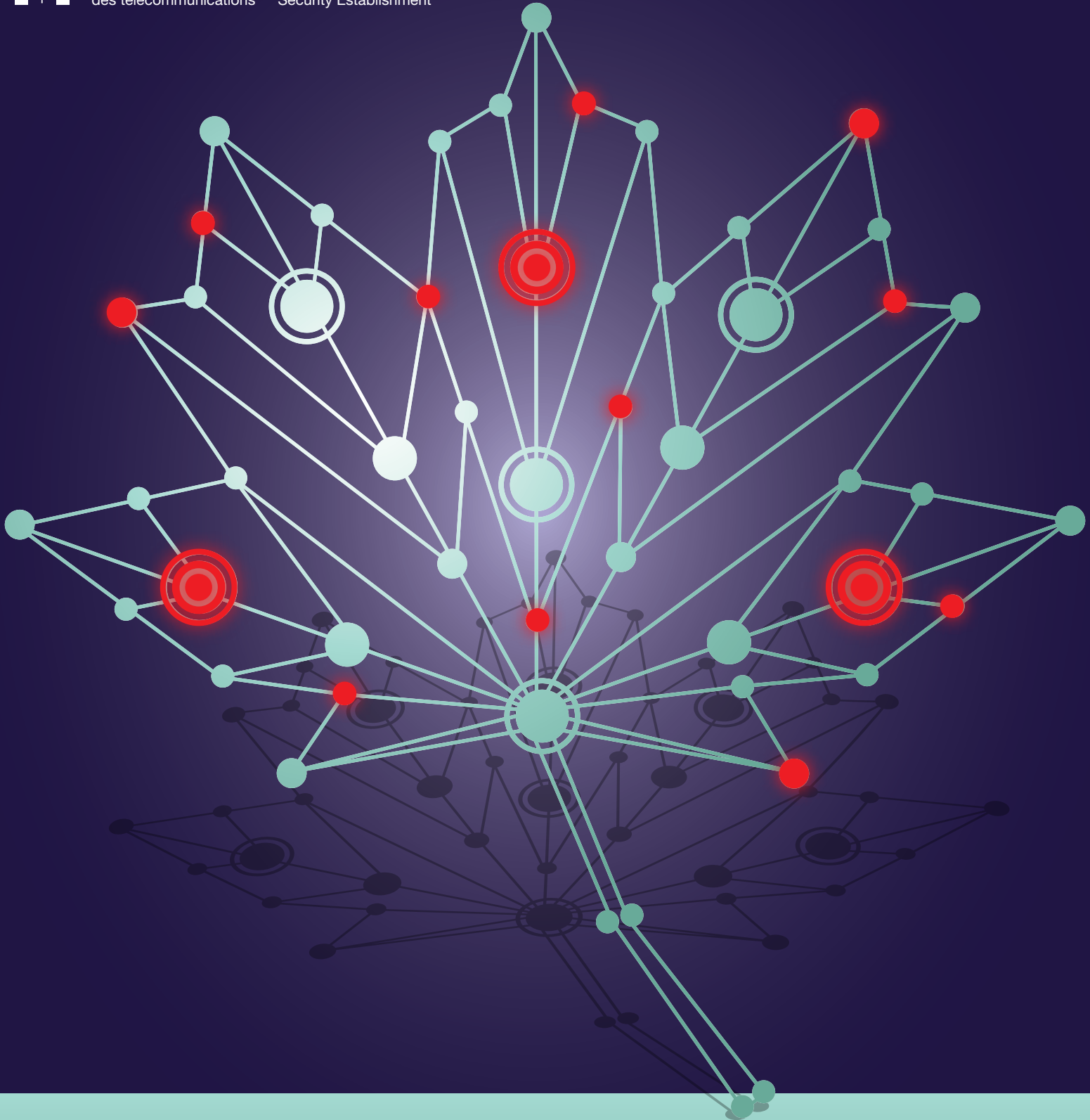




Centre de la sécurité  
des télécommunications

Communications  
Security Establishment



# CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA

Canada





## 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. Le CST fournit également de l'assistance aux organismes chargés de l'application de la loi et de la sécurité dans leurs activités légalement autorisées lorsqu'ils requièrent l'expertise unique de l'organisme.

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

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

# SOMMAIRE

Les récentes cybermenaces contre le **processus démocratique** aux États-Unis et en Europe ont suscité de nombreuses inquiétudes sur la possibilité de voir de pareilles menaces cibler le Canada. Dans le cadre de la présente évaluation, nous nous pencherons sur les **cybermenaces** ciblant le processus démocratique des ordres de gouvernement fédéral, provincial, territorial et municipal au Canada. Nous limiterons notre analyse du processus démocratique à ses trois aspects les plus ciblés par les adversaires : les élections, les partis politiques et les politiciens, ainsi que les médias.

Pour mieux comprendre le contexte de la menace, le CST a examiné les cybermenaces qui ont ciblé les processus démocratiques du Canada et d'autres pays dans le monde au cours des dix dernières années. Dans la présente évaluation, nous examinerons les cybercapacités des adversaires du Canada et la manière dont ils s'en servent pour exercer une influence sur un processus démocratique. Nous fournirons notre évaluation des cybermenaces qui ciblent les processus démocratiques, au Canada et dans le reste du monde, et des cybermenaces susceptibles de cibler le processus démocratique en 2019 (c.-à-d. les élections fédérales de 2019, les partis politiques, les politiciens et les médias qui joueront un rôle dans les élections).

## FAITS SAILLANTS

- On constate de plus en plus de cybermenaces contre les processus démocratiques aux quatre coins du monde, et le Canada n'est pas à l'abri. Le processus démocratique qui s'est déroulé lors des élections fédérales de 2015, au Canada, a été ciblé par une cybermenace peu sophistiquée<sup>1</sup>. Il est très probable que les auteurs de cette cybermenace étaient des hacktivistes et des cybercriminels. De plus, les détails entourant les incidents les plus graves ont fait l'objet de reportages dans plusieurs médias canadiens<sup>2</sup>.
- Un petit nombre d'États-nations sont derrière la majorité des cybermenaces contre les processus démocratiques du monde entier. Nous sommes d'avis que ces adversaires disposent presque certainement d'imposantes capacités contre les processus démocratiques.
- Toutefois, à ce jour, nous n'avons pas encore constaté l'utilisation de cybercapacités par des États-nations visant à influencer le processus démocratique du Canada pendant des élections. Nous croyons qu'en 2019, cette situation pourrait être la même ou changer, selon la perception qu'auront les États-nations adversaires des politiques nationales et étrangères du Canada ainsi qu'en fonction de l'ensemble des politiques adoptées par les candidats aux élections fédérales de 2019.
- Nous nous attendons à ce que de nombreux groupes d'hacktivistes déploient des cybercapacités en vue d'influencer le processus démocratique lors des élections fédérales qui auront lieu en 2019. Nous croyons que la majorité de ces activités seront de faible complexité, mais nous nous attendons à ce que certaines activités d'influence soient bien planifiées et ciblent plus d'un aspect du processus démocratique.

- ⊙ En ce qui a trait au processus démocratique fédéral du Canada, nous estimons que les partis politiques, les politiciens et les médias sont plus vulnérables aux cybermenaces et aux opérations d'influence que les activités entourant les élections à proprement parler. Ceci s'explique par le fait que le scrutin s'effectue avec des bulletins de vote en papier et par les mesures juridiques, procédurales et liées aux technologies de l'information mises en place par Élections Canada.
- ⊙ D'après notre évaluation, nous croyons que la menace contre les processus démocratiques infranationaux (c.-à-d. les processus provincial, territorial et municipal) demeurera très probablement à un faible niveau, mais que certains partis politiques, politiciens, activités électorales et médias infranationaux sont plus susceptibles d'être la cible de menaces émanant d'États-nations et d'hacktivistes.
- ⊙ Au cours des cinq dernières années, on a remarqué une hausse, à l'échelle mondiale, des cybermenaces contre les processus démocratiques. À ce jour, en 2017, les processus démocratiques d'environ 13 p. 100 des pays qui ont organisé des élections fédérales ont été ciblés par des cybermenaces.
- ⊙ On constate, à l'échelle mondiale, que les adversaires ciblent les trois aspects du processus démocratique (c.-à-d. les élections, les partis politiques et les politiciens, et les médias traditionnels et les médias sociaux).

  - Ces adversaires utilisent leurs cybercapacités pour nuire aux **élections** en entravant la participation des électeurs, en trafiquant les résultats des élections et en volant les renseignements personnels des électeurs.
  - Ils utilisent leurs cybercapacités contre les **partis politiques et les politiciens** en effectuant des activités de cyberespionnage à des fins de coercition, de manipulation et pour discréditer publiquement certaines personnes.
  - Ils utilisent leurs cybercapacités contre les **médias traditionnels et les médias sociaux** pour y faire de la désinformation et de la propagande, et manipuler les opinions des électeurs.
- ⊙ Nous croyons qu'il est très probable que les cybermenaces contre les processus démocratiques seront plus nombreuses et plus complexes au cours de l'année à venir, et peut-être à plus long terme, et ce, à l'échelle mondiale. Voici pourquoi :

  - de nombreuses cybercapacités sont accessibles au public, abordables et faciles à utiliser;
  - l'expansion rapide des médias sociaux et le déclin des sources d'information faisant autorité rendent la tâche plus facile aux adversaires qui utilisent leurs cybercapacités et d'autres méthodes pour faire des campagnes de désinformation et de propagande dans les médias et influencer les électeurs;
  - les organismes électoraux se tournent de plus en plus vers Internet pour améliorer leurs services aux électeurs, ce qui rend ces services plus vulnérables aux cybermenaces;
  - il est difficile de prévenir les cybermenaces, car elles sont habituellement difficiles à détecter, à attribuer et à contrer en temps opportun; par conséquent, l'équation coûts-avantages est plus favorable pour les auteurs de cybermenaces que pour ceux qui s'efforcent de les contrer;
  - enfin, les réussites des auteurs de cybermenaces enhardissent nos adversaires qui répètent leurs exploits et inspirent d'autres auteurs à imiter leurs comportements.





# TABLE DES MATIÈRES

⊙ À PROPOS DU PRÉSENT DOCUMENT .....	<b>9</b>
⊙ INTRODUCTION.....	<b>10</b>
⊙ PROCESSUS DÉMOCRATIQUE DU CANADA .....	<b>11</b>
⊙ APERÇU DES CYBERMENACES .....	<b>12</b>
⊙ POURQUOI CIBLER LE PROCESSUS DÉMOCRATIQUE DU CANADA? .....	<b>13</b>
⊙ COMMENT LE PROCESSUS DÉMOCRATIQUE EST-IL CIBLÉ? .....	<b>14</b>
CIBLE : LES ÉLECTIONS.....	<b>15</b>
CIBLE : LES PARTIS POLITIQUES ET LES POLITICIENS.....	<b>18</b>
CIBLE : LES MÉDIAS.....	<b>20</b>
⊙ DES EXPLICATIONS AU SUJET DES CYBERMENACES.....	<b>22</b>
LES OUTILS DE L'AUTEUR DE CYBERMENACES .....	<b>23</b>
UTILISATION SOPHISTIQUÉE DES CYBERCAPACITÉS.....	<b>26</b>
ÉTUDE DE CAS : INFLUENCER L'OPINION PUBLIQUE CONTRE UN CANDIDAT .....	<b>28</b>
ÉTUDE DE CAS : CYBERESPIONNAGE CONTRE UN CANDIDAT .....	<b>30</b>
⊙ LES TENDANCES MONDIALES ET LA MENACE ENVERS LE CANADA ...	<b>31</b>
DONNÉES DE RÉFÉRENCE MONDIALES SUR LES ÉVÉNEMENTS CONNUS .....	<b>32</b>
LE CONTEXTE CANADIEN .....	<b>33</b>
⊙ CONCLUSION.....	<b>34</b>
⊙ ANNEXE A.....	<b>35</b>
⊙ NOTES EN FIN DE TEXTE .....	<b>36</b>





# À PROPOS DU PRÉSENT DOCUMENT

Le présent rapport répond à une demande de la ministre des Institutions démocratiques et comprend une évaluation des **cybermenaces** contre le processus démocratique du Canada effectuée par le Centre de la sécurité des télécommunications (CST).

## PROCESSUS D'ÉVALUATION

L'objectif de notre analyse du renseignement est d'offrir aux lecteurs des produits d'information objectifs, opportuns et d'une grande rigueur intellectuelle. Le CST effectue ses évaluations des cybermenaces en se basant sur un processus d'analyse qui comprend l'évaluation de la qualité des renseignements disponibles, l'étude de différentes explications, l'atténuation des biais et la mise en œuvre d'approches probabilistes.

Dans la présente évaluation, nous ferons la distinction entre les faits, les hypothèses et les conclusions. Nous emploierons des termes comme « selon nos évaluations » ou « nous croyons » pour communiquer les évaluations analytiques ou les jugements du CST. Nous utiliserons aussi des termes comme « possiblement », « susceptible », « probable » et « très probable » pour exprimer les probabilités (voir l'annexe A).

## SOURCES

La plupart des jugements que contient le présent rapport se basent sur un ensemble de rapports provenant de nombreuses sources et sont fondés sur les connaissances et l'expertise du CST en matière de renseignement étranger et de cybersécurité. Cependant, comme il s'agit d'un document non classifié, nous ne pouvons pas y dévoiler du renseignement classifié, ce qui compromettrait les sources et les méthodes de collecte de renseignement de l'organisme. Le CST ne peut pas révéler publiquement l'étendue de ses connaissances ou les fondements complets de ses jugements.

## PORTÉE

Le présent document traite d'une vaste gamme de cybermenaces contre les activités politiques et électorales du Canada aux ordres fédéral, provincial, territorial et municipal<sup>3</sup>. En raison de la portée de l'évaluation, nous ne nous pencherons pas sur tous les risques et vulnérabilités liés aux élections, aux partis politiques, aux politiciens et aux médias du Canada. Nous ne fournirons pas non plus une liste exhaustive des cybercapacités ou des moyens dont disposent nos adversaires pour les déployer, car les activités des cyberadversaires du Canada prendraient des centaines de pages à cataloguer<sup>4</sup>.

De plus, la prestation de conseils sur l'atténuation des cybermenaces ne s'inscrit pas dans la portée de la présente évaluation. Généralement, la plupart des cybermenaces dont nous discuterons dans la présente peuvent être atténuées grâce à la cybersécurité (p. ex. les 10 meilleures mesures de sécurité des TI du CST), à la sécurité physique et aux pratiques exemplaires en matière de continuité des activités.

*La présente évaluation des menaces se fonde sur des renseignements disponibles en date du 7 juin 2017.*





## INTRODUCTION

Les récentes activités liées aux cybermenaces contre des institutions politiques et les communications personnelles de politiciens partout dans le monde suscitent des inquiétudes par rapport à la cybersécurité du processus démocratique du Canada. Dans le présent document, nous évaluerons les cybermenaces qui ciblent le processus démocratique du Canada.

Pour mieux comprendre le contexte de la menace, le CST a étudié les cybermenaces ayant ciblé les processus démocratiques au Canada et dans le reste du monde au cours des dix dernières années. Puis, dans la présente évaluation, nous définirons comment les aspects clés du processus démocratique (c.-à-d. les élections, les partis politiques, les politiciens et les médias) sont vulnérables aux cybermenaces et aux opérations d'influence. Nous nous pencherons sur les processus démocratiques canadiens des ordres de gouvernement fédéral, provincial, territorial et municipal. Nous vous présenterons certaines cybercapacités communes et la manière dont les adversaires du Canada peuvent utiliser ces capacités pour influencer le processus démocratique. Ensuite, nous décrirons les différents types d'adversaires qui pourraient faire appel à ces cybercapacités et la menace qu'ils représentent pour le Canada.

Enfin, en combinant nos connaissances de l'histoire récente et notre compréhension des tendances liées aux cybercapacités et aux adversaires du Canada, nous évaluerons comment les cybermenaces contre le processus démocratique du Canada sont susceptibles d'évoluer.

# PROCESSUS DÉMOCRATIQUE DU CANADA

Dans la présente évaluation, nous limiterons notre analyse à trois aspects clés du processus démocratique que nos adversaires peuvent cibler : (1) les élections; (2) les partis politiques et les politiciens; et (3) les médias (voir la figure 1).

Les **élections** sont au cœur de toute démocratie. Elles permettent aux citoyens de choisir leurs représentants et leur gouvernement. Pour qu'un changement de pouvoir ait lieu de façon ordonnée et pacifique, les citoyens doivent pouvoir être assurés que les résultats d'une élection sont valides et qu'ils n'ont fait l'objet d'aucune ingérence. C'est pourquoi les élections démocratiques doivent être effectuées avec transparence et en permettant à des observateurs de vérifier chaque étape du processus.

Les **partis politiques et les politiciens** sont les institutions politiques et les personnes qui rivalisent pour être portées au pouvoir lors d'élections. Ils représentent les intérêts des électeurs et cherchent à générer du soutien envers les politiques nationales et étrangères qu'ils considèrent être dans l'intérêt supérieur des Canadiens.

Les **médias** sont le théâtre de la majorité des interactions entre les politiciens et les électeurs. On entend par les médias les médias traditionnels (p. ex. journaux, chaînes de nouvelles télévisées) et les médias sociaux.

Ces trois aspects du processus démocratique sont tellement importants que leur protection est enchâssée dans la Constitution du Canada. En effet, la *Charte canadienne des droits et libertés* garantit aux Canadiens le droit de choisir les députés qui les représenteront au Parlement au cours d'élections libres et justes. La *Charte* protège aussi le droit de liberté d'expression et de conscience des Canadiens, ce qui permet notamment aux citoyens de présenter des idées en public, de les propager et d'en débattre. De plus, la *Charte* protège expressément la liberté de la presse.

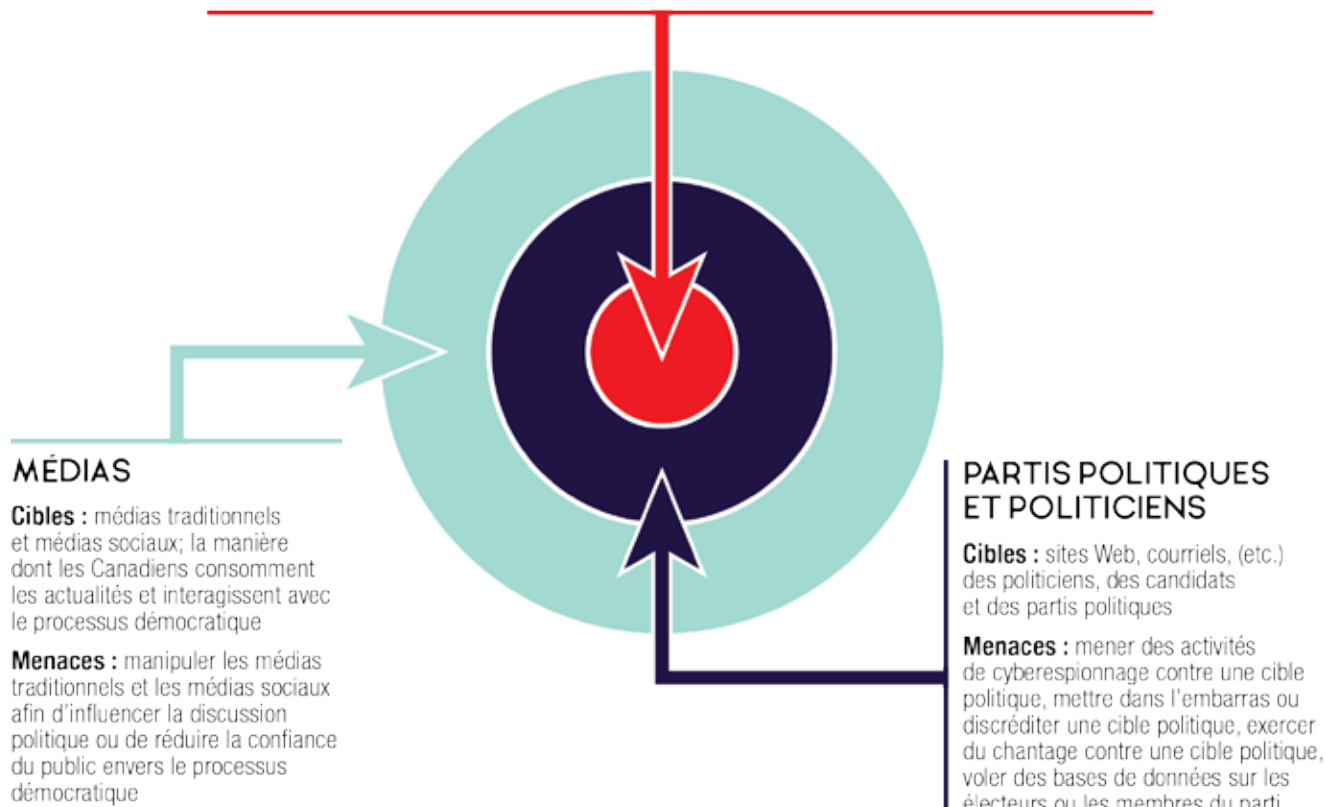
La confiance est au cœur de tous les aspects du processus démocratique. Pour que la démocratie triomphe, les citoyens doivent pouvoir être certains que le processus est juste, que les politiciens ne sont pas redevables à des intérêts étrangers ou criminels et que les médias ne sont pas influencés par des intérêts étrangers ou criminels qui tentent de manipuler l'opinion des électeurs et le résultat du processus démocratique.

FIGURE 1: Processus démocratique du Canada

## ÉLECTIONS

**Cibles :** organismes électoraux et leur infrastructure; processus de vote

**Menaces :** empêcher les électeurs de s'inscrire en ligne, empêcher les citoyens de voter, modifier les résultats des élections, voler des bases de données sur les électeurs



# APERÇU DES CYBERMENACES

L'avènement d'Internet a été accompagné d'une panoplie de nouvelles menaces contre le processus démocratique. La majeure partie du discours social lié au processus démocratique se produit désormais en ligne. On pense, entre autres, aux courriels, aux gazouillis, aux sites Web, aux bases de données, aux réseaux informatiques et à beaucoup d'autres technologies de l'information dont se servent les électeurs, les organismes électoraux, les partis politiques, les politiciens et les médias. Le Canada fait partie d'un groupe d'États de plus en plus nombreux qui doivent se défendre contre leurs adversaires qui utilisent des cybercapacités pour secrètement exercer une influence sur les trois aspects du processus démocratique.

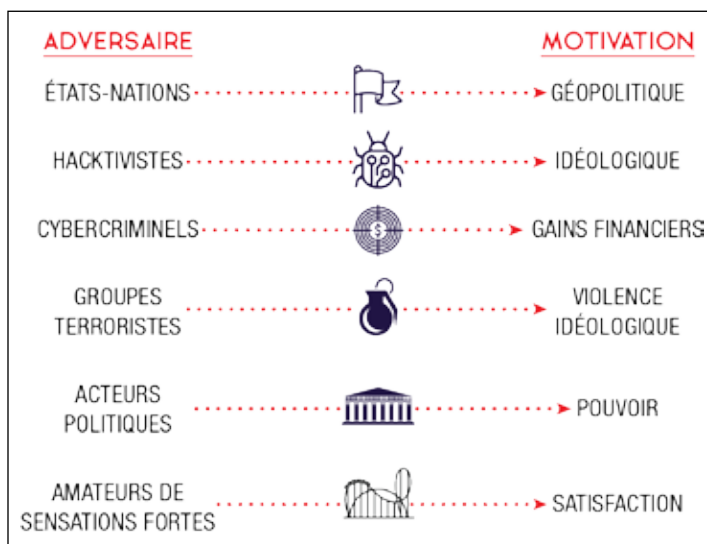
Par adversaire, on entend tout État, tout groupe ou toute personne qui a utilisé ou qui pourrait utiliser des cybercapacités pour menacer ou influencer le processus démocratique du Canada. Certains adversaires sont auteurs de **menaces stratégiques**, en ce sens qu'ils visent sciemment à influencer secrètement un processus démocratique en particulier.

D'autres adversaires ne visent pas à influencer les résultats d'un processus démocratique, mais peuvent y parvenir malgré eux : il s'agit alors de **menaces indirectes**. Souvent, les responsables des menaces indirectes ratissent large dans l'espoir d'exploiter une base de données ou un réseau non sécurisé pour des motifs financiers ou simplement pour se divertir. Le fait que leurs activités touchent le processus démocratique est une simple coïncidence.

En vue d'évaluer les menaces contre le processus démocratique, le CST a examiné les cybermenaces qui ont ciblé les processus démocratiques à l'échelle mondiale au cours des dix dernières années. On compte six catégories d'adversaires qui entreprennent des activités visant à influencer le processus démocratique ou qui ont les capacités d'y parvenir.

- ⊙ Les **États-nations** motivés par des intérêts économiques, idéologiques ou géopolitiques.
- ⊙ Les **hacktivistes** motivés par des questions idéologiques.
- ⊙ Les **cybercriminels** motivés par l'appât du gain<sup>5</sup>.
- ⊙ Les **groupes terroristes** motivés par des idéologies extrémistes et violentes.
- ⊙ Les **acteurs politiques** motivés par le désir d'être portés au pouvoir national.
- ⊙ Les **amateurs de sensations fortes** motivés par le désir de se faire une réputation ou par l'atteinte d'une satisfaction personnelle découlant d'activités de piratage réussies.

FIGURE 2 : Aperçu des adversaires qui ciblent le Canada



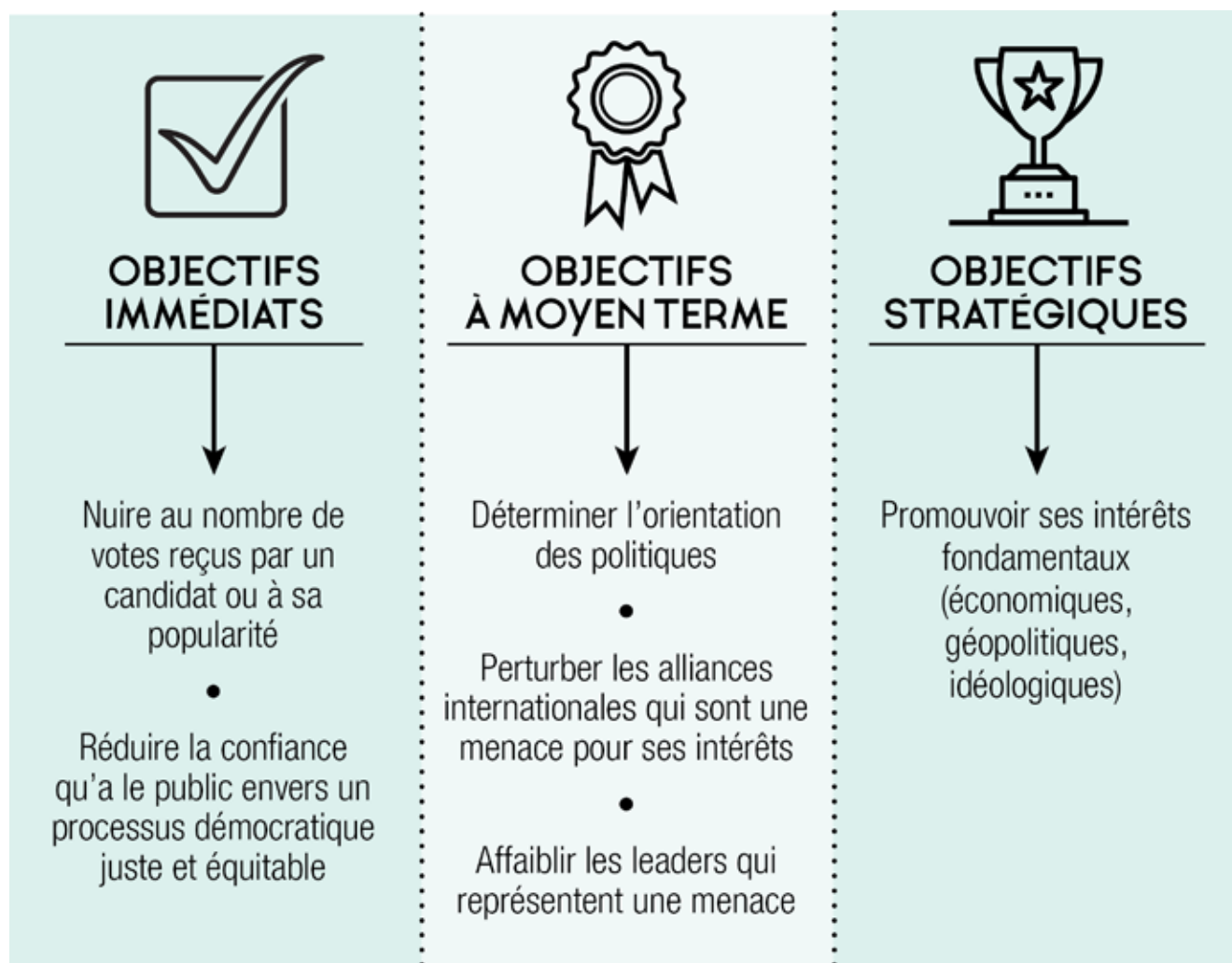
# POURQUOI CIBLER LE PROCESSUS DÉMOCRATIQUE DU CANADA?

Le Canada fait partie du G7 et de l'OTAN, et est un membre influent de la communauté internationale. Par conséquent, les choix du gouvernement fédéral du Canada en matière de déploiements militaires, d'accords commerciaux et d'investissements, de déclarations diplomatiques, d'aide étrangère ou d'immigration sont influents et percutants. Ces choix peuvent avoir une incidence sur les décisions prises par les alliés du Canada et les intérêts fondamentaux d'autres pays, de groupes étrangers et de particuliers. Les gouvernements provinciaux, territoriaux et municipaux du Canada créent aussi des politiques, dirigent les dépenses et adoptent des lois qui touchent des dizaines de millions de Canadiens et qui, dans certains cas (p. ex. politiques sur l'extraction de ressources naturelles), peuvent avoir des répercussions sur des intérêts étrangers.

Les adversaires qui ciblent le processus démocratique fédéral, provincial, territorial ou municipal à des fins stratégiques visent à concrétiser leurs intérêts primordiaux qui sont habituellement liés à la sécurité nationale, à la prospérité économique et à des objectifs idéologiques. Les cybermenaces peuvent aussi être utilisées comme des démonstrations de force ou pour dissuader d'autres États-nations.

Les adversaires peuvent chercher à modifier les résultats des élections, les choix des responsables des politiques, les relations du gouvernement avec ses partenaires étrangers et nationaux et à nuire à la réputation du Canada à l'échelle mondiale. Ils peuvent aussi tenter de saper la légitimité du concept de la démocratie et d'autres valeurs qui vont à l'encontre de leur vision idéologique du monde, à l'instar des droits et des libertés de la personne.

**FIGURE 3 :** Pourquoi les États-nations font-ils appel à des cybercapacités pour influencer les processus démocratiques de pays étrangers?





# COMMENT LE PROCESSUS DÉMOCRATIQUE EST-IL CIBLÉ?

*Dans cette section, nous expliquerons les trois aspects clés du processus démocratique du Canada et leurs vulnérabilités aux cybermenaces.*

## CIBLE : LES ÉLECTIONS

- ⊙ **Menace** : Empêcher les citoyens de s'inscrire pour voter.
- ⊙ **Menace** : Empêcher les électeurs de voter.
- ⊙ **Menace** : Trafiquer les résultats des élections.
- ⊙ **Menace** : Voler des bases de données sur les électeurs.

Les organismes électoraux fédéraux, provinciaux, territoriaux et municipaux sont responsables de l'organisation des élections partout au Canada. Les activités de ces organismes peuvent varier légèrement, cependant, toutes les élections comptent ces trois phases essentielles :

1. **L'inscription des électeurs** : on y détermine qui a le droit de voter;
2. **Le vote** : on reçoit, compte et consigne les votes;
3. **La diffusion des résultats** : on informe le public des résultats des élections.

Il y a plusieurs décennies, le processus de vote se déroulait entièrement sur papier. Mais aujourd'hui, comme le montre la figure 4, le processus du scrutin, au Canada, se déroule à la fois électroniquement et sur papier. Nous ne pouvons pas explorer les moindres détails de chaque organisme électoral canadien, mais vous trouverez ci-dessous une description globale des trois phases des élections et leurs vulnérabilités aux cybermenaces.

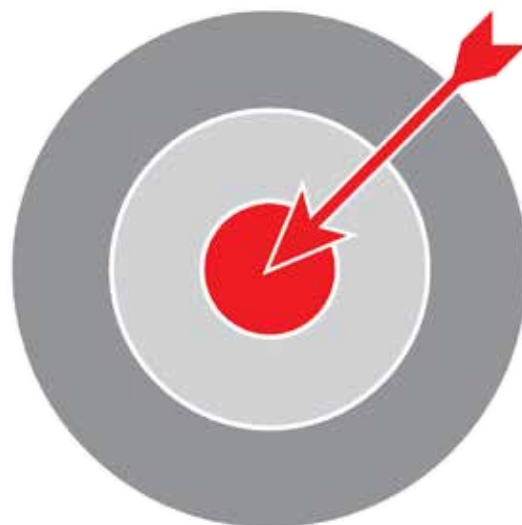






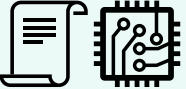










FIGURE 4 : Cible : Les élections

ORDRE DE GOUVERNEMENT	INSCRIPTIONS	VOTE	COMPTAGE	DIFFUSION DES RÉSULTATS <sup>6</sup>
Fédéral				
Provincial / Territorial				
Municipal				

LÉGENDE		
 <b>Papier</b>	 <b>Numérique</b>	 <b>Internet</b>
Le processus se déroule sur papier	Le processus se déroule à l'aide de dispositifs électroniques qui ne sont habituellement pas connectés à Internet (p. ex. pour numériser les bulletins papier ou stocker des renseignements sous forme numérique)	Le processus se déroule sur Internet (p. ex. vote en ligne)

1. Les électeurs de l'Alberta, de la Colombie-Britannique, des Territoires du Nord-Ouest, de l'Île-du-Prince-Édouard et de la Saskatchewan peuvent s'inscrire en ligne.
2. Seulement au Nouveau-Brunswick.
3. Certaines municipalités canadiennes permettent aux électeurs de s'inscrire en ligne.
4. Certaines municipalités de la Nouvelle-Écosse (36 %) et de l'Ontario (22 %) utilisent le vote en ligne.
5. Certaines municipalités utilisent des machines pour compter les bulletins de vote en papier; les votes sur Internet sont aussi comptés en ligne.
6. Les résultats non officiels sont diffusés pendant la soirée des élections. Dans la plupart des cas, les résultats des élections sont certifiés (c.-à-d. les résultats officiels) quelques jours ou semaines après la journée des élections.



## L'INSCRIPTION DES ÉLECTEURS

Toute élection comprend un processus visant à déterminer si les électeurs ont bel et bien le droit de vote. Seuls les électeurs qui répondent à des critères précis (p. ex. âge minimum, exigences liées au lieu de résidence) ont le droit de voter. Au Canada, tous les ordres de gouvernement dressent et tiennent à jour des listes d'inscriptions des électeurs<sup>6</sup>.

Si l'inscription des électeurs se déroule en ligne, les adversaires peuvent utiliser leurs cybercapacités pour tenter de polluer la base de données avec de faux fichiers d'électeurs. Ils peuvent aussi essayer de rendre le site Web inaccessible ou y inscrire de faux renseignements pour induire les électeurs en erreur. De plus, ils peuvent tenter d'effacer ou de chiffrer les données de manière à les rendre impossibles à consulter.

Toutes ces activités ont le potentiel de mettre les organismes électoraux dans l'embarras et de faire germer des doutes dans l'esprit des électeurs. Elles peuvent aussi ralentir le processus de scrutin, frustrer les électeurs ou leur donner un sentiment de répression, ce qui peut avoir une incidence sur les résultats des élections. Enfin, il est aussi possible que les bases de données sur les électeurs puissent être volées, et comme elles contiennent les renseignements personnels de millions de personnes, un tel cas représenterait une immense violation de la vie privée.

## LE VOTE

Le vote est le moment où les électeurs exercent leur droit de vote pour un candidat. La majorité des électeurs votent le jour des élections, mais ils peuvent aussi voter par anticipation ou grâce à un bulletin de vote pour électeur absent. Au Canada, les électeurs peuvent voter à l'aide de trois méthodes : bulletin papier, machine à voter ou vote par Internet<sup>7</sup>. Ensuite, après la fermeture des bureaux de vote, les votes sont comptés et les résultats sont compilés. Les bulletins de vote papier peuvent être comptés à la main ou à l'aide d'une machine électronique de comptage des votes. Les votes par Internet sont comptés électroniquement plutôt qu'à la main.

Généralement, les machines de comptage des votes et les machines à voter ne sont pas connectées à Internet, mais des adversaires possédant des capacités avancées pourraient trafiquer les machines avant qu'elles ne soient utilisées dans le cadre du scrutin. Les adversaires pourraient trafiquer les machines de manière à fausser le comptage des bulletins de vote ou à effacer les données à la fin de la soirée des élections. Le vote par Internet offre de plus nombreuses occasions de frapper aux adversaires qui peuvent utiliser leurs cybercapacités pour « remplir les urnes » ou rendre inaccessible le site Web où se déroule le vote, pour ne citer que ces deux exemples.



### **SYSTÈMES D'INSCRIPTION DES ÉLECTEURS DE L'ARIZONA ET DE L'ILLINOIS (2016)**

En juin 2016, l'Arizona a dû fermer son système d'inscription des électeurs pendant presque une semaine après que des adversaires ont tenté d'accéder au système. Puis, le mois suivant, l'organisme des élections de l'Illinois a dû fermer son site Web pendant deux semaines après avoir découvert que des dizaines de milliers de fichiers sur les électeurs (contenant par exemple des noms, adresses, numéros de permis de conduire) avaient possiblement été consultés par des adversaires<sup>8</sup>.

### **CHANGER SECRÈTEMENT LE COMPTAGE DES VOTES?**

Il existe un risque de voir des adversaires utiliser des cybercapacités pour changer secrètement le comptage des votes et ainsi modifier les résultats des élections, toutefois, d'après nos évaluations, il serait très difficile pour un adversaire d'y parvenir *si* les élections sont organisées en tenant compte des pratiques exemplaires en matière de cybersécurité et que des processus sur papier se déroulent en parallèle<sup>9</sup>. Il est généralement plus probable de voir les adversaires utiliser des cybercapacités pour perturber le processus de scrutin afin de semer le doute dans l'esprit des électeurs au sujet de l'impartialité du processus électoral.



## LA DIFFUSION DES RÉSULTATS

Dans la grande majorité des élections, on compte plus d'un seul bureau de vote. Après la fermeture des bureaux de vote, lorsque les bulletins ont été comptés, le total des voix doit être communiqué à un bureau de vote central. Dans le cadre de nombreuses élections, cette autorité centrale du scrutin fournit publiquement sur un site Web de nombreuses mises à jour sur les compilations des votes. De plus, les résultats peuvent être communiqués directement aux médias. La diffusion des résultats du comptage des votes peut être faite à la main, par téléphone ou par Internet. Si les résultats sont communiqués par Internet, des adversaires pourraient faire appel à leurs cybercapacités pour perturber ou modifier les résultats des élections pendant leur transmission.

Si l'on découvre la cybermenace à temps et si des mesures rigoureuses de sécurité sont en place (p. ex. si l'on dispose de bulletins de vote en papier que l'on peut recompter), les vrais résultats du scrutin pourront être connus. Toutefois, les délais de traitement et la confusion seraient susceptibles de réduire la confiance du public envers le processus et pourraient avoir des effets négatifs sur la capacité de la personne gagnante à gouverner. Dans le pire des cas, cette situation pourrait mener à une remise en question des résultats des élections, ce qui représenterait un important défi démocratique.



### PAYS-BAS (2017)

Les Pays-Bas ont décidé de modifier leurs procédures de scrutin au cours de leurs plus récentes élections, à la suite de possibles vulnérabilités logicielles découvertes dans les machines à compiler les votes et d'avertissements selon lesquels la Russie pourrait cibler les élections néerlandaises. Pour éliminer la possibilité de voir des adversaires perturber les élections, tous les votes ont été comptés à la main<sup>11</sup>.

Si la cybermenace passe inaperçue, les résultats des élections auront alors été secrètement modifiés pour sélectionner un candidat, ou un parti, au détriment des autres. Modifier les résultats d'élections à l'aide de cybercapacités serait ardu, mais à la portée de quelques adversaires exceptionnellement doués. La décision pour un adversaire d'essayer de modifier les résultats d'un scrutin et ses chances d'y parvenir dépendent des mesures de sécurité et des activités d'atténuation des cybermenaces intégrées au système électoral.

### GÉRER LES CYBERMENACES QUI CIBLENT LES ÉLECTIONS FÉDÉRALES DU CANADA

Les élections fédérales se déroulent encore grandement sur support papier et Élections Canada a mis en place un certain nombre de mesures juridiques, procédurales et liées aux technologies de l'information pour atténuer les cybermenaces. D'après nos évaluations, nous croyons qu'il est presque certain qu'en ce qui a trait au processus démocratique *fédéral* du Canada, les partis politiques, les politiciens et les médias sont plus vulnérables que les élections à proprement parler.



### GHANA (2016)

En décembre 2016, des adversaires ont accédé au site Web de la commission électorale centrale du Ghana, pendant que l'on procédait au comptage des voix des élections générales. Un adversaire inconnu a ensuite publié sur Twitter une fausse nouvelle affirmant que le candidat du parti sortant avait perdu les élections. Puis, la commission électorale a rétorqué, sur Twitter, que la nouvelle était fausse. Les résultats des élections n'ont pas été trafiqués, mais cet incident a su semer le doute dans l'esprit de nombreux électeurs<sup>10</sup>.



## CIBLE : LES PARTIS POLITIQUES ET LES POLITICIENS

- ⊙ **Menace** : Mener des activités de cyberespionnage contre une cible politique.
- ⊙ **Menace** : Exercer du chantage contre une cible politique.
- ⊙ **Menace** : Embarrasser ou discréditer une cible politique.
- ⊙ **Menace** : Voler ou manipuler les bases de données du parti ou celles sur les électeurs.

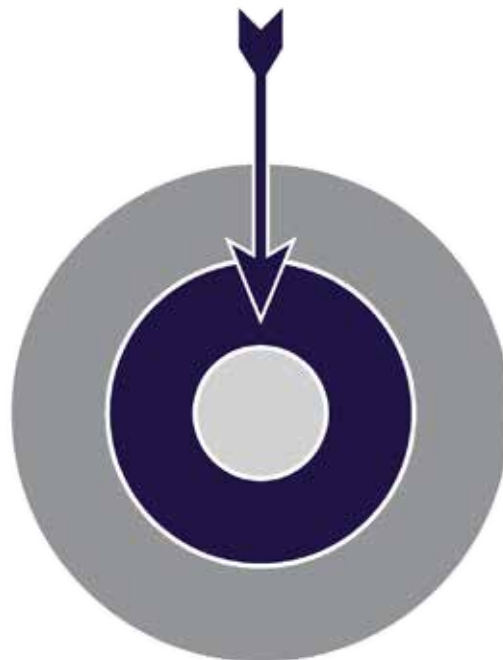
Au cours du processus démocratique, les électeurs jugent et évaluent les partis politiques et les politiciens. Les partis politiques et les politiciens essaient de persuader les électeurs à l'aide d'idées et de messages particuliers. Les adversaires peuvent essayer d'obtenir des renseignements préjudiciables pour manipuler les personnes visées ou pour influencer l'opinion publique à leur sujet.

### CYBERESPIONNAGE

Les partis politiques et les politiciens utilisent des téléphones intelligents, des dispositifs et des ordinateurs pour traiter et conserver des renseignements personnels et politiques. Ces renseignements peuvent comprendre des bases de données contenant des renseignements personnels sur des millions de Canadiens, tant des électeurs que des donateurs politiques. Les partis politiques sont autorisés à recevoir une partie du registre des électeurs de la part des organismes électoraux et ils peuvent y ajouter des renseignements supplémentaires sur les électeurs. Ces renseignements personnels et politiques ont une grande valeur et incitent les adversaires à se tourner vers le cyberespionnage pour y accéder<sup>12</sup>.

### MANIPULER UNE CIBLE OU FAIRE DU CHANTAGE : UTILISER DES RENSEIGNEMENTS OU MENACER DE LES DIVULGUER PUBLIQUEMENT

Les adversaires peuvent décider d'utiliser des renseignements personnels sur un politicien, ou sur le personnel politique, pour essayer de manipuler la personne ou de la contraindre à faire des choses. Ce type d'activités peut comprendre du chantage, des pots-de-vin ou l'orchestration de situations visant à pousser la cible à adopter des comportements inhabituels ou participer à des activités nuisibles.





## ÉTATS-UNIS (2016)

**Au cours des dernières élections présidentielles américaines, les deux principaux partis politiques ont fait l'objet de nombreuses tentatives de cyberespionnage de la part de la Russie. Des espions russes ont utilisé des cybercapacités pour accéder aux courriels de membres clés du personnel politique travaillant à la campagne du parti démocrate. Ces courriels ont ensuite été divulgués publiquement pour mettre la candidate du parti démocrate dans l'embarras<sup>13</sup>.**

### EMBARRASSER OU DISCRÉDITER UNE CIBLE : DIVULGATION DE RENSEIGNEMENTS

Les adversaires peuvent cibler des partis politiques ou des politiciens en recueillant d'abord des renseignements (comme dans l'exemple précédent), puis en divulguant publiquement ces renseignements en vue d'embarrasser ou de discréditer la cible. Parfois, les adversaires modifient les renseignements avant de les divulguer afin d'obtenir un effet plus spectaculaire. Les adversaires peuvent aussi faire appel à une tierce partie (p. ex. journaliste, WikiLeaks) pour accroître la légitimité des renseignements et pour demeurer anonymes ou masquer autant que possible leur identité. L'objectif de cette activité est d'embarrasser ou de discréditer la cible ou encore d'aider les rivaux de la cible.

### EMBARRASSER OU DISCRÉDITER UNE CIBLE : INGÉRENCE DES SITES WEB OU DES MÉDIAS SOCIAUX

Un autre moyen de discréditer un parti politique ou un politicien est d'interrompre ou compromettre sa présence sur Internet. Par exemple, les adversaires peuvent cibler le compte dans les médias sociaux ou le site Web d'une personne et le dégrader avec du contenu obscène ou de la désinformation, pour berner les électeurs et embarrasser le politicien. Selon le moment auquel survient un tel événement, ses conséquences peuvent représenter une simple nuisance ou un tournant décisif en cas d'élections serrées.

Les cybercapacités nécessaires à la mise hors service d'un site Web sont relativement simples à acheter ou à louer, ce qui permet aux adversaires qui ne possèdent pas de capacités techniques de se les procurer à peu de frais afin d'atteindre leurs objectifs malveillants.

Lorsque des adversaires essaient d'embarrasser ou de discréditer publiquement une cible, ils le font en espérant voir les renseignements qu'ils ont divulgués se retrouver dans les actualités courantes, afin de nuire à un parti politique, même si cela n'est que temporaire. Les médias peuvent être ciblés pour influencer le processus politique et l'opinion publique. Nous en parlerons plus en détail dans la section suivante.

À long terme, ce genre d'activité peut avoir de terribles effets sur la démocratie. Par exemple, des candidats qualifiés pourraient décider de ne pas se présenter à des élections en raison de la myriade de conséquences négatives que cela pourrait avoir sur leur vie personnelle et leur réputation.

### VOLER OU MANIPULER LES BASES DE DONNÉES DU PARTI OU CELLES SUR LES ÉLECTEURS

Les adversaires tentent parfois de dérober les bases de données d'un parti politique ou celles sur les électeurs, car ils peuvent en tirer un bon prix dans des parties illicites d'Internet (c.-à-d. sur le Web invisible) où l'on achète et vend constamment de grandes quantités de renseignements nominatifs personnels<sup>14</sup>.

Les adversaires peuvent aussi modifier les données ou les rendre inaccessibles (p. ex. en les chiffrant) aux partis politiques et aux politiciens qui les utilisent pour identifier les électeurs et communiquer avec eux. Les adversaires qui ciblent ainsi un parti politique peuvent influencer le cours des élections en empêchant le parti politique en question d'utiliser un important outil d'approche et d'engagement de l'électorat.

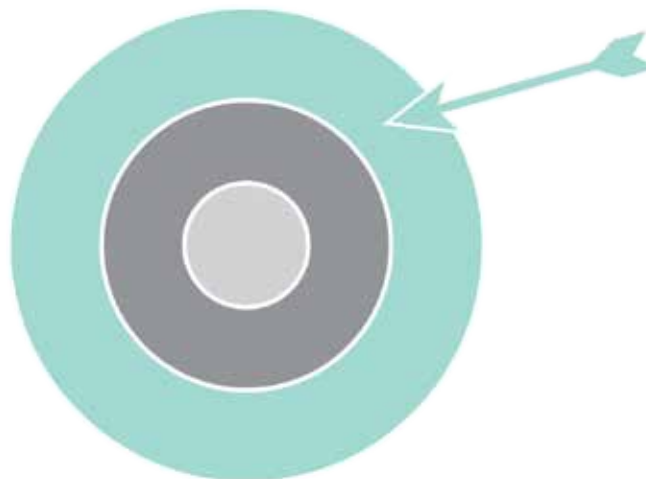


## CIBLE : LES MÉDIAS

- ⊙ **Menace** : Manipuler secrètement les médias traditionnels et les médias sociaux afin d'influencer le discours politique ou pour amenuiser la confiance du public envers le processus démocratique.

La *Charte canadienne des droits et libertés* protège la liberté d'expression et la liberté de réunion. À l'instar des autres démocraties occidentales, les médias canadiens (médias traditionnels et médias sociaux) facilitent les échanges de renseignements et d'opinions, et représentent une tribune où les idées et mouvements politiques connaissent leur essor.

Une participation politique significative au processus démocratique du Canada dépend de l'accès qu'a le public à un large éventail de renseignements et de points de vue politiques. De nos jours, les Canadiens suivent les actualités en ligne, par l'entremise des médias traditionnels, des médias sociaux, ou des deux. C'est aussi en ligne que la majorité des Canadiens font valoir leur point de vue sur les questions politiques du jour<sup>15</sup>.



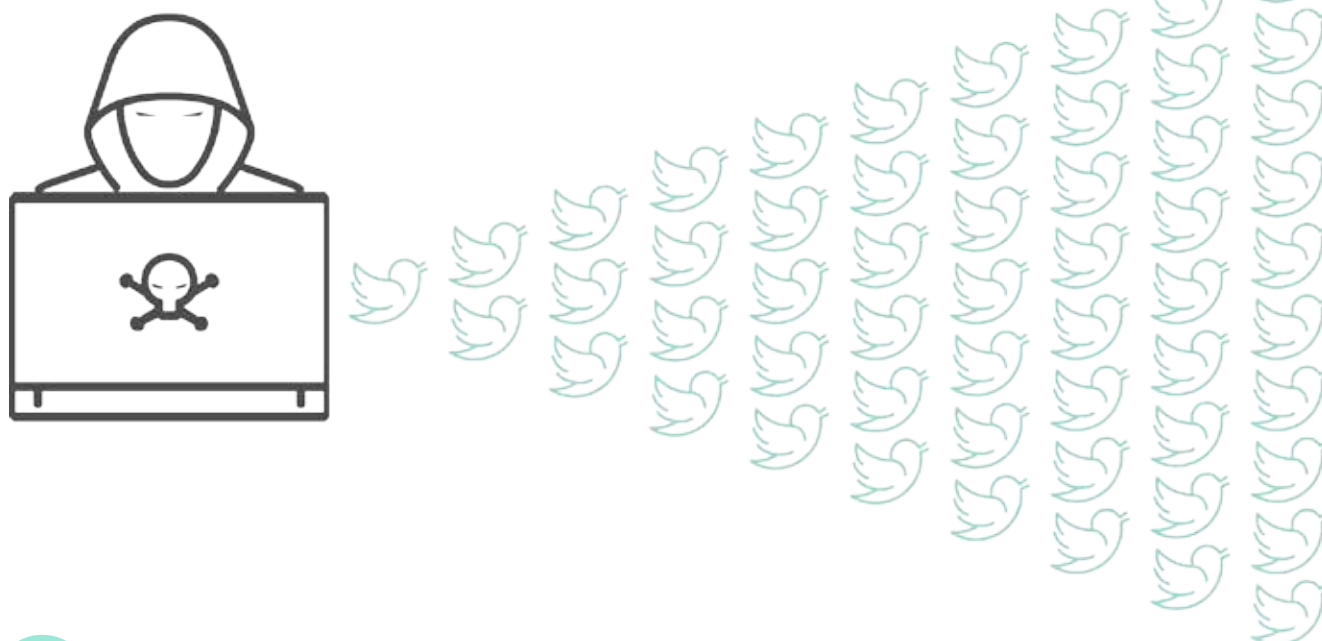
### FRANCE (2017)

D'après des reportages publiés dans les médias, le service français de renseignement croit que des réseaux de zombies (*botnet*) ont été employés dans les médias sociaux pour influencer les élections présidentielles. Certains comptes dans les médias sociaux, les mêmes qui avaient été actifs au cours des élections américaines de 2016, faisaient circuler des renseignements faux et diffamatoires contre l'une des figures majeures des élections. Dans les derniers jours des élections, des milliers de courriels liés à la campagne et appartenant à un parti politique ont été divulgués publiquement<sup>16</sup>.

Il existe la préoccupante possibilité de voir des adversaires étrangers se servir secrètement de cybercapacités pour essayer d'influencer l'environnement médiatique du Canada. Les adversaires pourraient y parvenir en ayant une excellente compréhension du fonctionnement des médias traditionnels et des médias sociaux et de la manière dont les Canadiens consomment l'information. L'existence d'une influence étrangère, ou la perception d'une telle influence pourrait avoir des répercussions sur l'opinion des électeurs et réduire la confiance que les Canadiens ont envers l'information qu'on leur présente.

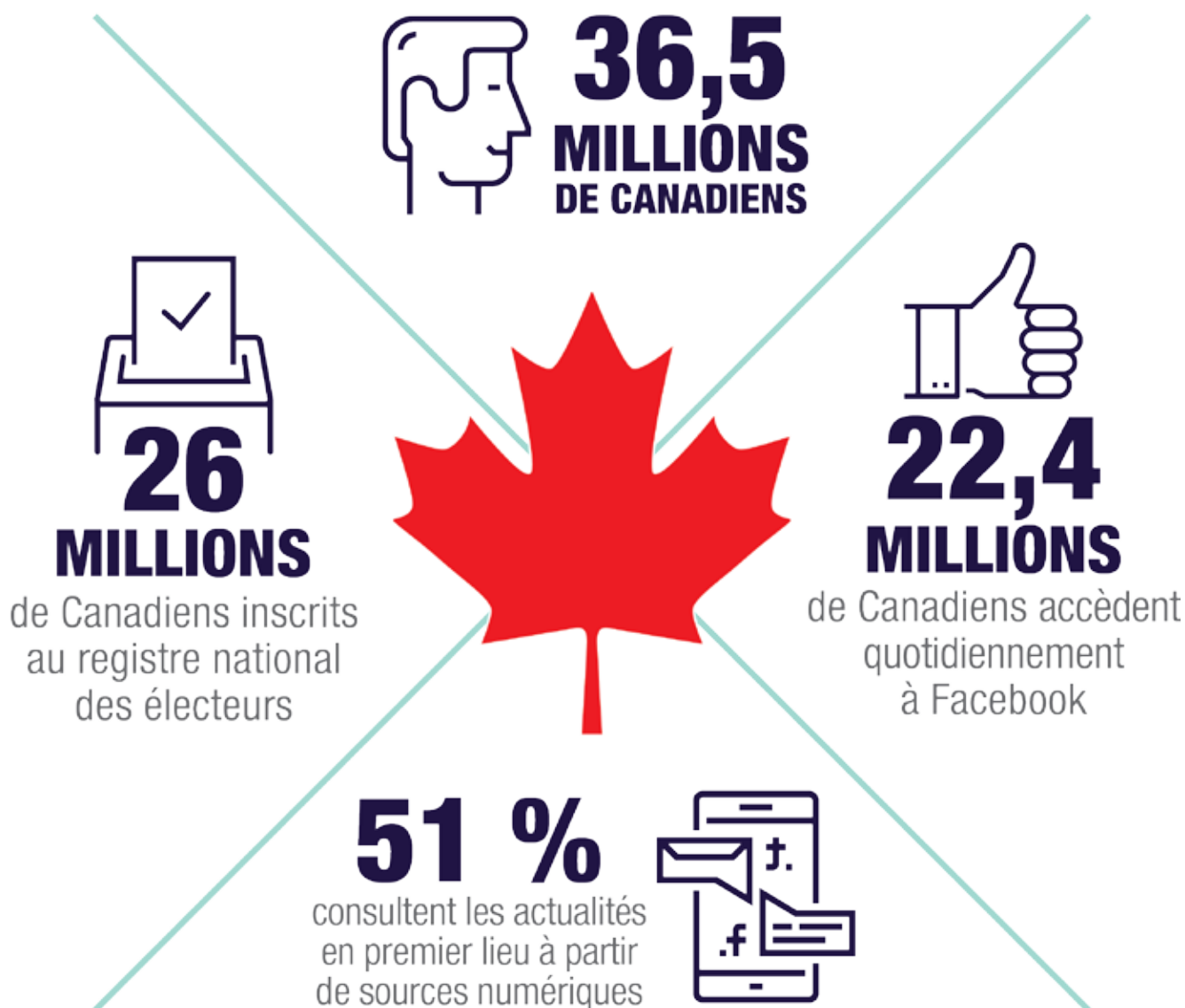
Les adversaires pourraient utiliser les médias sociaux pour répandre des mensonges et de la propagande à un large public, et ce, à très peu de frais. Les adversaires peuvent se faire passer pour des fournisseurs d'information légitimes et brouiller les frontières entre les vraies nouvelles et la désinformation. Ils peuvent y parvenir en piratant des comptes dans les médias sociaux, ou en créant des sites Web ou des comptes dans les médias sociaux qu'ils font passer pour des fournisseurs de nouvelles et d'information dignes de confiance.

FIGURE 5 : Amplification à l'aide de réseaux de zombies dans les médias sociaux



Certains adversaires se tournent vers des usines de trolls, des gens rémunérés pour diffuser de la propagande dans la section des commentaires des sites Web des médias traditionnels, ainsi que sur Twitter, Facebook et toute autre plateforme qui leur permet de rejoindre leur public. D'autres adversaires se tournent vers les réseaux de zombies, un ensemble d'ordinateurs coordonnés par un seul utilisateur. Comme l'illustre la figure 5, une seule personne peut exploiter des centaines, voire des milliers de comptes afin d'amplifier son message ou de donner artificiellement l'apparence d'un consensus public à l'appui d'un point de vue en particulier.

Les adversaires peuvent choisir parfois de soumettre les journalistes, ou toute personne à qui ils veulent nuire, à d'importantes campagnes de harcèlement et d'intimidation. Si des journalistes ou des citoyens essaient de répondre aux attaques, ils peuvent mettre en danger leur vie privée, leurs finances ou leur sécurité personnelle. Une autocensure peut alors résulter de ces démarches, ce qui aurait des conséquences désastreuses sur le discours politique et sur les enquêtes qui vont à l'encontre des intérêts des adversaires.





# DES EXPLICATIONS AU SUJET DES CYBERMENACES

*Les sections suivantes portent sur les cybercapacités et sur la façon dont les adversaires utilisent leurs cybercapacités pour nuire au processus démocratique.*

## LES OUTILS DE L'AUTEUR DE CYBERMENACES

Dans le monde d'aujourd'hui, une grande partie de ce que nous faisons, pensons et communiquons se déroule en ligne, sur nos dispositifs (p. ex. ordinateurs, téléphones intelligents, tablettes électroniques). Par conséquent, notre travail, nos renseignements personnels, nos relations, nos souvenirs, nos connaissances et nos passions sont vulnérables lorsque des personnes souhaitent accéder illégalement et sans autorisation à nos dispositifs électroniques ou à nos comptes en ligne. À l'instar des ordinateurs et d'Internet, les cybercapacités ont grandement évolué au cours des dernières décennies; elles sont non seulement plus avancées, mais aussi plus faciles à utiliser. De nos jours, de nombreuses cybercapacités très techniquement avancées et puissantes sont gratuites ou offertes à titre de service, ce qui permet à plus de gens et de groupes de s'en servir.

Les cybercapacités présentent de nombreux défis à ceux qui essaient de les contrecarrer. Lorsque l'on utilise les cybercapacités contre le processus démocratique, les activités connexes se mêlent souvent aux activités normales qui se déroulent sur Internet. Ainsi, il arrive souvent que les activités nuisibles passent inaperçues, qu'elles ne soient pas attribuées et que les coupables ne soient pas punis. Le peu de risque de conséquences négatives et les coûts très faibles de ces cybercapacités motivent grandement les adversaires à y faire appel. De plus, les adversaires profitent du fait que de plus en plus d'appareils contenant des renseignements sont connectés à Internet souvent sans mesures de sécurité appropriées.

Ce n'est pas l'objectif de la présente évaluation de définir toutes les cybercapacités que les adversaires pourraient déployer pour compromettre les courriels, les bases de données, les sites Web et les méthodes de communication dont se servent les médias, les partis politiques, les politiciens et les organismes électoraux du Canada.

Vous trouverez ci-dessous une description de quelques cybercapacités communes et efficaces qui ont été utilisées pour influencer les processus démocratiques de plusieurs pays.

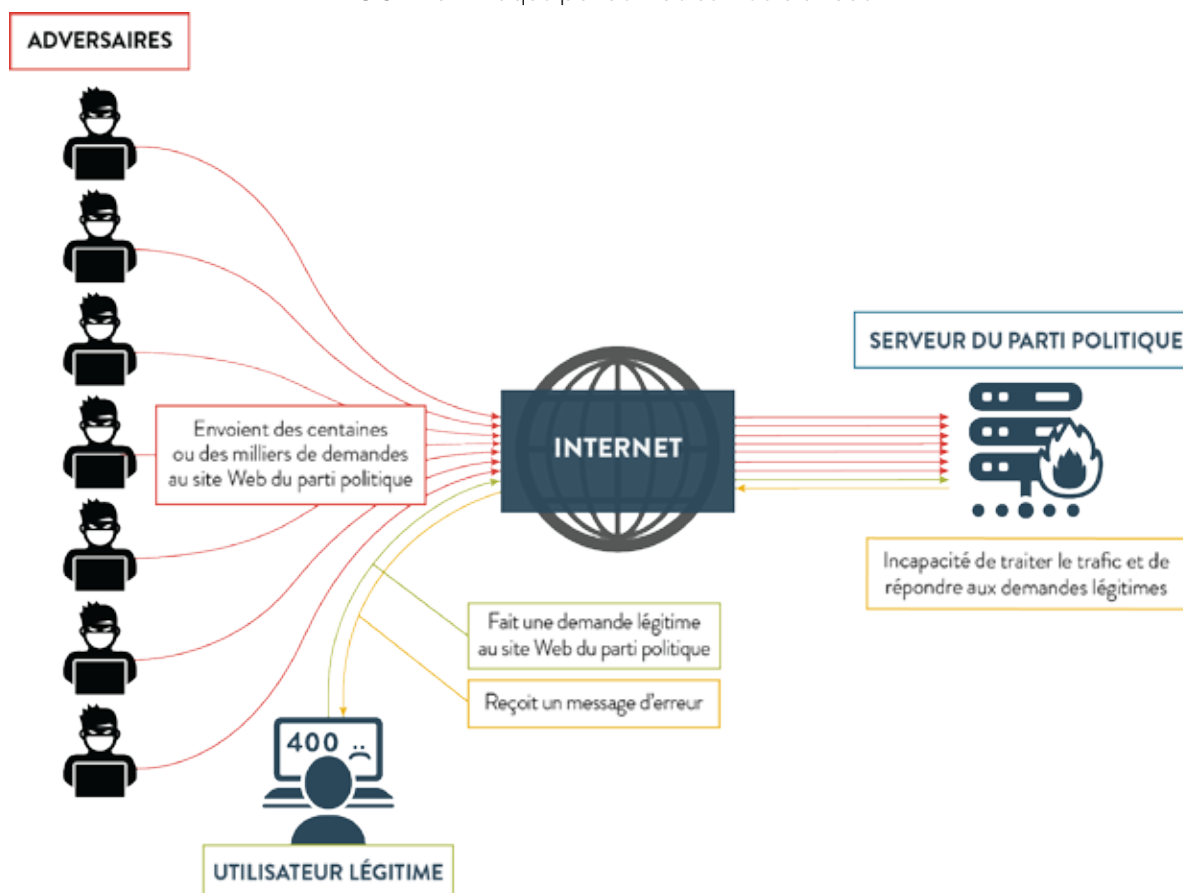
### DÉNI DE SERVICE DISTRIBUÉ (DDoS)

Une attaque par déni de service distribué (DDoS) interrompt temporairement les services d'un site Web en l'inondant de trafic réseau, ce qui le rend inutilisable. On peut obtenir cette cybercapacité gratuitement. Dans certains cas, les adversaires paient de tierces parties pour déployer ces outils à leur place.

Pour seulement 25 dollars, les adversaires peuvent lancer une attaque DDoS afin de bloquer temporairement l'accès à un site Web. Les répercussions de ce type d'attaque dépendent de l'ampleur du DDoS par rapport aux capacités de cybersécurité de l'hébergeur du site Web ou du fournisseur de service Internet. Nous estimons que de nombreux sites Web liés au processus démocratique (p. ex. sites Web personnels de politiciens) ne pourraient probablement pas résister à une grande attaque par DDoS<sup>17</sup>.

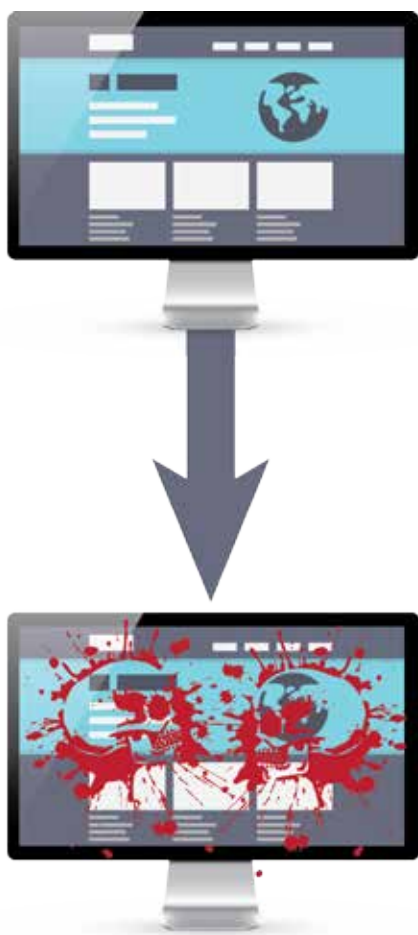
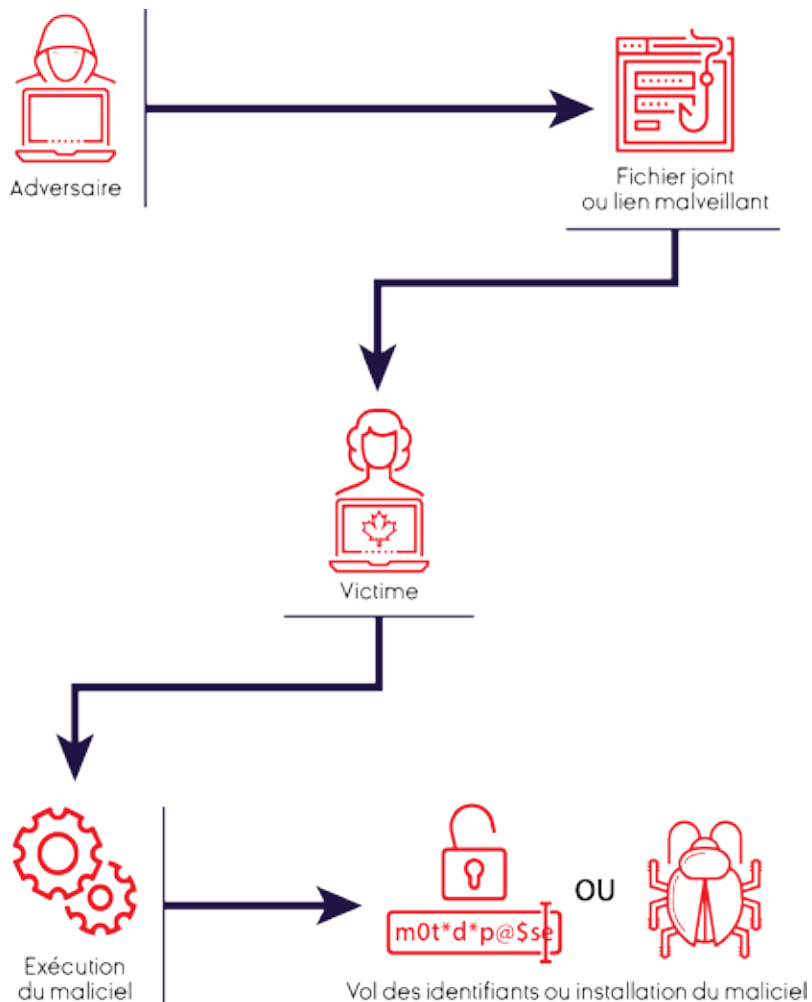
La figure 6, ci-dessous, illustre comment une attaque par DDoS se déroule. Une telle attaque peut, par exemple, empêcher des utilisateurs légitimes d'accéder au site Web d'un parti politique. Une attaque par DDoS contre le site Web d'un parti politique peut être source d'embarras ou de confusion, particulièrement si elle survient à quelques jours des élections.

FIGURE 6 : Attaque par déni de service distribué



**DÉGRADER UN SITE WEB**

Cette pratique est l'équivalent virtuel d'un graffiti. Un adversaire peut modifier le contenu d'un site Web en y ajoutant une image ou un message en vue d'embarrasser le parti politique ou l'organisme électoral, ou pour sensibiliser le public par rapport à une question en particulier.

**FIGURE 7 : Dégrader un site Web****FIGURE 8 : Harponnage****HARPONNAGE**

Le harponnage est une technique communément utilisée pour accéder aux dispositifs de la victime, à ses renseignements personnels et à ses identifiants (c.-à-d. noms d'utilisateur et mots de passe). La victime reçoit un courriel conçu sur mesure et qui semble légitime. Ensuite, la victime est invitée à cliquer sur un lien ou à ouvrir un fichier joint qui infecte son dispositif en y installant un maliciel qui permet aux adversaires d'accéder à ses renseignements personnels ou de contrôler son dispositif électronique<sup>18</sup>. Les partis politiques et les politiciens sont souvent la cible de ce genre d'activité.



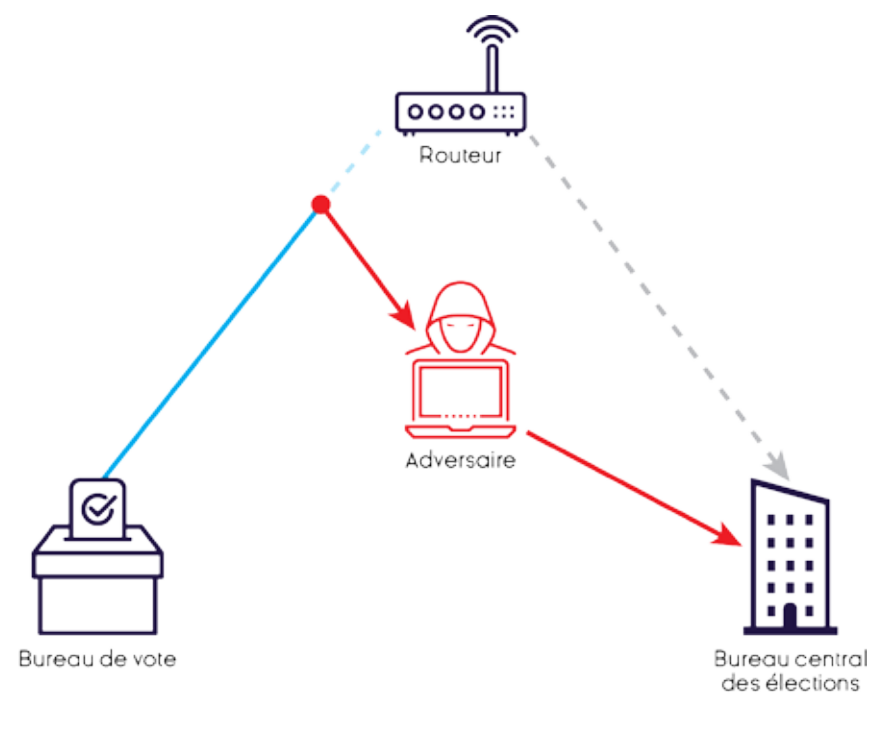




### ATTAQUE PAR L'INTERCEPTEUR (OU ATTAQUE DE L'HOMME DU MILIEU)

Une attaque par l'intercepteur déroute une communication entre deux connexions, par exemple entre un bureau de vote et le bureau central des élections, en vue d'écouter ou de modifier les informations communiquées. À l'aide de cette capacité, un adversaire pourrait modifier les résultats du comptage des voix communiqués par le bureau de vote au bureau central des élections.

FIGURE 9 : Attaque par l'intercepteur (ou attaque de l'homme du milieu)



### PENNSYLVANIE (2017)

Au début 2017, les systèmes informatiques d'un parti politique de l'état de la Pennsylvanie ont été chiffrés par un rançongiciel, les rendant inutilisables<sup>19</sup>.

### RANÇONGICIEL

Les rançongiciels sont des maliciels qui, une fois installés, interdisent l'accès aux données et forcent les victimes à payer une rançon pour retrouver l'accès à leurs données ou services. Ils sont de plus en plus communs et les victimes sont souvent choisies uniquement en fonction de la vulnérabilité de leur système, plutôt que pour des raisons stratégiques.

FIGURE 10 : Rançongiciel



1

Un adversaire crée et envoie un message qui contient un rançongiciel



2

Un membre du parti politique ouvre le pourriel et clique sur le fichier joint ou sur le lien malveillant



3

Installation du rançongiciel dans l'ordinateur



4

Les fichiers contenus dans l'ordinateur sont chiffrés



5

Un message de rançon s'affiche, indiquant le montant à payer et la date limite



6

Les victimes doivent payer la rançon en bitcoins



7

Après avoir reçu le paiement, la victime reçoit une clé de chiffrement pour déverrouiller les fichiers et y avoir accès de nouveau

## UTILISATION SOPHISTIQUÉE DES CYBERCAPACITÉS

Comme nous l'avons mentionné plus tôt, les cybercriminels et les amateurs de sensations fortes se servent de leurs cybercapacités pour des motifs économiques ou pour le plaisir qu'ils en retirent. Nous sommes davantage préoccupés par les adversaires qui utilisent des cybercapacités stratégiques avec pour objectif clair d'exercer secrètement une influence sur le processus démocratique. Comme tout autre outil, les cybercapacités peuvent être utilisées avec amateurisme ou sophistication.

Lorsque nous évaluons la sophistication de ces menaces stratégiques contre le processus démocratique, nous tenons compte d'une combinaison de trois éléments :

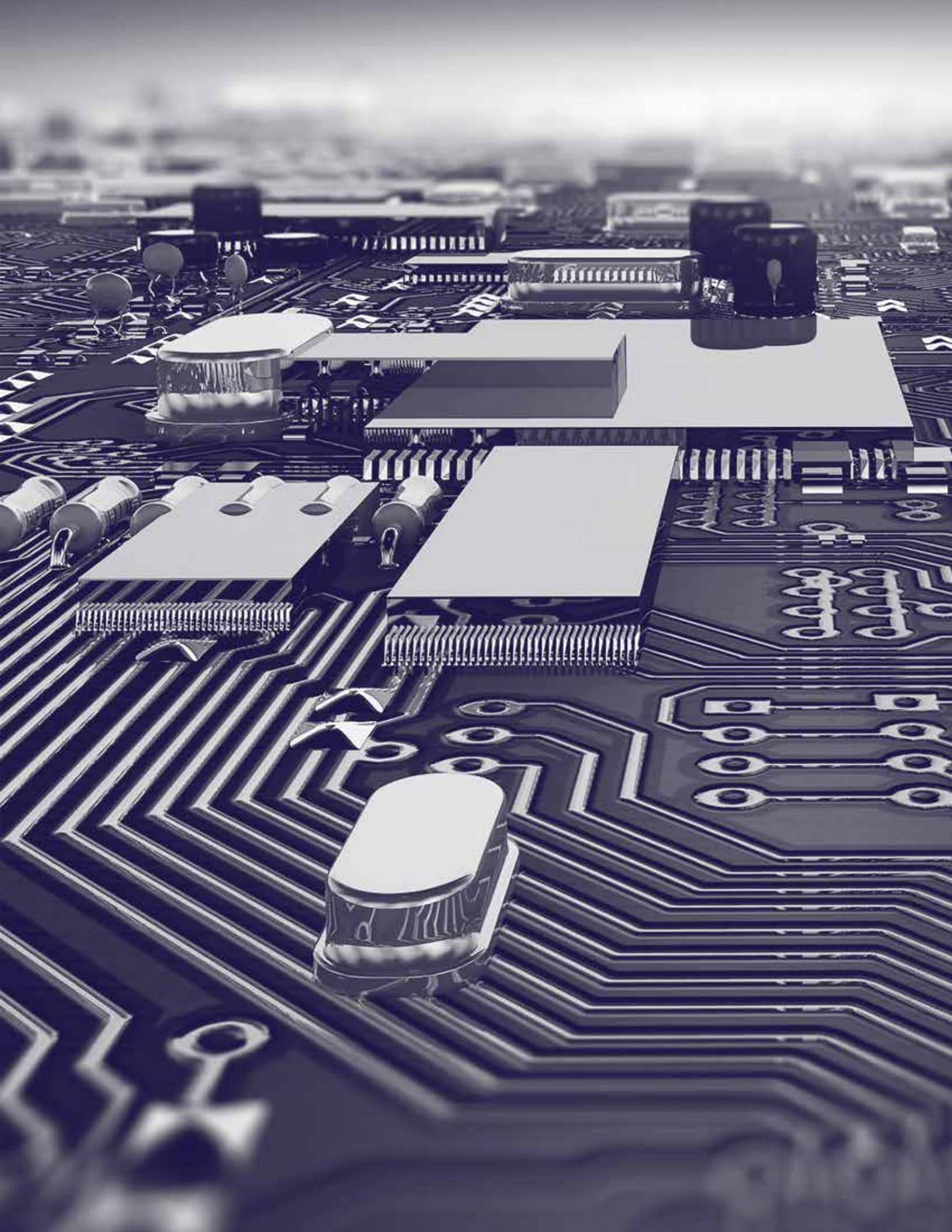
1. **Sophistication technique de la cybercapacité** : Certaines cybercapacités sont faciles à obtenir sur Internet et il n'est pas nécessaire de très bien s'y connaître pour les déployer. Par contre, les cybercapacités plus sophistiquées sont conçues sur mesure pour répondre à un ensemble défini de circonstances (p. ex. pour accéder à un téléphone intelligent ou un réseau informatique particulier) et il faut beaucoup plus de connaissances pour les mettre sur pied et les déployer;
2. **Connaissance du processus démocratique du Canada et de la façon dont on peut le manipuler** : Le processus démocratique du Canada comprend les élections, les partis politiques, les politiciens, les médias et autres institutions, les idées et les événements qui, rassemblés, forment un environnement très complexe et dynamique. Les cybermenaces stratégiques plus sophistiquées démontrent une compréhension de l'environnement du processus démocratique et de la manière dont on peut exercer une influence à l'aide de cybercapacités;
3. **Capacité d'orchestrer des activités et mobiliser des groupes** : Une personne agissant seule est beaucoup moins susceptible d'être en mesure d'influencer le cours du processus démocratique qu'un adversaire qui peut coordonner plusieurs activités et groupes de personnes. Les adversaires les plus doués utilisent des capacités organisationnelles et financières, souvent mises sur pied au fil du temps.

Généralement, on présume que plus les cybercapacités utilisées sont sophistiquées, plus il est probable qu'elles puissent avoir des répercussions sur les résultats d'un processus démocratique (voir la figure 11 ci-dessous). Cependant, comme nous l'avons mentionné dans le deuxième point ci-dessus, un processus démocratique est un environnement complexe et dynamique et plusieurs facteurs autres que les adversaires peuvent influencer un processus démocratique et jouer un rôle dans son dénouement. Il est habituellement très difficile de déterminer si les activités des adversaires ont exercé une influence sur les résultats d'un processus démocratique et, le cas échéant, dans quelle mesure.

FIGURE 11 : Niveaux de sophistication

NIVEAU DE SOPHISTICATION	CARACTÉRISTIQUES DE LA SOPHISTICATION	ADVERSAIRES OBSERVÉS
Faible	<ul style="list-style-type: none"> <li>Utilise une seule et simple cybercapacité</li> <li>Une seule cible</li> <li>Peu ou pas de planification</li> <li><u>Répercussions probables</u> : nuisance, aucun effet à long terme sur qui que ce soit</li> </ul>	<ul style="list-style-type: none"> <li>États-nations, hacktivistes, cybercriminels, acteurs politiques, amateurs de sensations fortes</li> </ul>
Moyen	<ul style="list-style-type: none"> <li>Quelques cybercapacités utilisées avec compétence</li> <li>Plus d'une cible</li> <li>Planification requise</li> <li><u>Répercussions probables</u> : plusieurs personnes touchées, du temps et des ressources sont nécessaires pour régler le problème</li> </ul>	<ul style="list-style-type: none"> <li>États-nations, hacktivistes, acteurs politiques</li> </ul>
Élevé	<ul style="list-style-type: none"> <li>Plusieurs cybercapacités utilisées avec expertise</li> <li>Nombreuses cibles</li> <li>Planification et coordination à long terme et exhaustives</li> <li><u>Répercussions probables</u> : nombreuses personnes touchées et contraintes à investir beaucoup de temps et de ressources pour contrer la cybermenace</li> </ul>	<ul style="list-style-type: none"> <li>États-nations, acteurs politiques</li> </ul>

Dans la prochaine section, nous vous présenterons deux études de cas **fictives** afin d'illustrer comment les adversaires utilisent stratégiquement leurs cybercapacités pour influencer le processus démocratique. La première étude de cas décrit des activités conçues pour influencer l'opinion publique en défaveur d'un candidat politique. La deuxième étude de cas décrit comment le cyberespionnage peut servir à obtenir des documents stratégiques d'une campagne politique et des renseignements personnels pour donner un avantage à un rival politique.



# ÉTUDE DE CAS : INFLUENCER L'OPINION PUBLIQUE CONTRE UN CANDIDAT

**CIBLE :** Médias sociaux

**OBJECTIF :** Faire chuter la popularité d'un candidat

**Scénario:** À la veille des élections fédérales, un adversaire dresse un plan en vue de ternir la réputation d'un candidat qui épouse des politiques qui s'opposent à ses propres intérêts. L'adversaire compte influencer l'opinion des électeurs en menant une campagne de désinformation dans les médias sociaux.

Cette opération d'influence, si elle porte ses fruits, fera tomber la popularité du candidat qui risquera alors de perdre l'élection. L'adversaire peut arriver à ses fins en comprenant le fonctionnement des médias sociaux et en se servant de cybercapacités faciles à obtenir et à utiliser. Quoiqu'un tel processus puisse se dérouler de différentes façons, cette étude de cas décrit les fondements d'une opération d'influence dans les médias sociaux.

1. **Planification :** À cette étape, l'adversaire étudie le contexte actuel des médias sociaux et conçoit une stratégie pour le manipuler de sorte à discréditer le candidat aux élections fédérales. L'adversaire détermine les types d'enjeux qui sont importants aux yeux des abonnés du candidat, ainsi que le genre d'histoires qui feront probablement l'objet d'une grande couverture dans les médias traditionnels et seront diffusées à grande échelle dans les médias sociaux.
2. **Intervention dans Internet :** À cette étape, l'adversaire conçoit ses activités en se basant sur ses connaissances exhaustives de la façon dont les électeurs se renseignent dans les médias sociaux, y forment leurs opinions et les perpétuent. Par exemple, chaque fournisseur de médias sociaux utilise différents algorithmes pour promouvoir les sujets tendance auprès des utilisateurs. Armé de ces connaissances, l'adversaire manipule le système afin d'introduire des idées et de l'information susceptibles de ternir la réputation du candidat.

L'adversaire manipule principalement les médias sociaux de trois façons, soit au moyen d'usines de trolls, de réseaux de zombies et du détournement de comptes. L'adversaire paie des groupes de personnes (des usines de trolls) pour diffuser de la propagande et faire de la désinformation sur Internet. Ces personnes affichent de l'information fausée dans des sites Web qui ressemblent à des sites d'actualités dignes de confiance, ainsi que dans les sections commentaires des sites Web des médias traditionnels et dans les médias sociaux.

L'adversaire achète des réseaux de zombies, soit une série de comptes dans les médias sociaux qui sont tous contrôlés par un seul utilisateur.

De cette façon, une personne peut contrôler plusieurs comptes et introduire des milliers de messages dans des conversations politiques afin d'endiguer certains faits et opinions, et d'en répandre d'autres.

Le détournement de comptes est une pratique où l'adversaire utilise des cybercapacités pour prendre le contrôle des comptes des façonneurs d'opinion dans les médias sociaux, dont les abonnés voteraient probablement pour le candidat.

En exploitant ces capacités en vue d'atteindre un objectif précis, l'adversaire réussit à faire de la désinformation et de la propagande dans les médias sociaux, à amplifier les messages qui discréditent le candidat (p. ex. sujets tendance) et à étouffer les messages neutres ou en faveur du candidat.

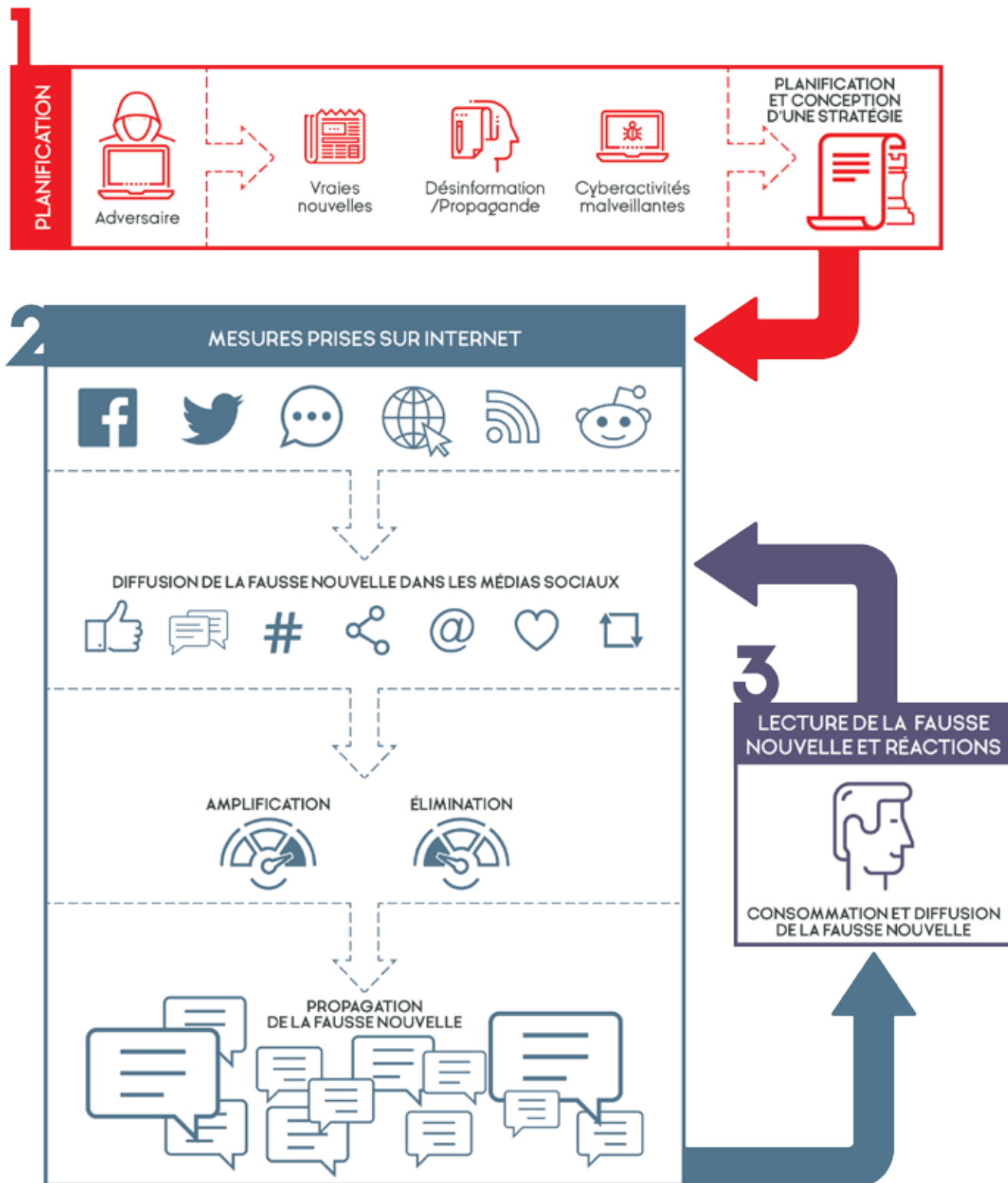
3. **Réaction des électeurs :** Les électeurs ne sont pas conscients de la manipulation et que l'information personnalisée qu'ils reçoivent dans les médias sociaux est truffée de désinformation et de propagande.

Les électeurs réagissent à l'information reçue qui influe sur leur opinion du candidat. Ils réagissent également en transmettant et en commentant l'information reçue et, ce faisant, ils aident l'adversaire à atteindre son objectif en favorisant la propagation du message.

Un adversaire politique peut aussi réagir à cette information et s'en servir à son avantage, multipliant ainsi l'incidence du message.



FIGURE 12 : Étude de cas : Opération d'influence organisée dans le cyberenvironnement



# ÉTUDE DE CAS : CYBERESPIONNAGE CONTRE UN CANDIDAT

**CIBLE :** Candidat à la mairie

**OBJECTIF :** Obtenir la stratégie de campagne et l'information personnelle du candidat pour les transmettre à son rival.

**Scénario :** Lors d'une campagne municipale serrée, un adversaire réussit à avoir accès au téléphone intelligent, puis au système informatique d'un des candidats à la mairie. Une fois connecté au système, l'adversaire est en mesure de trouver la stratégie de campagne du candidat et de l'information personnelle compromettante. Il s'empare de cette information et la transmet anonymement au rival du candidat, qui pourra s'en servir pour faire avancer sa propre campagne.

L'accès illégal au courriel, au téléphone intelligent ou à l'ordinateur d'un candidat peut s'avérer bien plus avantageux pour un adversaire qu'une recherche dans des sources ouvertes. Quoiqu'un tel processus puisse se dérouler de différentes façons, cette étude de cas décrit les fondements du cyberespionnage.

1. **Accès au téléphone intelligent de la cible :** L'adversaire envoie un courriel de harponnage directement à un candidat (ou à un de ses proches). L'objectif consiste à inciter la cible à cliquer sur un lien ou à ouvrir un fichier. Par exemple, l'objet du courriel pourrait être intitulé « Ébauche de discours à approuver » et le lien vers un fichier Word, « Ébauche avec vos modifications ». Le candidat clique sur le lien à partir de son téléphone intelligent, ce qui installe un maliciel.

Grâce au maliciel, l'adversaire a maintenant accès (par l'entremise d'Internet) au téléphone intelligent. Il peut donc surveiller tous les textos, les courriels, les messages instantanés et les photos qui s'y trouvent, et même activer les fonctions d'enregistrement vidéo et audio du téléphone intelligent à l'insu de la victime.

2. **Passage du téléphone intelligent au portable (déplacement latéral) :** En ayant le contrôle d'un premier dispositif (un téléphone intelligent), l'adversaire peut obtenir l'accès à d'autres dispositifs connectés à Internet, comme un portable. Il pourrait tenter de se déplacer latéralement entre les dispositifs des membres du personnel ou de la famille du candidat.

3. **Surveillance du téléphone intelligent et du portable :** Les dispositifs électroniques, en plus de comprendre des documents sur la stratégie de campagne du candidat, renferment des détails intimes sur la vie privée de celui-ci, y compris ses antécédents politiques et financiers, sa santé et sa vie amoureuse.

4. **Analyse et recherche d'information exploitable :** L'adversaire analyse les documents, les textos, les enregistrements audio et vidéo, et trouve la stratégie de campagne et de l'information délicate sur le plan politique ou personnel qui pourrait mettre le candidat dans l'embarras.

5. **Envoi de l'information au rival :** L'adversaire communique anonymement avec le rival du candidat et lui envoie l'information qui pourrait lui être utile.

Le rival utilise l'information : Le rival obtient de l'information cruciale, dont il peut se servir soit dans les coulisses, soit en l'étalant sur la place publique pour aider sa propre campagne.

FIGURE 13 : Processus de cyberintrusion





# **LES TENDANCES MONDIALES ET LA MENACE ENVERS LE CANADA**

## DONNÉES DE RÉFÉRENCE MONDIALES SUR LES ÉVÉNEMENTS CONNUS

Au cours des dix dernières années, le CST a étudié des dizaines d'incidents où des adversaires ont ciblé le processus démocratique au moyen de cybercapacités. Ces incidents, qui ont visé près de 40 pays sur cinq continents différents, mettent en cause certains des pays les plus riches – et les plus pauvres – au monde. Comme bon nombre de ces activités sont menées secrètement, nous supposons qu'un grand nombre d'entre elles restent probablement dans l'ombre.

### Menaces stratégiques et indirectes

Au cours des dix dernières années, la majorité des activités menées par des adversaires contre le processus démocratique ont été stratégiques (environ 80 p. 100). Cela signifie que les adversaires ont pris des mesures dans le but précis d'influencer le processus démocratique. Environ trois quarts de ces activités stratégiques employaient des méthodes moyennement ou grandement sophistiquées. Quant aux 25 p. 100 restants, il s'agissait principalement d'activités peu sophistiquées menées par des cybercriminels afin de voler des renseignements sur les électeurs.

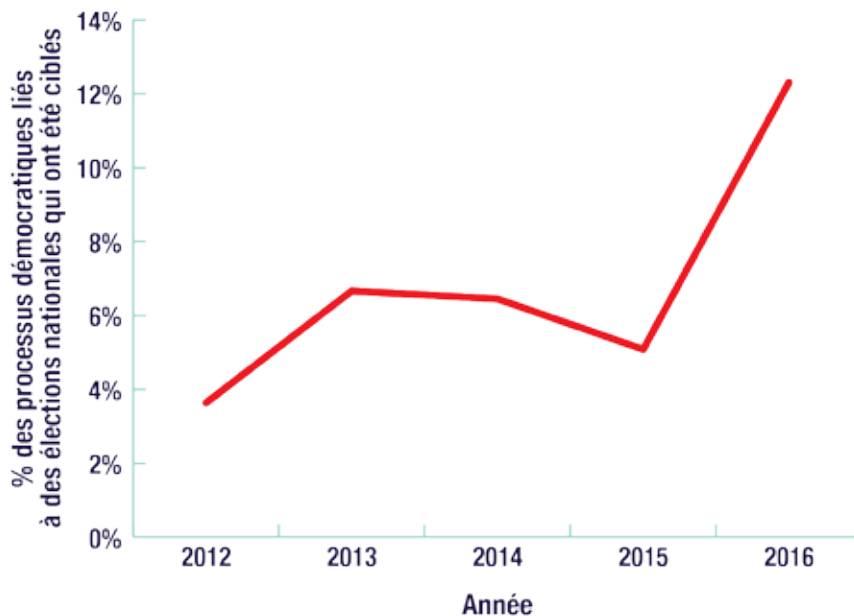
Dans 53 p. 100 des cas d'activités stratégiques observés, les adversaires ciblaient plus d'un aspect du processus démocratique. Les activités électorales étaient ciblées un peu plus de la moitié du temps (53 p. 100), suivies des partis politiques et des politiciens (47 p. 100), puis des médias (46 p. 100). Par conséquent, les adversaires semblent s'intéresser aux trois aspects du processus démocratique.

On constate une hausse inquiétante des cybermenaces contre les processus démocratiques. À ce jour, en 2017, des adversaires ont ciblé le processus démocratique de 13 p. 100 des pays qui ont tenu des élections nationales. Nous croyons qu'il est très probable que les cybermenaces contre les processus démocratiques à l'échelle mondiale seront plus nombreuses et plus sophistiquées au cours de l'année à venir, et peut-être même à plus long terme.

De nombreux facteurs contribuent à cette hausse des cybermenaces.

- De nombreuses cybercapacités sont **disponibles au public, abordables et faciles à utiliser**.
- Il est difficile de **prévenir les cybermenaces**. Nous sommes incapables d'attribuer environ 20 p. 100 des incidents à un adversaire en particulier. De plus, il semblerait que la plupart des incidents attribués à un adversaire soient demeurés impunis.
- **L'expansion rapide des médias sociaux**, jumelée au déclin des sources d'information traditionnelles faisant autorité, rend la tâche plus facile aux adversaires qui utilisent leurs cybercapacités et d'autres méthodes pour faire de la désinformation et de la propagande dans les médias afin d'influencer les électeurs.
- Les organismes électoraux adoptent **de plus en plus de processus en ligne**, ce qui les rend plus vulnérables aux cybermenaces.
- **La réussite des auteurs de cybermenaces enhardit nos adversaires** qui répètent leurs exploits et inspirent d'autres auteurs à imiter leurs comportements.

FIGURE 14 : Ciblage des processus démocratiques liés à des élections nationales, partout dans le monde





## LE CONTEXTE CANADIEN

### CYBERMENACES CONTRE LE PROCESSUS DÉMOCRATIQUE DU CANADA

La cybermenace qui touche le processus démocratique au Canada ne représente qu'une petite fraction d'une activité mondiale bien plus vaste. Le processus démocratique qui s'est déroulé en 2015, au Canada, a été ciblé par une cybermenace peu sophistiquée. Il est très probable que les auteurs de cette cybermenace étaient des hacktivistes et des cybercriminels. Les détails entourant les incidents les plus graves ont d'ailleurs fait l'objet de reportages dans plusieurs médias canadiens<sup>20</sup>.

Au Canada, les prochaines élections fédérales auront lieu en 2019. Sans tenir compte des événements imprévisibles, nous estimons qu'il est presque certain que plusieurs groupes d'hacktivistes déploieront des cybercapacités en vue d'influencer ce processus démocratique. Les hacktivistes étudieront probablement les opérations d'influence qui ont été concluantes par le passé, et mèneront des activités plus sophistiquées et mieux réussies.

La majorité de ces activités sera de faible complexité, mais nous nous attendons à ce que certaines activités d'influence soient bien planifiées et ciblent plus d'un aspect du processus démocratique, de sorte qu'elles pourraient presque atteindre un niveau moyen de sophistication.

Les États-nations ont fait preuve du plus haut niveau de sophistication (surtout moyen et élevé, mais parfois faible) et un petit nombre d'entre eux sont derrière la majorité des cybermenaces contre les processus démocratiques du monde entier. Les États-nations font aussi appel à des méthodes qui ne sont pas ancrées dans le cyberenvironnement (p. ex. la manipulation, la coercition et l'espionnage traditionnels, ainsi que les journaux et stations de télévision parrainés par l'État) pour tenter d'influencer les médias, les partis politiques et les politiciens.

Les États-nations déploient constamment des cybercapacités pour tenter d'accéder aux réseaux du gouvernement du Canada et aux communications des représentants du gouvernement fédéral<sup>21</sup>.

Les groupes terroristes n'ont pas manifesté leur intention d'utiliser des cybercapacités pour influencer les processus démocratiques à l'échelle internationale ou au Canada.



***À ce jour, rien n'indique que des États-nations aient utilisé des cybercapacités en vue d'influencer le processus démocratique du Canada au cours des élections. Nous croyons qu'en 2019, cette situation pourrait être la même ou changer selon la perception qu'auront les États-nations adversaires des politiques nationales et étrangères du Canada, au cours des deux prochaines années, ainsi qu'en fonction de l'ensemble des politiques adoptées par les candidats aux élections fédérales de 2019.***

Cependant, certains groupes ont démontré qu'ils sont capables d'utiliser des cybercapacités, d'orchestrer une vaste gamme d'activités et de manipuler les médias sociaux et les médias traditionnels. Nous croyons que certains groupes terroristes seraient en mesure de monter une campagne d'un niveau de sophistication moyen. Il est probable que l'absence d'activité témoigne de leur manque d'intention de se mettre à l'œuvre.

À l'extérieur du Canada, des acteurs politiques corrompus emploient des cybercapacités pour influencer sur les processus démocratiques de leurs pays; toutefois, cela ne représente que 9 p. 100 des activités observées. Étant donné la popularité des cybercapacités et les avantages qu'elles confèrent, les acteurs politiques à l'étranger s'en serviront probablement de plus en plus pour façonner leur avenir politique. Puisque le taux de corruption est faible au Canada, il est bien plus probable que ce genre d'activités se produise ailleurs dans le monde.<sup>22</sup>

Au-delà du fédéral, le CST n'a aucune indication que des cybermenaces aient visé le processus démocratique d'une des milliers d'élections provinciales, territoriales ou municipales au cours des cinq dernières années.

Il s'agit d'une bonne nouvelle. D'après notre évaluation, nous croyons qu'il est très probable que le niveau de menace contre le processus démocratique lié aux élections infranationales reste faible. Toutefois, les tendances que nous avons soulignées ci-dessus risquent d'avoir un effet de vent arrière en accroissant la menace envers les activités électorales, les partis politiques et les politiciens municipaux, provinciaux et territoriaux du Canada, ainsi que les médias pertinents.

Tout particulièrement, nous savons que les principaux intérêts de certains États-nations peuvent être directement influencés par les politiques canadiennes liées aux ressources naturelles, lesquelles sont souvent élaborées par les provinces et les territoires. En outre, certains leaders provinciaux, territoriaux et municipaux du Canada sont à l'origine de politiques et de déclarations qui ont attiré l'attention à l'échelle nationale et internationale. Les élections, les partis politiques et les politiciens au niveau infranational pourraient donc devenir des cibles dignes d'intérêt pour les hacktivistes.



## CONCLUSION

Dans la présente évaluation, nous avons expliqué comment les principaux aspects du processus démocratique (c.-à-d. les élections, les partis politiques, les politiciens et les médias) sont vulnérables aux cybermenaces et aux opérations d'influence. Nous avons décrit les différents types d'adversaires qui pourraient faire appel à des cybercapacités, et évalué comment les cybermenaces contre le processus démocratique du Canada sont susceptibles d'évoluer.

Généralement, la plupart des cybermenaces dont nous avons discuté peuvent être atténuées grâce à la cybersécurité, à la sécurité physique et aux pratiques exemplaires en matière de continuité des activités. Toutefois, les cybermenaces et les opérations d'influence sont souvent réussies, car elles ne reposent pas uniquement sur les vulnérabilités technologiques, mais exploitent des comportements humains et des habitudes sociales profondément ancrés. Pour défendre le processus démocratique du Canada contre les cybermenaces et les opérations d'influence connexes, il faut se pencher sur les aspects techniques et sociaux du problème.

### LECTURE COMPLÉMENTAIRE

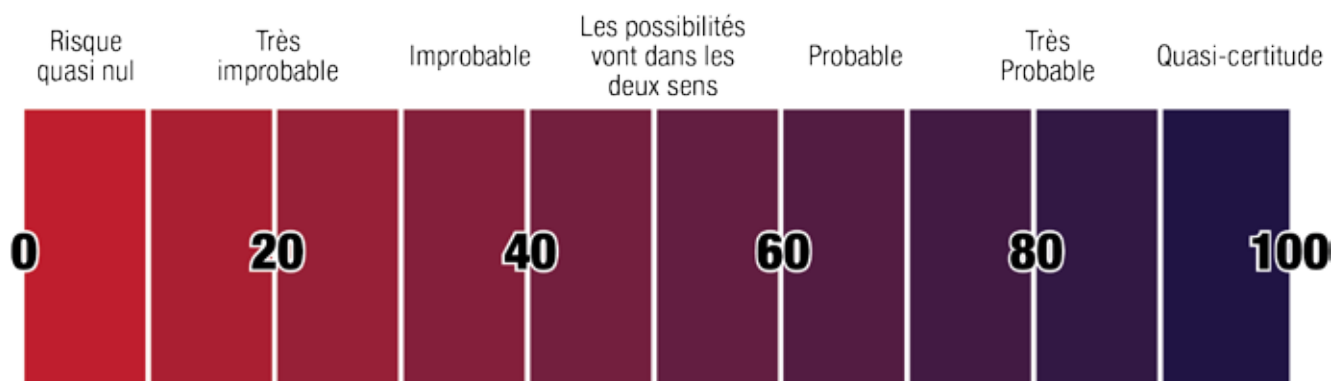
Pour en savoir plus sur l'atténuation des cybermenaces, consultez les documents suivants du CST :

- [Les 10 meilleures mesures de sécurité des TI;](#)
- [Les pratiques exemplaires en cybersécurité;](#)
- [La sécurité mobile.](#)

# ANNEXE A

## LEXIQUE DES ESTIMATIONS

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



# NOTES EN FIN DE TEXTE

1. Consultez la figure 11 pour en savoir plus sur la description des niveaux de sophistication des cybermenaces.
2. Humphreys, Adrian. « Anonymous leaks another high-level federal document as part of vendetta against government ». The National Post. 26 septembre 2015. <<http://news.nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government>> (consulté en avril 2017).
3. Les cybermenaces contre le Canada sont causées par des personnes ou des groupes qui utilisent des cybercapacités contre des ordinateurs, réseaux et autres technologies de l'information du Canada, ou contre les renseignements qu'ils contiennent.
4. Les cybercapacités sont des activités informatiques et liées à Internet qui peuvent servir à détériorer la confidentialité, l'intégrité et la disponibilité de l'information et des technologies de l'information.
5. Les cybercriminels embauchés par d'autres adversaires (p. ex. des États-nations ou des acteurs politiques) sont des fournisseurs de services. Nous évaluons ces exemples en nous basant sur les intentions du groupe qui fait la demande de service.
6. Dans certains cas, les organismes électoraux échangent entre eux leurs listes d'électeurs. Par exemple, Élections Canada transmet certaines parties du Registre national des électeurs aux provinces, à certaines municipalités et aux partis politiques. « Description of the National Register of Electors. » Élections Canada. 20 février 2017. <<http://www.elections.ca/content.aspx?section=vot&dir=reg/des&document=index&lang=f>> (consulté en février 2017).
7. Habituellement, on n'utilise pas les machines à voter électroniques au Canada, mais on s'en sert dans d'autres pays. Les électeurs qui utilisent ces machines votent à l'aide d'un ordinateur muni d'un écran tactile au lieu d'un bulletin de vote en papier.
8. Nakashima, Ellen. « Russian Hackers Targeted Arizona Election System. » The Washington Post. 29 août 2016. <[https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e\\_story.html?utm\\_term=.76054fb28944](https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html?utm_term=.76054fb28944)> (consulté en février 2017); et « Illinois Voter Registration System Records Breached. » State Board of Elections. 31 août 2016. <[https://www.elections.il.gov/Downloads/AboutTheBoard/PDF/08\\_31\\_16PressRelease.pdf](https://www.elections.il.gov/Downloads/AboutTheBoard/PDF/08_31_16PressRelease.pdf)> (consulté en février 2017).
9. « Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information du gouvernement du Canada. » Centre de la sécurité des télécommunications. <<https://www.cse-cst.gc.ca/fr/publication/itsb-89v3>>. Novembre 2014.
10. BBC News Staff. « Ghana Election Commission Website Hit by Cyber Attack. » BBC News. 8 décembre 2016. <<http://www.bbc.com/news/world-africa-38247987>> (consulté en février 2017).
11. Escritt, Thomas. « Dutch will hand count ballots due to hacking fears. » Reuters. 1<sup>er</sup> février 2017. <<http://www.reuters.com/article/us-netherlands-election-cyber-idUSKBN15G55A>> (consulté en avril 2017).
12. Voir la page 30 pour une étude de cas sur le fonctionnement du cyberespionnage.
13. Office of the Director of National Intelligence. « Assessing Russian Activities and Intentions in Recent US Elections. » 6 janvier 2017. <[https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)> (consulté en février 2017).
14. Le Web invisible est composé d'une série de sites Web publics mais dissimulés, puisque les utilisateurs doivent avoir recours à des configurations, à des autorisations et à des logiciels particuliers pour y accéder.
15. Soixante-quinze pour cent des Canadiens sondés affirment consulter les actualités en ligne. Newman, Nic, et autres. « Reuters Institute Digital News Report 2016. » Reuters Institute for the Study of Journalism. <<http://www.digitalnewsreport.org/survey/2016/canada-2016>>. (consulté en avril 2017).
16. Auchard, Eric et Bate, Felix. « French candidate Macron claims massive hack as emails leaked. » Reuters. 6 mai 2017. <<http://reuters.com/article/us-france-election-macron-leaks-idUSKBN1812AZ>> (consulté en mai 2017).
17. BBC News Staff. « Push to tackle online 'booter' services. » BBC News. 5 août 2016. <<http://www.bbc.com/news/technology-36993107>> (consulté en avril 2017).
18. Le terme « maliciel » est un néologisme découlant de la fusion de deux mots : « malveillant » et « logiciel ». Il s'agit de tout logiciel utilisé pour obtenir l'accès à un système informatique privé, pour perturber des opérations informatiques ou pour recueillir des renseignements de nature sensible.
19. The Associated Press. « Ransomware Attack Hits Pennsylvania State Senate Democrats. » The Wall Street Journal. 3 mars 2017. <<https://www.wsj.com/articles/ransomware-attack-hits-pennsylvania-state-senate-democrats-1488584037>> (consulté en avril 2017).
20. Humphreys, Adrian. « Anonymous leaks another high-level federal document as part of vendetta against government ». The National Post. 26 septembre 2015. <<http://news.nationalpost.com/news/canada/anonymous-leaks-another-high-level-federal-document-as-part-of-vendetta-against-government>> (consulté en avril 2017).
21. Les activités de détection du CST révèlent que des adversaires sondent les systèmes du gouvernement du Canada des centaines de millions de fois chaque jour.
22. Freedom House. « Freedom in the World 2017 ». <<https://freedomhouse.org/report/freedom-world/2017/canada>> (consulté en avril 2017).



