les processus démocratiques en prenant divers moyens, notamment en cernant les éventuelles campagnes d'influence étrangère en ligne et en attirant l'attention du public sur celles-ci, en renforçant la posture de cybersécurité des organismes participant aux élections et en améliorant la réaction des médias sociaux aux activités malveillantes sur leur plateforme.[69] Les élections qui ont eu lieu à Taïwan en 2020 sont une autre preuve que les enquêtes menées par les gouvernements, la mobilisation de la société civile pour contrer la fausse information et l'intervention des médias sociaux permettent d'atténuer les activités d'influence étrangères et de protéger la démocratie.[70]

FIGURE 08 CYBERMENACES CIBLANT LES PROCESSUS DÉMOCRATIQUES LIÉS À DES ÉLECTIONS



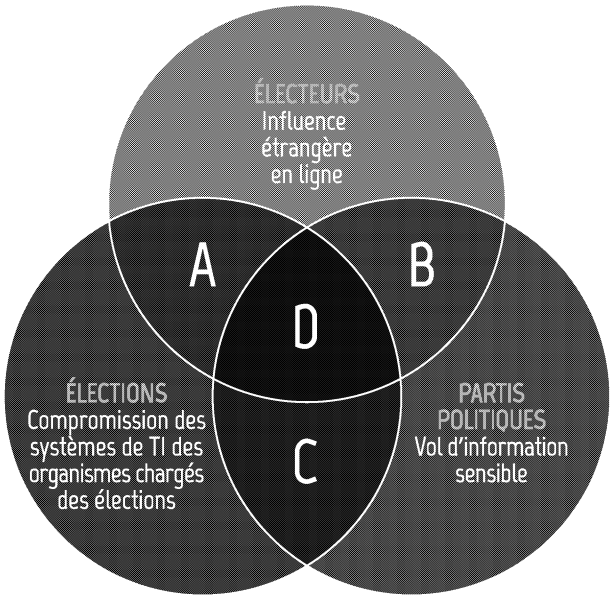
TENDANCE Nº 4 LES CYBERACTIVITÉS ONT SOUVENT UNE INCIDENCE SUR DE NOMBREUSES CIBLES D'UN PROCESSUS DÉMOCRATIQUE

Entre 2015 et 2020, environ un cinquième des processus étudiés a été ciblé par des cybermenaces. Dans la majorité des cas (84 %), lorsqu'un processus était touché, les menaces visaient plus d'un type de cible – électeurs, partis politiques et élections. Parfois, un même incident touchait plusieurs types de cible, comme une opération de piratage et de divulgation d'information qui cible à la fois un candidat et les électeurs exposés à cette information.

Les électeurs ont été plus souvent victimes de cybermenaces que les partis politiques et les élections; ils étaient impliqués dans 87 % des processus démocratiques que nous avons étudiés et qui ont été touchés entre 2015 et 2020. Ils sont souvent ciblés en même temps que les partis politiques, les élections ou les deux. Les partis politiques, impliqués dans 66 % des incidents, viennent au deuxième rang alors que les élections arrivent en troisième avec 53 %.

La figure 10 illustre que les électeurs sont touchés le plus souvent et qu'ils sont fréquemment ciblés en même temps que les partis politiques, les élections ou les deux. Ainsi, nous sommes d'avis que les auteurs de cybermenace considèrent probablement que cibler des électeurs est une façon plus efficace ou avantageuse de s'immiscer dans des processus démocratiques ou que cibler à la fois des électeurs, des partis politiques et des élections est plus efficace que de s'en prendre à un seul groupe.

FIGURE 09 LES CYBERMENACES PEUVENT TOUCHER PLUSIEURS CIBLES



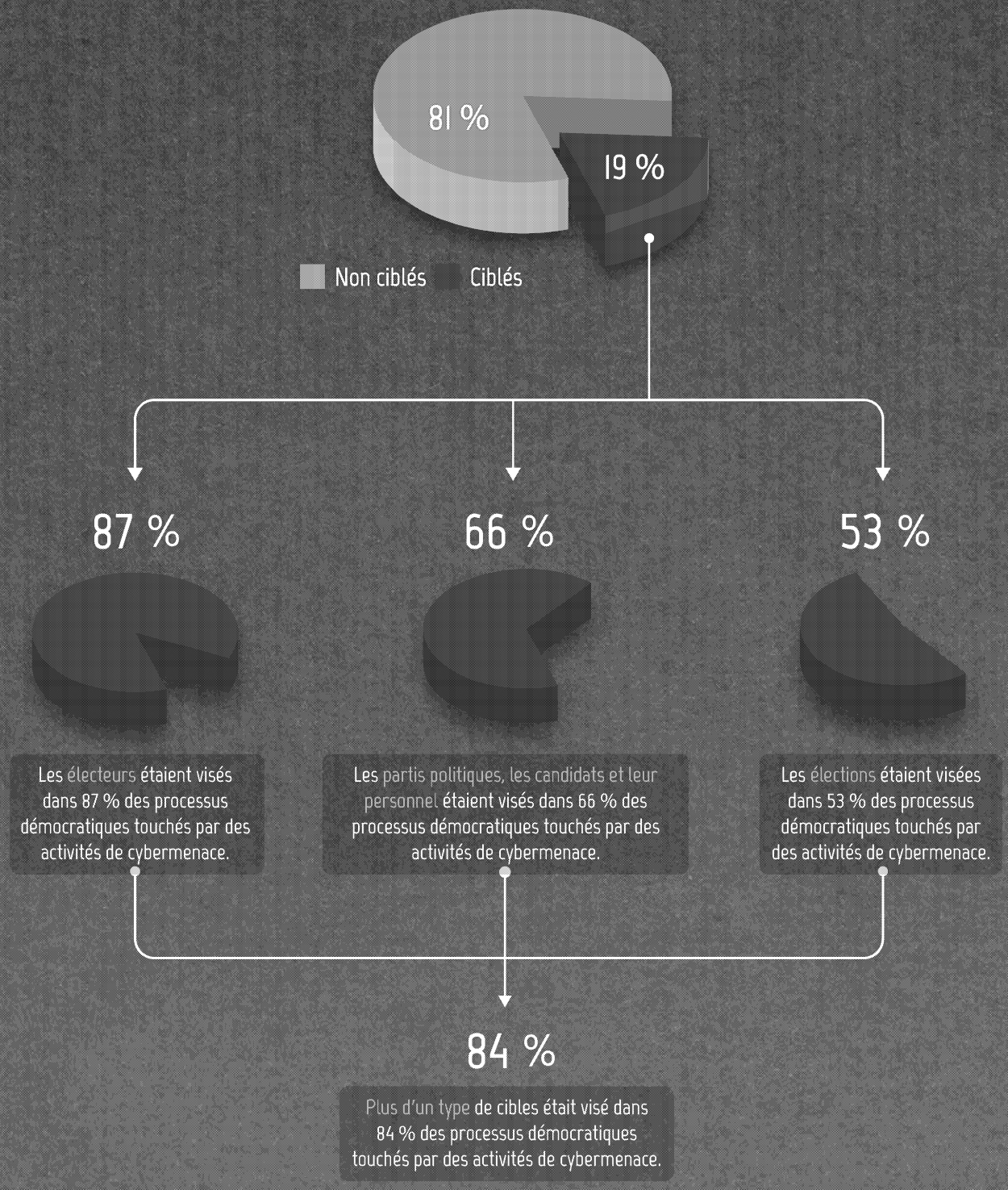
A Perturbation de sites Web liés aux élections

B Opération de piratage et de divulgation d'information

C Compromission des systèmes de vote et modification des résultats

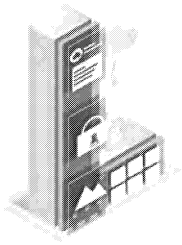
D Mise en valeur des fausses allégations selon lesquelles un candidat a profité d'une fraude électorale

FIGURE 10 | PROCESSUS DÉMOCRATIQUES LIÉS AUX ÉLECTIONS CIBLÉS PARTOUT DANS LE MONDE, 2015–2020



LE CONTEXTE CANADIEN

LES CYBERMENACES QUI PÈSENT SUR LE PROCESSUS DÉMOCRATIQUE DU CANADA



E Canada n'est victime que d'une fraction des cyberactivités observées qui visaient d'autres processus démocratiques dans le monde. 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 manipuler secrètement le résultat de vote officiel.

Par contre, pour ce qui est des élections infranationales, on adopte à certains endroits au Canada le vote en ligne, comme dans certaines municipalités de l'Ontario et de la Nouvelle-Écosse, alors qu'aux Territoires du Nord-Ouest, on permet aux électeurs absents de voter en ligne. À l'échelle nationale, on continue toutefois d'utiliser les bulletins de vote sur papier. Pour avoir un aperçu du déroulement des élections aux niveaux fédéral, provincial ou territorial et municipal au Canada, consultez la figure 11.

En outre, les membres des partis politiques nationaux et provinciaux ont voté en ligne pour choisir le chef de leur parti.[71] Cependant, les votes en ligne sont vulnérables aux auteurs de cybermenace qui pourraient vouloir modifier le résultat des votes ou semer la méfiance au sein d'un parti.

FIGURE 11 | UTILISATION DE LA TECHNOLOGIE DANS LES ÉLECTIONS AU CANADA

ORDRE DE GOUVERNEMENT	INSCRIPTION ÉLECTORALE	VOTE	DÉPOUILLEMENT DU VOTE	ANNONCE DU RÉSULTAT
FÉDÉRAL				
PROVINCIAL/ TERRITORIAL	[2]	[3] [4]	[5]	
MUNICIPAL	[6]	[7]	[8] [9]	

LÉGENDE

Le processus se fait sur papier

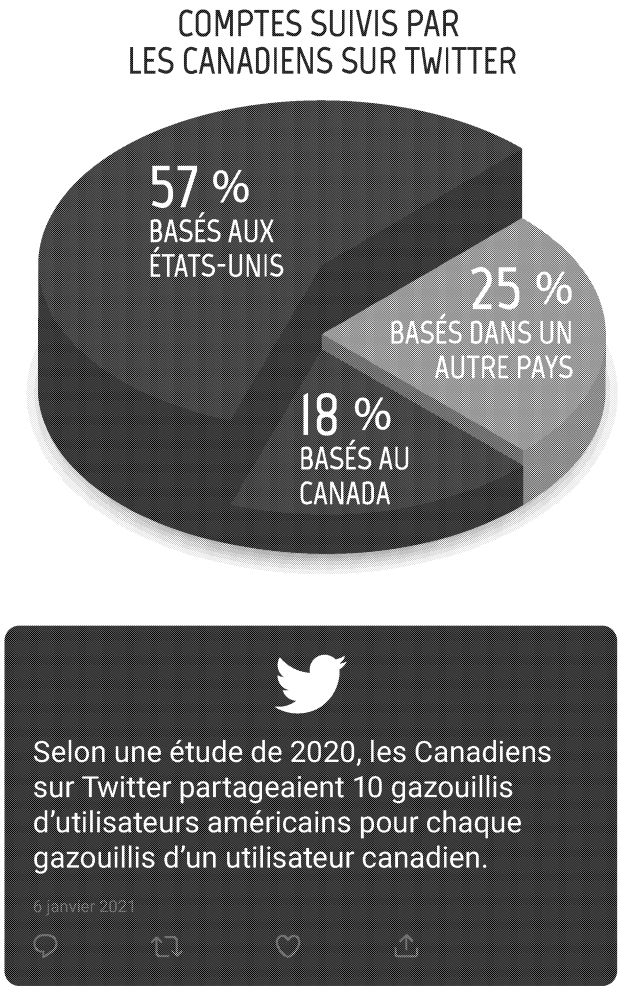
Le processus est mené au moyen d'appareils électroniques qui ne sont pas connectés à Internet régulièrement (p. ex. pour balayer les bulletins de vote papier ou stocker de l'information sous forme numérique)

Le processus est mené sur Internet (p. ex. vote en ligne)

1. Pour tous les ordres de gouvernement, les résultats non officiels sont annoncés la soirée de l'élection. Dans la plupart des cas, y compris au gouvernement fédéral, le résultat de l'élection (c'est-à-dire le résultat officiel) est certifié des jours, voire des semaines plus tard.
2. Les provinces et territoires suivants offrent l'inscription électorale en ligne : Alberta, Colombie-Britannique, Manitoba, Terre-Neuve-et-Labrador, Nouvelle-Écosse, Territoires du Nord-Ouest, Ontario, Île-du-Prince-Édouard, Saskatchewan et Yukon.
3. Le Nouveau-Brunswick utilise les registres de scrutin électroniques. La Colombie-Britannique compte les adopter ultérieurement.
4. Certains électeurs absents peuvent voter en ligne aux Territoires du Nord-Ouest.
5. Le Nouveau-Brunswick et l'Ontario utilisent des appareils électroniques pour dépouiller le vote. La Colombie-Britannique compte adopter ces appareils ultérieurement.
6. Certaines municipalités offrent l'inscription électorale en ligne.
7. Certaines municipalités en Nouvelle-Écosse et en Ontario ont recours au vote en ligne.
8. Certaines municipalités utilisent des machines pour dépouiller les bulletins de vote papier.
9. Les municipalités qui ont recours au vote en ligne dépouillent aussi le vote en ligne.

Nous sommes d'avis que le Canada, comparativement à d'autres pays, n'est pas une cible prioritaire pour les activités d'influence étrangère en ligne. Il faut toutefois noter qu'au Canada, l'écosystème des médias est étroitement lié à celui des États-Unis et d'autres alliés. Cela signifie que lorsque leurs citoyens sont ciblés, les Canadiens s'exposent à des dommages collatéraux en raison de l'influence en ligne. En 2020 et au début de 2021, nous avons pu constater à quel point la désinformation et la mésinformation croissantes aux États-Unis et dans d'autres pays alliés peuvent se répercuter sur la population canadienne.

FIGURE 12 | LES CANADIENS SUR TWITTER



Tayler Owen, et al. | Understanding vaccine hesitancy in Canada: attitudes, beliefs, and the information ecosystem | Media Ecosystem Observatory | 6 janvier 2021 | https://files.cargocollective.com/c745315/meo vaccine hesistancy.pdf

En 2019, le gouvernement du Canada a établi le Protocole public en cas d'incident électoral majeur, un mécanisme qui lui permet de communiquer avec la population canadienne de façon claire, transparente et impartiale advenant un incident qui pourrait compromettre la tenue d'élections libres et justes au pays.[72] Lors de l'élection générale de 2019, aucune menace n'a atteint le seuil élevé du Protocole relatif à l'information des Canadiens, mais le groupe chargé de prendre cette décision était prêt à intervenir, au besoin. D'autres mesures d'atténuation avaient également été adoptées, notamment pour protéger les électeurs, les partis politiques et les élections. La figure 13 contient des exemples de ces mesures.

FIGURE 13 | MESURES ADOPTÉES POUR PROTÉGER LE PROCESSUS DÉMOCRATIQUE DU CANADA

PROTOCOLE PUBLIC EN CAS D'INCIDENT ÉLECTORAL MAJEUR
- Mécanisme de communication avec la population canadienne advenant un incident qui pourrait empêcher le Canada de tenir une élection libre et juste

GROUPE DE TRAVAIL SUR LES MENACES EN MATIÈRE DE SÉCURITÉ ET DE RENSEIGNEMENTS VISANT LES ÉLECTIONS
- Composé de représentants du CST, du Service canadien du renseignement de sécurité, d'Affaires mondiales Canada et de la Gendarmerie royale du Canada

CONSEILS ET INFORMATION DU CCC
- Ligne directe avec Élections Canada
- Information à l'intention des partis politiques
- Ressources en matière de cybersécurité à l'intention du public

EFFORTS DÉPLOYÉS PAR ÉLECTIONS CANADA
- Amélioration de la posture de cybersécurité
- Surveillance de l'environnement de l'information
- Correction d'information fausse ou trompeuse au sujet du processus électoral

ENTENTES AVEC LES ENTREPRISES DE MÉDIAS SOCIAUX ET DE TECHNOLOGIE
- Déclaration du Canada sur l'intégrité électorale en ligne

LITTÉRATIE NUMÉRIQUE
- Initiative de citoyenneté numérique
- Programme de recherche en matière de citoyenneté numérique
- Projet de démocratie numérique du Forum des politiques publiques

LA COVID-19 ET L'AVENIR DU PROCESSUS DÉMOCRATIQUE DU CANADA

Élections Canada a pris des mesures pour augmenter la capacité et la commodité du système de vote postal pour satisfaire à une éventuelle augmentation de la demande et a indiqué qu'une hausse du volume de bulletins de vote postaux pourrait retarder l'annonce du résultat d'une élection.[73] Certains des changements apportés, comme de permettre à davantage d'électeurs de s'inscrire en ligne pour voter par la poste ou d'adopter des moyens de reconnaissance optique de caractères pour faciliter la lecture de certaines pièces d'identité, augmentent l'exposition aux cybermenaces. Cependant, ils sont fondés sur des systèmes déjà en place, font l'objet de processus rigoureux de mise à l'essai et de validation avant d'être adoptés et prévoient une solution de rechange faisant appel à des humains au besoin. Tout bien considéré, nous sommes d'avis que ces changements ne modifient pas de façon importante la cybermenace qui pèse sur le processus démocratique du Canada, d'autant plus que celui-ci n'est pas une cible prioritaire comparativement à d'autres pays et qu'une vaste gamme de mesures d'atténuation sont en place pour défendre les élections au Canada.

Les changements apportés au processus électoral du Canada en raison de la COVID-19, comme le recours accru au vote par la poste et les changements aux bureaux de scrutin, offrent de nouvelles possibilités d'influence étrangère en ligne, c'est-à-dire qu'ils donnent aux auteurs de cybermenace l'occasion de diffuser de la fausse information sur les processus électoraux et les résultats. Selon nous, il est très probable qu'on assiste, à la prochaine élection fédérale, à la dissémination de fausse information qui tisserait un lien entre le vote par la poste et la fraude électorale. Toutefois, nous croyons que ces faux messages seront moins présents et influents que lors des élections américaines de 2020.

Le CCC a instauré des mesures pour contrer les tentatives frauduleuses de se faire passer pour le gouvernement du Canada en ligne. Depuis mars 2020, le CCC travaille avec des partenaires pour fermer plus de 8600 sites Web, comptes de médias sociaux et serveurs de courrier électronique qui représentent frauduleusement le gouvernement du Canada.

Comme l'indique l'*ECN 2020*, la COVID-19 a forcé de nombreuses organisations à adopter le travail à distance, ce qui entraîne des vulnérabilités additionnelles. Le personnel d'Élections Canada travaille aussi de la maison et l'organisme offre de la formation en ligne liée à l'élection. Malgré tout, nous croyons qu'il est peu probable que de l'information sensible appartenant à Élections Canada soit compromise par des auteurs de cybermenace ou que des cyberactivités ébranlent les infrastructures essentielles de vote. Comme nous l'avons déjà mentionné, l'élection fédérale du Canada se fait sur papier et est protégée par des mesures de défense robustes pour assurer la légitimité du résultat.

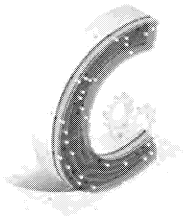
ÉTUDE DE CAS : ÉLECTIONS PROVINCIALES AU CANADA PENDANT LA PANDÉMIE DE COVID-19

En 2020, les provinces du Nouveau-Brunswick, de la Nouvelle-Écosse, de la Colombie-Britannique et de la Saskatchewan ont tenu des élections pendant la pandémie de COVID-19. Bien que les quatre provinces aient enregistré une faible baisse du taux de participation, elles ont reçu un nombre record de votes par la poste et d'inscriptions en ligne. Chacune d'elles a modifié le processus de vote pour que les électeurs puissent voter en toute sécurité, par exemple en mettant en place des mesures de santé publique et de nettoyage dans les bureaux de scrutin, en ajoutant des jours de vote et des bureaux de scrutin, en offrant aux électeurs et aux communautés à risque des occasions de voter plus sécuritaires et accessibles et en faisant en sorte que les électeurs incapables de se rendre dans un bureau de scrutin puissent quand même enregistrer leur bulletin de vote. Les quatre provinces ont également guidé les partis politiques et les candidats sur la façon de mener une campagne sécuritaire en période de pandémie. Plusieurs partis politiques ont tenu des rassemblements virtuels, ont eu davantage recours à la publicité numérique et postale et ont compté énormément sur la sollicitation par téléphone.[74] Les candidats ont aussi fait campagne en personne en respectant les règles de distanciation physique.[75] Malgré l'utilisation accrue des outils technologiques et de l'espace en ligne, rien n'indique que des campagnes sophistiquées d'influence étrangère en ligne ou des cyberactivités ont été menées contre les électeurs, les partis politiques ou les élections en tant que telles.

Si la prochaine élection fédérale canadienne a lieu avant la fin de la pandémie de COVID-19, il est presque certain que les partis politiques et les candidats mèneront davantage d'activités de campagne sur Internet et utiliseront plus d'outils en ligne qu'auparavant. Nous croyons que ces activités feront très vraisemblablement l'objet de cybermenace. Toutefois, selon nous, il est très improbable que cette cybermenace s'inscrive dans une campagne sophistiquée menée précisément contre un parti politique ou un candidat.

Conformément à ce que nous avons présenté dans *Le point sur les cybermenaces contre le processus démocratique du Canada en 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 en ligne contre des élections fédérales futures. 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 la prochaine élection fédérale. Par contre, nous considérons qu'il est improbable pour l'instant que le Canada soit visé par une campagne d'ingérence étrangère de la même ampleur que l'activité parrainée par un État et menée contre les élections américaines

CONCLUSION



COMPARATIVEMENT à d'autres pays, le Canada n'est pas une cible prioritaire de cybermenaces dirigées contre des processus démocratiques. 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 la prochaine élection fédérale même si elles ne seront probablement pas de la même ampleur que celles vécues aux États-Unis.

La pandémie de COVID-19 a transformé les processus électoraux et modifié la tenue d'élections; ces changements pourraient perdurer après la pandémie. Il est à noter que certains des changements ont augmenté l'exposition du processus démocratique aux menaces. La COVID-19 a aussi créé de nouveaux messages que les auteurs de menace peuvent utiliser pour miner la soi-disant légitimité d'une élection ou affaiblir la confiance dans les institutions démocratiques, comme celui qui établit faussement un lien entre les votes par la poste et la fraude électorale.

La présente évaluation porte sur l'influence étrangère en ligne contre les processus démocratiques, mais il est important de noter que les auteurs de cybermenace étrangers peuvent exploiter les faussetés qui se propagent dans les médias sociaux et l'écosystème informationnel canadien pour se livrer secrètement à de la désinformation.

Le *Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections* du gouvernement du Canada, qui compte des représentants du CST, du Service canadien du renseignement de sécurité, d'Affaires mondiales Canada et de la Gendarmerie royale du Canada, continue d'aider le gouvernement à évaluer les menaces étrangères qui pèsent sur le processus électoral du Canada et à prendre les mesures nécessaires pour les contrer.

La page Web *Protection de la démocratie* brosse un portrait de l'ensemble des mesures prises par le gouvernement du Canada pour protéger les élections et les institutions démocratiques, entre autres le Plan pour protéger la démocratie canadienne.

Le CCC offre des avis et des conseils en matière de cybersécurité à tous les partis politiques majeurs, entre autres au moyen du *Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales*, et travaille en étroite collaboration avec Élections Canada pour protéger son infrastructure. Il a aussi publié les deux documents suivants : *Conseils en matière de cybersécurité à l'intention des organismes électoraux* et *Guide de cybersécurité à l'intention des organismes électoraux*.

Nous encourageons d'ailleurs les Canadiens et les Canadiennes à consulter les *Conseils ciblés sur la cybersécurité non classifié applicables durant la pandémie de COVID-19*. Dans le cadre de sa campagne *Pensez cybersécurité*, le CST continuera de publier des avis et des conseils pertinents pour sensibiliser les Canadiennes et les Canadiens à la cybersécurité et leur montrer les mesures qu'ils peuvent prendre pour optimiser leur sécurité en ligne.

NOTES DE FIN

1 **Partenaires et organisations** | *Affaires mondiales Canada* | 27 mars 2020 | *https://www.international.gc.ca/world-monde/international_relations-relations_internationales/partnerships_organizations-partenariats_organisations.aspx?lang=fra*

2 Simon Kemp | **Digital 2021 : Canada** | *DataReportal* | 9 février 2021 | *https://datareportal.com/reports/digital-2021-canada*

Enquête canadienne sur l'utilisation de l'Internet | *Statistique Canada* | 29 octobre 2019 | *https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-fra.htm*

3 Tom Simonite | **What Happened to the Deepfake Threat to the Election?** | *Wired* | 16 novembre 2020 | *https://www.wired.com/story/what-happened-deepfake-threat-election*

4 Tim Huwang | **Deepfakes - Primer and Forecast** | *NATO Strategic Communications Centre of Excellence* | mai 2020 | *https://stratcomcoe.org/publications/deepfakes-primer-and-forecast/42*

5 Tom B. Brown, et al | **Language Models are Few-Shot Learners** | *OpenAI* | 22 juillet 2020 | *https://arxiv.org/abs/2005.14165*

6 Max Weiss | **Deepfake Bot Submissions to Federal Public Comment Websites Cannot Be Distinguished from Human Submissions** | *Journal of Technology Science* | 17 décembre 2019 | *https://techscience.org/a/2019121801*

7 **Foreign Threats to the 2020 US Federal Elections** | *National Intelligence Council* | 10 mars 2021 | *https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf*

8 **The Long Fuse: Misinformation and the 2020 Election** | *Election Integrity Partnership* | 2021 | *https://www.eipartnership.net/report*

9 Gordon Pennycook et David G. Rand | **Research note: Examining false beliefs about voter fraud in the wake of the 2020 Presidential Election** | *Harvard Kennedy School* | 11 janvier 2021 | *https://misinforeview.hks.harvard.edu/article/research-note-examining-false-beliefs-about-voter-fraud-in-the-wake-of-the-2020-presidential-election*

10 **Global overview of COVID-19: Impact on elections** | *International Institute for Democracy and Electoral Assistance* | consulté le 19 février 2021 | *https://www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections*

11 **Featured Elections Held and Mitigation Measures Taken During COVID-19** | *International Foundation for Electoral Systems* | 21 octobre 2020 | *https://www.ifes.org/sites/default/files/elections_held_and_mitigating_measures_taken_during_covid-19.pdf*

Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 septembre 2020 | *https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic*

Vote by Mail: International Practice During COVID-19 | *International Foundation for Electoral Systems* | 28 octobre 2020 | *https://www.ifes.org/publications/vote-mail-international-practice-during-covid-19*

12 Erik Asplund, et al | **Elections and COVID-19: How election campaigns took place in 2020** | *International Institute for Democracy and Electoral Assistance* | 2 février 2020 | *https://www.idea.int/news-media/news/elections-and-covid-19-how-election-campaigns-took-place-2020*

Julian E. Barnes | **Schiff Sees Rise in Russian Disinformation as Trump Attacks Mail-In Voting** | *New York Times* | 29 septembre 2020 | *https://www.nytimes.com/2020/09/29/us/politics/mail-in-voting-russian-disinformation.html*

13 Josh Margolin et Lucien Bruggeman | **Russia is 'amplifying' claims of mail-in voter fraud, intel bulletin warns** | *ABC News* | 3 septembre 2020 | *https://abcnews.go.com/Politics/russia-amplifying-claims-mail-voter-fraud-intel-bulletin/story?id=72799959*

Kirsten Korosec | **'Stay home' robocalls on Election Day prompt warnings, investigation** | *TechCrunch* | 3 novembre 2020 | *https://techcrunch.com/2020/11/03/stay-home-robocalls-on-election-day-prompt-warnings-investigation/?guccounter=1*

14 **Le journalisme, « les fausses nouvelles » (fake news) et désinformation : un manuel pour l'enseignement et la formation du journalisme** | *Organisation des Nations Unies pour l'éducation, la science et la culture* | consulté le 25 février 2021 | https://fr.unesco.org/fightfakenews

Claire Wardle et Hossein Derakhshan | **Information disorder: Toward an interdisciplinary framework for research and policy making** | *Council of Europe* | 27 septembre 2017 | https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

15 **Le journalisme, « les fausses nouvelles » (fake news) et désinformation : un manuel pour l'enseignement et la formation du journalisme** | *Organisation des Nations Unies pour l'éducation, la science et la culture* | consulté le 25 février 2021 | https://fr.unesco.org/fightfakenews

Claire Wardle et Hossein Derakhshan | **Information disorder: Toward an interdisciplinary framework for research and policy making** | *Council of Europe* | 27 septembre 2017 | https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

16 Scott Brennen, Felix Simon, Philip N. Howard, et Rasmus Kleis Nielsen | **Types, sources, and claims of COVID-19 misinformation** | *Reuters Institute* | 7 avril 2020 | https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation

17 Serena Giusti et Elisa Piras (édit.) | **Democracy and Fake News: Information Manipulation and Post-Truth Politics** | *Routledge* | 2020 | https://doi.org/10.4324/9781003037385

18 **Uganda elections 2021: Facebook shuts government-linked accounts** | *BBC News* | 11 janvier 2021 | https://www.bbc.com/news/world-africa-55623722

19 Stephen Kafeero | **Uganda has cut off its entire internet hours to its election polls opening** | *Quartz Africa* | 13 janvier 2021 | https://qz.com/africa/1957137/uganda-cuts-off-internet-ahead-of-election-polls-opening

Stephen Kafeero | **Uganda has shut down all social media two days ahead of a tense election** | *Quartz Africa* | 12 janvier 2021 | https://qz.com/africa/1956188/uganda-shuts-social-media-ahead-of-election-army-out-in-streets

20 Felicia Anthonio, Carolyn Tackett, Leanna Garfield, et Sage Cheng | **How internet shutdowns are threatening 2020 elections, and what you can do about it** | *Access Now* | 15 octobre 2020 | https://www.accessnow.org/internet-shutdowns-2020-elections

Miguel Angel Lara Otaola | **Annex: Internet restriction during elections** | *ACE Electoral Knowledge Network* | consulté le 25 février 2021 | https://aceproject.org/ace-en/topics/me/annex/case-studies/internet-restriction-during-elections

21 Samantha Bradshaw, Hannah Bailey, et Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 janvier 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

22 Samantha Bradshaw, Hannah Bailey, et Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 janvier 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

23 Samantha Bradshaw, Hannah Bailey, et Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 janvier 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

Andy Carvin | **Operation Carthage: How a Tunisian company conducted influence operations in African presidential elections** | *Atlantic Council* | 5 juin 2020 | https://www.atlanticcouncil.org/wp-content/uploads/2020/06/operation-carthage-002.pdf

McKay Coppins | **The Billion-Dollar Disinformation Campaign to Reelect the President** | *The Atlantic* | mars 2020 | https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530

24 Samantha Bradshaw, Hannah Bailey, et Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 janvier 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

25 Craig Timberg et Tony Romm | **Facebook shuts down Israel-based disinformation campaigns as election manipulation increasingly goes global** | *Washington Post* | 16 mai 2019 | https://www.washingtonpost.com/technology/2019/05/16/facebook-shuts-down-israel-based-disinformation-campaigns-election-manipulation-increasingly-goes-global

26 **The Making of QAnon: A Crowdsourced Conspiracy** | *Bellingcat* | 7 janvier 2021 | *https://www.bellingcat.com/news/americas/2021/01/07/the-making-of-qanon-a-crowdsourced-conspiracy*

27 Brenna Owen | **Canada not immune to QAnon as pandemic fuels conspiracy theories, experts say** | *CTV News* | 22 décembre 2020 | *https://www.ctvnews.ca/sci-tech/canada-not-immune-to-qanon-as-pandemic-fuels-conspiracy-theories-experts-say-1.5226762*

Matthew Remski | **When QAnon Came to Canada** | *The Walrus* | 3 décembre 2021 | *https://thewalrus.ca/when-qanon-came-to-canada*

Melanie Smith | **Interpreting Social Qs: Implications of the Evolution of QAnon** | *Graphika* | 24 août 2020 | *https://graphika.com/reports/interpreting-social-qs-implications-of-the-evolution-of-qanon*

28 Un rapport du Soufan Center présenté en 2021 fait état des liens qu'entretiennent la Russie, la Chine, l'Iran et l'Arabie Saoudite avec QAnon. Cela dit, un débat est en cours quant à sa méthodologie | Jason Blazakis, et al | **Quantifying the Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon** | *The Soufan Center* | avril 2021 | *https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon*

David Gilbert | **No, Russia and China Didn't 'Weaponize' QAnon. It's a Homegrown Nightmare** | *Vice* | 22 avril 2021 | *https://www.vice.com/en/article/pkby9z/no-russia-and-china-didnt-weaponize-qanon-its-a-homegrown-nightmare*

29 Joseph Menn | **QAnon received earlier boost from Russian accounts on Twitter, archives show** | *Reuters* | 2 novembre 2020 | *https://www.reuters.com/article/us-usa-election-qanon-cyber-idUSKBN27I18I*

30 Joseph Menn | **Russian-backed organizations amplifying QAnon conspiracy theories, researchers say** | *Reuters* | 24 août 2020 | *https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T*

31 Shayan Sardarizadeh | **US election 2020: Twitter removes Iranian accounts disrupting debate** | *BBC News* | 1 octobre 2020 | *https://www.bbc.com/news/election-us-2020-54373314*

32 Joseph Menn | **Russian-backed organizations amplifying QAnon conspiracy theories, researchers say** | *Reuters* | 24 août 2020 | *https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T*

33 Jen Kirby | **US intelligence officials say Iran and Russia obtained voter registration information to interfere in election** | *Vox* | 21 octobre 2020 | *https://www.vox.com/2020/10/21/21527784/iran-russia-fbi-ratcliffe-voter-registration-emails*

34 Sheera Frenkel | **A Freelance Writer Learns He Was Working for the Russians** | *New York Times* | 2 septembre 2020 | *https://www.nytimes.com/2020/09/02/technology/peacedata-writer-russian-misinformation.html*

Jack Stubbs | **Duped by Russia, freelancers ensnared in disinformation campaign by promise of easy money** | *Reuters* | 2 septembre 2020 | *https://www.reuters.com/article/us-usa-election-facebook-russia-idUSKBN25T35E*

35 Stephan Heblich | **The effect of the internet on voting behavior** | *IZA World of Labor* | consulté le 25 février 2021 | *https://wol.iza.org/articles/effect-of-internet-on-voting-behavior/long*

Nic Newman, et al | **Reuters Institute Digital News Report 2020** | *Reuters Institute* | juin 2020 | *https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf*

36 Chris Meserole | **How misinformation spreads on social media—And what to do about it** | *Brookings Institution* | 9 mai 2018 | *https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it*

Jack Nicas | **How YouTube Drives People to the Internet's Darkest Corners** | *Wall Street Journal* | 7 février 2018 | *https://www.wsj.com/articles/how-youtube-drives-viewers-to-the-internets-darkest-corners-1518020478*

Trudeaus and Trudeaun'ts – memes polarize in Canadian elections | *Digital Forensic Research Lab* | 19 novembre 2019 | *https://medium.com/dfrlab/trudeaus-and-trudeaunts-memes-have-an-impact-during-canadian-elections-4c842574dedc*

Katherine J. Wu | **Radical ideas spread through social media. Are the algorithms to blame?** | *PBS NOVA* | 28 mars 2019 | *https://www.pbs.org/wgbh/nova/article/radical-ideas-social-media-algorithms*

37 Julia Alexander | **YouTube claims its crackdown on borderline content is actually working** | *The Verge* | 3 décembre 2019 | *https://www.theverge.com/2019/12/3/20992018/youtube-borderline-content-recommendation-algorithm-news-authoritative-sources*

Julia Alexander | **YouTube introducing changes to give people more control over recommended videos** | *The Verge* | 26 juin 2019 | *https://www.theverge.com/2019/6/26/18759840/youtube-recommendation-videos-homepage-changes-algorithm-harmful-content*

Josh Constine | **Facebook will change algorithm to demote "borderline content" that almost violates policies** | *TechCrunch* | 15 novembre 2018 | *https://techcrunch.com/2018/11/15/facebook-borderline-content*

Ronald J. Deibert | **Reset: Reclaiming the Internet for Civil Society** | *House of Anansi Press* | 2020

Kaveh Waddell | **On Social Media, Only Some Lies Are Against the Rules** | *Consumer Reports* | 13 août 2020 | *https://www.consumerreports.org/social-media/social-media-misinformation-policies*

Queenie Wong, Andrew Morse, et Richard Nieva | **Here's how social media companies are fighting election misinformation** | *CNet* | 7 novembre 2020 | *https://www.cnet.com/news/heres-how-social-media-companies-are-fighting-election-misinformation*

38 Kevin Roose | **'Shut the Site Down,' Says the Creator of 8chan, a Megaphone for Gunmen** | *New York Times* | 4 août 2019 | *https://www.nytimes.com/2019/08/04/technology/8chan-shooting-manifesto.html*

39 Ben Nimmo | **Russian Narratives on Election Fraud** | *Election Integrity Partnership* | consulté le 25 février 2021 | *https://www.eipartnership.net/rapid-response/russian-narratives-on-election-fraud*

40 **When Twitter Bans Extremists, GAB Puts Out the Welcome Mat** | *Anti-Defamation League* | 11 mars 2019 | *https://www.adl.org/blog/when-twitter-bans-extremists-gab-puts-out-the-welcome-mat*

41 **Step into My Parler** | *Graphika* | 1er octobre 2020 | *https://graphika.com/reports/step-into-my-parler*

42 Nicole Hong | **WeChat, Wild Rumors and All, Is Their Lifeline. Washington mai End That** | *New York Times* | 5 octobre 2020 | *https://www.nytimes.com/2020/10/05/nyregion/us-wechat-ban.html*

Paul Mozur | **Forget TikTok. China's Powerhouse App is WeChat, and Its Power Is Sweeping** | *New York Times* | 4 septembre 2020 | *https://www.nytimes.com/2020/09/04/technology/wechat-china-united-states.html*

Joe Fitzgerald Rodriguez, Shannon Lin, et Jessica Huseman | **Misinformation Image on WeChat Attempts to Frighten Chinese Americans Out of Voting** | *ProPublica* | 2 novembre 2020 | *https://www.propublica.org/article/misinformation-image-on-wechat-attempts-to-frighten-chinese-americans-out-of-voting*

Yaqiu Wang | **WeChat Is a Trap for China's Diaspora** | *Human Rights Watch* | 14 août 2020 | *https://www.hrw.org/news/2020/08/14/wechat-trap-chinas-diaspora*

Jeanne Whalen | **Chinese censorship invades the U.S. via WeChat** | *Washington Post* | 7 janvier 2021 | *https://www.washingtonpost.com/technology/2021/01/07/wechat-censorship-china-us-ban*

43 Harrison Mantas | **Growing usage of encrypted messaging apps could make it harder to combat misinformation** | *Poynter* | 14 janvier 2021 | *https://www.poynter.org/fact-checking/2021/growing-usage-of-encrypted-messaging-apps-could-make-it-harder-to-combat-misinformation*

44 Kyle Daly et Sarah Fischer | **The online far right is moving underground** | *Axios* | 12 janvier 2021 | *https://www.axios.com/the-online-far-right-is-moving-underground-e429d45d-1b30-46e0-82a3-6e240bf44fef.html*

45 Jasmine Garsd | **WhatsApp's privacy features make it a hotbed for COVID-19 hoaxes** | *Marketplace* | 23 mars 2020 | *https://www.marketplace.org/2020/03/23/misinformation-about-covid19-spread-whatsapp*

46 Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 septembre 2020 | *https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic*

47 Jocelyn Woolbright | **Election Cybersecurity: Protecting the 2020 U.S. Elections** | *Cloudflare* | 17 août 2020 | https://blog.cloudflare.com/election-cybersecurity-preparing-for-the-2020-u-s-elections

48 Devin Coldewey | **Trump's campaign website hacked by cryptocurrency scammers** | *TechCrunch* | 27 octobre 2020 | https://techcrunch.com/2020/10/27/trumps-campaign-website-hacked-by-cryptocurrency-scammers

49 Axel F. | **Emotet Makes Timely Adoption of Political Elections Lures** | *Proofpoint* | 1er octobre 2020 | https://www.proofpoint.com/us/blog/threat-insight/emotet-makes-timely-adoption-political-and-elections-lures

50 Katie Shepherd | **Racist trolls hijacked a Zoom town hall to hurl slurs at Connecticut's first Black congresswoman** | *Washington Post* | 14 octobre 2020 | https://www.washingtonpost.com/nation/2020/10/14/jahana-hayes-zoom-racial-slurs

Byron Tau | **Scammers, hackers and spies hit trail** | *Politico* | 7 juillet 2014 | https://www.politico.com/story/2014/07/campaign-technology-data-security-voter-information-108585

51 **Federal Liberal leadership race: Countdown to the vote** | *CityNews* | 1er avril 2013 | https://toronto.citynews.ca/2013/04/01/federal-liberal-leadership-race-countdown-to-the-vote

Ryan Van Horne | **Nova Scotia Liberal Party opens up leadership voting to all members** | *CTV News* | 14 septembre 2020 | https://atlantic.ctvnews.ca/nova-scotia-liberal-party-opens-up-leadership-voting-to-all-members-1.5104224

52 Janosch Delcker | **Cyber threat looms large over German election** | *Deutche Welle* | 6 mai 2021 | https://www.dw.com/en/cyber-threat-looms-large-over-german-election/a-56775960

53 **Election Considerations in the Pacific During an Infodemic** | *International Foundation for Electoral Systems* | 20 juillet 2020 | https://www.ifes.org/news/election-considerations-pacific-during-infodemic

Joe Biden hosts drive-in campaign rallies amid coronavirus pandemic ahead of US election | *ABC News* | 19 octobre 2020 | https://www.abc.net.au/news/2020-10-19/joe-biden-rally-drive-in-us-election-votes-donald-trump/12781206

A look at other Canadian elections that took place during the COVID-19 pandemic | *CityNews* | 15 janvier 2021 | https://ottawa.citynews.ca/national-news/a-look-at-other-canadian-elections-that-took-place-during-the-covid-19-pandemic-3266403

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 décembre 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

54 Benjamin Barber | **Deep canvassing effort in Georgia aims to flip the U.S. Senate** | *Facing South* | 17 décembre 2020 | https://www.facingsouth.org/2020/12/deep-canvassing-effort-georgia-aims-flip-us-senate

B.C.'s virtual COVID-19 election campaign lacks human touch: expert | *CityNews* | 9 octobre 2020 | https://ottawa.citynews.ca/national-news/bcs-virtual-covid-19-election-campaign-lacks-human-touch-expert-2784083

Kendall Karson et Benjamin Siegel | **2020 Democratic National Convention Viewer's Guide: Biden anchored in Delaware, a virtual nomination and history to be made** | *ABC News* | 17 août 2020 | https://abcnews.go.com/Politics/2020-democratic-national-convention-viewers-guide-biden-anchored/story?id=72234720

Lisa Mascaro | **To door knock or not? Campaigning for Congress in COVID era** | *AP News* | 14 septembre 2020 | https://apnews.com/article/senate-elections-health-elections-philadelphia-campaigns-94c06fe50821979d6b4280968178e5aa

Marianna Sotomayor | **Biden's first virtual event encounters technological glitches** | *NBC News* | 14 mars 2020 | https://www.nbcnews.com/politics/meet-the-press/blog/meet-press-blog-latest-news-analysis-data-driving-political-discussion-n988541/ncrd1158951#blogHeader

Trudeau takes questions in Liberal party's first-ever virtual fundraiser | *CTV News* | 10 septembre 2020 | https://www.ctvnews.ca/politics/trudeau-takes-questions-in-liberal-party-s-first-ever-virtual-fundraiser-1.5100439

2020 Convention November 7 | *Green Party of Ontario* | consulté 1er mars 2021 | https://gpo.ca/convention2020

55 **Adapting to the New Normal: Political Parties During Lockdown and Social Distancing** | *International Institute for Democracy and Electoral Assistance* | 2020 | https://www.idea.int/sites/default/files/publications/adapting-to-the-new-normal-political-parties-during-lockdown-and-social-distancing.pdf

Ricki Harris | **How the Pandemic Reshaped Election Campaigns—maibe Forever** | *Wired* | 21 août 2020 | https://www.wired.com/story/pandemic-reshaped-2020-election-campaigns-democrats-republicans

56 Antonio Spinelli | **Managing Elections under the COVID-19 Pandemic: The Republic of Korea's Crucial Test** | *International Institute for Democracy and Electoral Assistance Technical Paper 2/2020* | 30 juillet 2020 | https://www.idea.int/sites/default/files/publications/managing-elections-during-pandemic-republic-korea-crucial-test.pdf

57 **Vote by Mail: International Practice During COVID-19** | *International Foundation for Electoral Systems* | 28 octobre 2020 | https://www.ifes.org/publications/vote-mail-international-practice-during-covid-19

58 Meredith Applegate, Thomas Chanussot, et Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 avril 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

59 Meredith Applegate, Thomas Chanussot, et Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 avril 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

60 **Belarus: EU imposes sanctions for repression and election falsification** | *Council of the European Union* | 2 octobre 2020 | https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/belarus-eu-imposes-sanctions-for-repression-and-election-falsification

Jordan Fabian | **Belarus Election 'Fraudulent,' White House Spokeswoman Says** | *BNN Bloomberg* | 9 septembre 2020 | https://www.bnnbloomberg.ca/belarus-election-fraudulent-white-house-spokeswoman-says-1.1491536

Statement by Minister Champagne on Belarusian presidential elections | *Global Affairs Canada* | 17 août 2020 | https://www.canada.ca/en/global-affairs/news/2020/08/statement-by-minister-champagne-on-belarusian-presidential-elections.html

61 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab.* | 1er octobre 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

62 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab* | 1er octobre 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

63 Nika Aleksejeva | **Lukashenka's regime confused by protest-driven cyber attacks** | *Digital Forensic Research Lab* | 1er octobre 2020 | https://medium.com/dfrlab/lukashenkas-regime-confused-about-belarus-cyber-partisans-activity-29f4bb530956

64 Meredith Applegate, Thomas Chanussot, et Vladlen Basysty | **Considerations on Internet Voting: An Overview for Electoral Decision-Makers** | *International Foundation for Electoral Systems White Paper* | 7 avril 2020 | https://www.ifes.org/sites/default/files/considerations_on_internet_voting_an_overview_for_electoral_decision-makers.pdf

65 **Election Considerations in the Pacific During an Infodemic** | *International Foundation for Electoral Systems* | 20 juillet 2020 | https://www.ifes.org/news/election-considerations-pacific-during-infodemic

66 **Featured Elections Held and Mitigation Measures Taken During COVID-19** | *International Foundation for Electoral Systems* | 21 octobre 2020 | https://www.ifes.org/sites/default/files/elections_held_and_mitigating_measures_taken_during_covid-19.pdf

Lindsay Maizland | **How Countries Are Holding Elections During the COVID-19 Pandemic** | *Council on Foreign Relations* | 17 septembre 2020 | https://www.cfr.org/backgrounder/how-countries-are-holding-elections-during-covid-19-pandemic

67 Tim Starks | **Looking back at a landmark law on government IT modernization** | *Politico* | 10 août 2020 | https://www.politico.com/newsletters/weekly-cybersecurity/2020/08/10/looking-back-at-a-landmark-law-on-government-it-modernization-789782

68 Samantha Bradshaw, Hannah Bailey, et Philip N. Howard | **Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation** | *Oxford Internet Institute* | 13 janvier 2021 | https://comprop.oii.ox.ac.uk/research/posts/industrialized-disinformation

69 Scott Jasper | **Why foreign election interference fizzled in 2020** | *Atlantic Council* | 23 novembre 2020 | https://www.atlanticcouncil.org/blogs/new-atlanticist/why-foreign-election-interference-fizzled-in-2020

70 **When Election Interference Fails** | *Council on Foreign Relations* | 29 janvier 2020 | https://www.cfr.org/blog/when-election-interference-fails

71 **Federal Liberal leadership race: Countdown to the vote** | *CityNews* | 1er avril 2013 | https://toronto.citynews.ca/2013/04/01/federal-liberal-leadership-race-countdown-to-the-vote

Ryan Van Horne | **Nova Scotia Liberal Party opens up leadership voting to all members** | *CTV News* | 14 septembre 2020 | https://atlantic.ctvnews.ca/nova-scotia-liberal-party-opens-up-leadership-voting-to-all-members-1.5104224

72 James Judd | **Rapport sur la Directive sur le Protocole public en cas d'incident électoral majeur** | *Gouvernement du Canada* | mai 2020 | https://www.canada.ca/fr/institutions-democratiques/services/rapports/rapport-directive-protocole-public-cas-incident-electoral-majeur.html

73 **Incidence de la COVID-19** | *Élections Canada* | 5 janvier 2021 | https://www.elections.ca/content.aspx?section=med&dir=cor&document=index&lang=f

74 Olamide Olaniyan | **BC's Party Insiders on Campaigning in a Pandemic** | *The Tyee* | 3 novembre 2020 | https://thetyee.ca/News/2020/11/03/BC-Party-Insiders-Campaigning-Pandemic

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 décembre 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

Laura Brown | **Pandemic forces New Brunswick politicians to think outside the box while campaigning** | *CTV News* | 25 août 2020 | https://atlantic.ctvnews.ca/pandemic-forces-new-brunswick-politicians-to-think-outside-the-box-while-campaigning-1.5079399

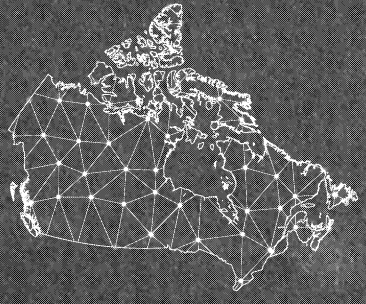
Andy Walker | **The race is on for P.E.I.'s first electoral test in COVID-19 era** | *Saltwire* | 13 octobre 2020 | https://www.saltwire.com/opinion/local-perspectives/andy-walker-the-race-is-on-for-peis-first-electoral-test-in-covid-19-era-508856

75 Olamide Olaniyan | **BC's Party Insiders on Campaigning in a Pandemic** | *The Tyee* | 3 novembre 2020 | https://thetyee.ca/News/2020/11/03/BC-Party-Insiders-Campaigning-Pandemic

David McGrane | **Campaigning in Canada during a pandemic** | *Policy Options* | 28 décembre 2020 | https://policyoptions.irpp.org/magazines/december-2020/campaigning-in-canada-during-a-pandemic

Laura Brown | **Pandemic forces New Brunswick politicians to think outside the box while campaigning** | *CTV News* | 25 août 2020 | https://atlantic.ctvnews.ca/pandemic-forces-new-brunswick-politicians-to-think-outside-the-box-while-campaigning-1.5079399

Andy Walker | **The race is on for P.E.I.'s first electoral test in COVID-19 era** | *Saltwire* | 13 octobre 2020 | https://www.saltwire.com/opinion/local-perspectives/andy-walker-the-race-is-on-for-peis-first-electoral-test-in-covid-19-era-508856



CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA