ISSN 2564-1395
CAT D95-10F-PDF

Cybermenaces contre le processus démocratique du CANADA

Mise à jour de 2023

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

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

ISSN 2564-1395
CAT D95-10F-PDF

TABLE DES MATIÈRES

À PROPOS DE NOUS

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 chargés de l'application de la loi et de la sécurité dans leurs activités légalement autorisées lorsque ces derniers requièrent ses capacités techniques uniques.

En outre, le CST protège les réseaux informatiques et 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 ses 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 décisionnaires de mieux comprendre les crises et les événements mondiaux, et de promouvoir les intérêts du Canada dans le monde.

Faisant partie du CST, le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) est l'autorité technique canadienne en matière de cybersécurité. Relevant du CST, le Centre pour la cybersécurité représente la seule source unifiée fournissant des avis, des conseils, des services et du soutien spécialisés en matière de cybersécurité pour les Canadiennes et Canadiens et pour les entreprises canadiennes.

Le CST et le Centre pour la cybersécurité 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 Canadiennes ou Canadiens à l'étranger, les attentats contre les ambassades canadiennes 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

Les adversaires étrangers utilisent de plus en plus des cyberoutils dans le but de cibler les processus démocratiques partout dans le monde. La désinformation est devenue omniprésente durant les élections nationales, et les adversaires utilisent dorénavant l'intelligence artificielle (IA) générative pour créer et propager du faux contenu. Le présent rapport aborde les activités de cybermenace visant les élections, ainsi que la menace croissante que représente l'IA générative pour les processus démocratiques mondiaux et canadiens.

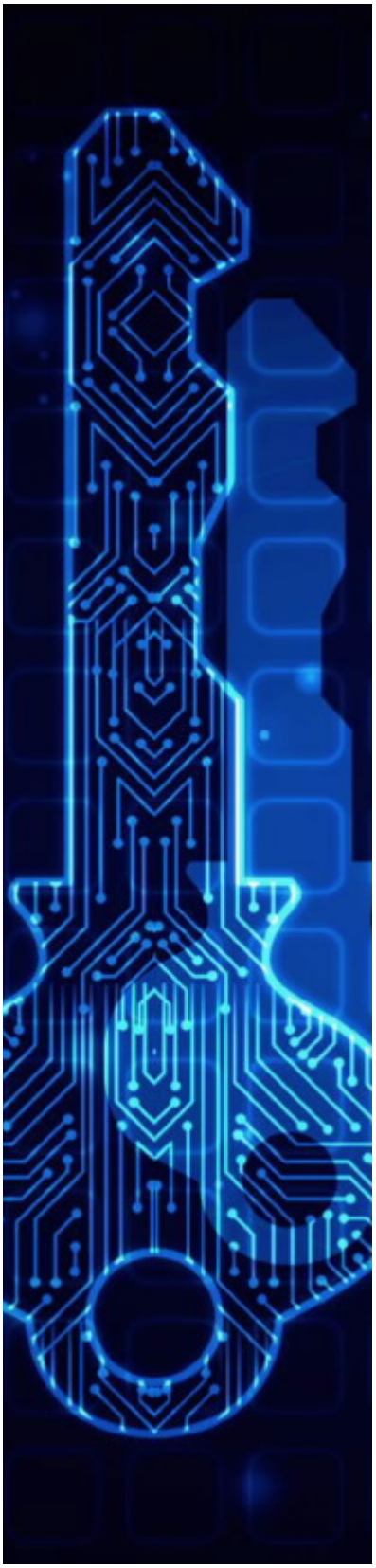
Principales conclusions et tendances mondiales

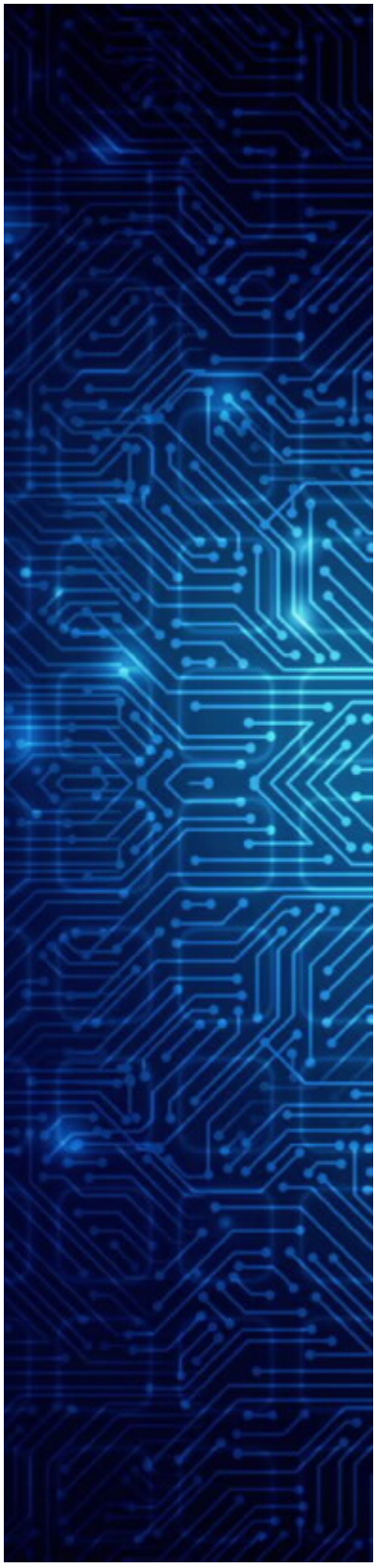
- Les cybermenaces visant les élections connaissent une hausse à l'échelle mondiale. La proportion de processus électoraux ciblés par des activités de cybermenace comparativement au nombre total d'élections nationales dans le monde est passée de 10 % en 2015 à 26 % en 2022. Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[1] », nous avons constaté une augmentation de la proportion de processus électoraux touchés, qui est passée de 23 % à 26 % entre 2021 et 2022[2].

- En 2022, nous avons déterminé qu'un peu plus du quart (26 %) de tous les processus électoraux nationaux au monde avaient été touchés par au moins un cyberincident. Parmi les pays dont le processus électoral national a été touché par les activités de cybermenace de 2015 à 2022, environ 25 % sont membres de l'Organisation du Traité de l'Atlantique Nord (OTAN) et 35 % de l'Organisation de coopération et de développement économiques (OCDE).

- Nous constatons que les auteures et auteurs de cybermenace étatiques ayant des liens avec la Russie et la Chine continuent d'être à l'origine de la plupart des activités de cybermenace visant les élections étrangères depuis 2021. Les activités de cybermenace de la Russie et de la Chine comprennent entre autres des tentatives d'attaque par déni de service distribué (DDoS pour *distributed denial of service*) contre les sites Web des organismes électoraux, d'accès aux renseignements personnels des électrices et électeurs ou à l'information électorale et d'analyse des vulnérabilités sur les modes de scrutin électronique[3]. Nous estimons qu'il est très probable que la Russie et la Chine soient encore responsables de la plupart des activités de cybermenace attribuées visant les élections étrangères dans les deux prochaines années, particulièrement contre les pays ayant une importance stratégique pour elles.

- Les activités de cybermenace parrainées par des États visant





le Canada représentent une menace constante et continue, qui s'inscrivent souvent dans des campagnes mondiales plus vastes qu'entreprennent ces adversaires. Lorsque les tensions bilatérales sont fortes, des auteures et auteurs de menace peuvent être appelés à effectuer des cyberactivités ou des opérations d'influence ciblant des événements nationaux d'importance, y compris des élections. Nous évaluons que l'exacerbation des tensions et de l'antagonisme entre le Canada et un État hostile ferait presque certainement en sorte que les auteures et auteurs de cybermenace veillant aux intérêts de cet État ciblent les processus démocratiques du Canada ou perturbent l'écosystème d'information en ligne du Canada en prévision d'élections nationales.

- La majorité des activités de cybermenace visant les élections demeurent non attribuées. Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[4] », l'origine de plus de la moitié des activités de cybermenace visant les élections nationales est inconnue. En 2022, 85 % des activités de cybermenace ciblant les élections n'étaient pas attribuées, c'est-à-dire que ces cyberincidents n'étaient pas imputés à une ou un auteur de cybermenace parrainé par un État. Dans les cas où l'origine est connue, seuls deux pays ont ciblé activement les processus électoraux étrangers depuis deux ans et demi : la Russie et la Chine. Nous sommes d'avis qu'il est fort probable que les auteures et auteurs de cybermenace utilisent plus de techniques de camouflage et/ou l'externalisation des cyberactivités dans le but de masquer leur identité ou leurs liens avec un gouvernement étranger.
- Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[5] » jusqu'au printemps 2023, nous avons déterminé que toutes les élections nationales dans le monde (146 au total) ont été la cible de désinformation en ligne visant à influencer le vote et les élections. Nous avons également détecté une augmentation de la production de contenu synthétique en lien avec des élections nationales, presque certainement attribuable à l'accès accru à l'IA générative. Toutefois, nous avons noté que le nombre de cas signalés quant à du contenu synthétique utilisé à des fins de désinformation au sujet d'élections demeure relativement bas, comparativement à la quantité de contenu synthétique détecté en ligne. Nous croyons que l'utilisation de l'IA générative afin de produire du contenu synthétique au sujet d'élections nationales augmentera presque certainement au cours des deux prochaines années, alors que cette technologie deviendra accessible à un public plus large.

À PROPOS DE CE RAPPORT

La présente constitue le quatrième rapport sur les cybermenaces contre le processus démocratique du Canada et fait le point sur la situation depuis les rapports publiés par le CST en 2017, en 2019 et en 2021. Il vise à informer la population canadienne des cybermenaces qui pèsent sur le processus démocratique du Canada en 2023.

Portée

Le présent rapport traite des cybermenaces qui touchent les processus démocratiques. Une activité de cybermenace est menée au moyen de cyberoutils et de techniques (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. L'évaluation tient compte des activités de cybermenace et des campagnes d'influence organisées dans le cyberenvironnement, c'est-à-dire lorsque des auteures et auteurs de menace se servent des activités de cybermenace ou de l'IA générative pour manipuler secrètement l'information en ligne dans le but d'influencer les opinions et les comportements.

Sources

Les propos formulés dans le présent rapport 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 contre les activités politiques et électorales à l'échelle nationale et internationale, tout particulièrement dans le contexte des prochaines élections fédérales canadiennes qui sont actuellement prévues en 2025. La prestation de conseils sur l'atténuation des menaces ne s'inscrit pas dans la portée du présent rapport. Vous trouverez plus de détails dans les pages suivantes.

Information supplémentaire

Des ressources se trouvent sur la page de conseils sur la cybersécurité du Centre pour la cybersécurité[6] et sur le site Web de Pensez cybersécurité[7].

Les personnes qui souhaitent en savoir plus sur les cyberoutils et le contexte en évolution des cybermenaces sont priées de consulter les documents suivants :

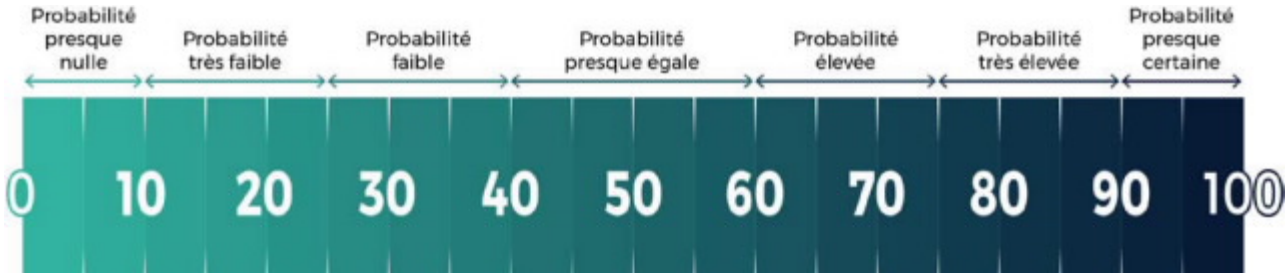
- Évaluation des cybermenaces nationales 2023-2024[8];
- Introduction à l'environnement de cybermenaces[9];
- Repérer les cas de mésinformation, désinformation et malinformation[10].

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. Nous utilisons des formulations telles que « nous évaluons que » ou « nous jugeons que » pour présenter une évaluation analytique. Les qualificatifs tels que « possiblement », « probable » et « très probable » servent à évoquer une probabilité selon l'échelle ci-dessous.

Le contenu du présent rapport est basé sur des renseignements disponibles en date du 26 octobre 2023.

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

La présente évaluation est la quatrième version de la publication « Cybermenaces contre le processus démocratique du Canada » et se veut une mise à jour sur les tendances mondiales des activités de cybermenace visant les élections nationales depuis la dernière publication en 2021. Elle fournit également de l'information sur la façon dont les activités de cybermenace ciblent les infrastructures électorales, les campagnes d'influence organisées dans le cyberenvironnement se répercutent sur l'écosystème d'information du Canada et les technologies d'IA générative influenceront l'avenir des débats électoraux en ligne.

Processus démocratique du Canada : la cible d'activités de cybermenace?

Les activités de cybermenace représentent une menace réelle et croissante contre les processus démocratiques du Canada. Les auteures et auteurs de cybermenace, y compris ceux parrainés par des États, les hacktivistes et les cybercriminelles et cybercriminels, interfèrent avec le processus démocratique et cherchent à nuire à la capacité du Canada de mener des élections libres et justes. Les efforts du Canada en vue de favoriser le commerce et le développement internationaux, la paix et la sécurité internationales, de même que les droits internationaux de la personne font du Canada une cible pour les auteures et auteurs de cybermenace qui cherchent à changer les résultats des élections dans le but d'influencer les politiques ou les relations diplomatiques. En tant que membre d'importantes organisations, comme l'Organisation du Traité de l'Atlantique Nord (OTAN) et le groupe des sept (G7), ainsi qu'en raison de son rôle dans la région indopacifique et de son soutien à l'Ukraine, le Canada est presque certainement une cible de choix pour les activités de cybermenace et les campagnes d'influence, y compris celles ciblant directement ses processus démocratiques.

Nous avons constaté que les électrices et les électeurs sont les cibles les plus fréquentes des activités de cybermenace touchant les élections dans le monde, et l'électorat canadien, un des plus connectés au monde, devient une grande cible potentielle de ces activités[11]. Étant donné qu'un grand nombre de Canadiennes et Canadiens transmettent de l'information en ligne, les auteures et auteurs de cybermenace souhaitant influencer leurs opinions et leurs comportements peuvent manipuler l'information en ligne au moyen de cybertechniques dans le cadre d'opérations d'influence (p. ex. piratage et divulgation) ou utiliser les technologies d'IA pour produire du faux contenu (p. ex. hypertrucage). L'exacerbation des tensions entre le Canada et d'autres États pourrait inciter des auteures et auteurs de cybermenace parrainés par des États à cibler les élections canadiennes et à perturber le processus démocratique du Canada. Lorsque les tensions bilatérales sont fortes, des auteures et auteurs de menace peuvent être appelés à effectuer des cyberactivités ou des opérations d'influence ciblant des événements nationaux d'importance, y compris des élections. Nous évaluons que l'exacerbation des tensions et de l'antagonisme entre le Canada et un État hostile fera presque certainement en sorte que les auteures et auteurs de cybermenace veillant aux intérêts de cet État ciblent les processus démocratiques du Canada ou perturbent l'écosystème d'information en ligne du Canada en prévision d'élections nationales.

Les adversaires étrangers utilisent des cybercapacités pour menacer les processus démocratiques

Les adversaires étrangers utilisent des cybercapacités pour influencer les résultats politiques et menacer le processus démocratique au pays en ciblant les électrices et électeurs, les politiciennes et politiciens, les partis politiques et les infrastructures électorales. Une ou un auteur de cybermenace peut compromettre directement des sites Web, des comptes de média social, des réseaux et des appareils utilisés par les organismes d'administration électorale ou, encore, polluer l'écosystème d'information en propageant de la désinformation et en menant des campagnes d'influence en prévision des élections.

Voici des exemples de cyberactivités que nous avons relevées dans le monde depuis 2021 :

- Attaques par déni de service distribué (DDoS pour *distributed denial of service*) contre les sites Web des organismes électoraux et les modes de scrutin électronique;
- Accès non autorisés aux bases de données d'inscription des électrices et électeurs afin de recueillir des renseignements personnels;
- Attaques par harponnage contre le personnel électoral et les politiciennes et politiciens;
- Tentatives de manipulation des résultats de vote en compromettant l'accès du personnel électoral aux bases de données de vote;
- Utilisation de robots et de faux comptes de médias sociaux dans le but d'influencer le discours politique.

Il est de plus en plus difficile de déterminer quel adversaire est responsable d'une activité de cybermenace visant les processus démocratiques. L'externalisation de ces activités à des tiers, comme à des hacktivistes et à des cybercriminelles et cybercriminels, ou l'acquisition de cyberoutils et services auprès de fournisseurs commerciaux et de places de marché virtuelles aident les adversaires étrangers à masquer leurs opérations. Les adversaires étrangers ont accès à une grande variété de cyberoutils et services sur les marchés illégaux qui complètent leurs cybercapacités internes. Le fait d'avoir recours à des entreprises d'influence onéreuses peut également aider à masquer la source des campagnes d'influence, puisqu'elles offrent des outils et des services qui propagent de la désinformation et manipulent les discours politiques

Par exemple, en février 2023, une équipe de journalistes a découvert le piratage et les opérations de désinformation d'une entreprise d'influence onéreuse israélienne, qui se vantait d'avoir aidé sa clientèle, y compris des gouvernements étrangers, à cibler plus de 30 élections dans le monde[12]. De plus, les adversaires étrangers externalisent leurs cyberactivités à des cybergroupes non étatiques, comme des groupes de cybercriminalité ou d'hacktivisme, dans le but d'éviter que des activités leur soient attribuées directement et d'accéder à de meilleures cybercapacités.

Activité de cybermenace et technologie d'IA : Objectifs des auteures et auteurs de menace

Objectifs à court terme

Semer le doute sur les résultats des élections

Promouvoir des discours politiques polarisants en manipulant les algorithmes des médias sociaux au moyen de faux comptes robots

Réduire la participation électorale

Produire du contenu trompeur, comme des vidéos hypertruquées et d'autres contenus synthétiques générés par l'IA

Objectifs à moyen terme

Amenuiser la confiance envers les dirigeantes et dirigeants

Créer un discours public unilatéral en ligne et favoriser le mécontentement et les mouvements sociaux par la polarisation politique

Affaiblir la confiance envers les infrastructures électorales

Accroître le scepticisme envers l'information en ligne

Objectifs à long terme

Susciter la méfiance envers la démocratisation du processus électoral

S'approprier les mouvements sociaux nationaux afin de soutenir des intérêts économiques, militaires ou idéologiques étrangers

Nuire à la participation électorale et faire en sorte que les électrices et électeurs perdent intérêt envers les élections

Semer le doute sur l'information en ligne

TENDANCES MONDIALES

Le Centre pour la cybersécurité analyse les activités de cybermenace ciblant les élections nationales dans le monde depuis 2015. Ce ne sont pas toutes les activités de cybermenace qui sont signalées; une grande partie demeure secrète. C'est pourquoi nous supposons que nos données sous-estiment presque certainement 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 2023.

Tendance nº 1 : Les processus démocratiques sont plus ciblés

La proportion de processus électoraux ciblés par des activités de cybermenace comparativement au nombre total d'élections nationales dans le monde est passée de 10 % en 2015 à 26 % en 2022. Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[13] », nous constatons une augmentation de la proportion de processus électoraux touchés, qui est passée de 23 % à 26 % entre 2021 et 2022[14]. Le pourcentage de processus électoraux ciblés en 2020 était nettement inférieur que les autres années, et nous estimons qu'il s'agit presque certainement d'une anomalie liée à la pandémie de COVID-19. De plus, nous avons déterminé qu'un peu plus du quart (26 %) de tous les processus électoraux nationaux au monde ont été touchés par au moins un cyberincident en 2022. Ces conclusions montrent une activité de cybermenace élevée; cependant, certaines activités de cybermenace visant les processus démocratiques demeurent non identifiées et non signalées. Nous croyons qu'il est très probable que ces conclusions constituent des estimations prudentes.

Nous avons déterminé que le principal type de cyberincident influençant les processus électoraux nationaux était le refus d'accès ou l'altération des sites Web de commissions électorales, suivi de l'interruption du réseau Internet pendant les élections. La part totale d'élections ciblées dans les pays de l'OTAN a augmenté de 2,8 % en 2021 à 3,7 % en 2022 (figure 1a). La pandémie de COVID-19 explique probablement pourquoi moins de pays de l'OCDE ont vu leurs processus électoraux ciblés en 2020 et en 2021, étant donné que nous notons une hausse de 4 % à 13 % de la part de pays de l'OCDE touchés entre 2021 et 2022 (figure 1b).

Figure 1 : Pourcentage d'élections nationales ciblées par des cyberactivités par année

Figure 1a

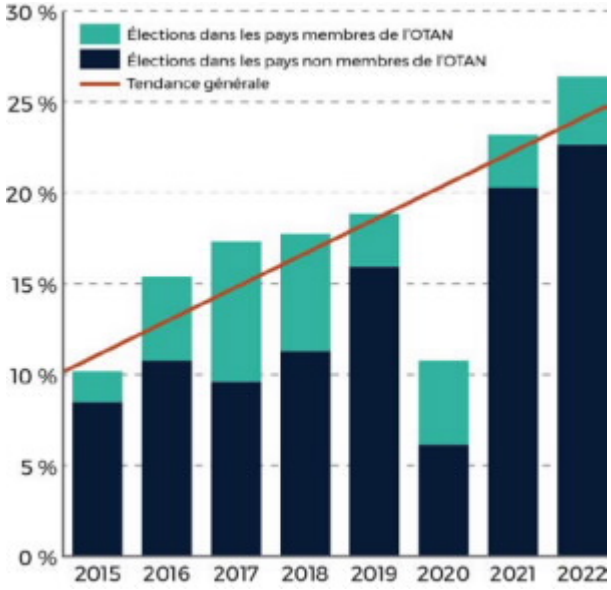
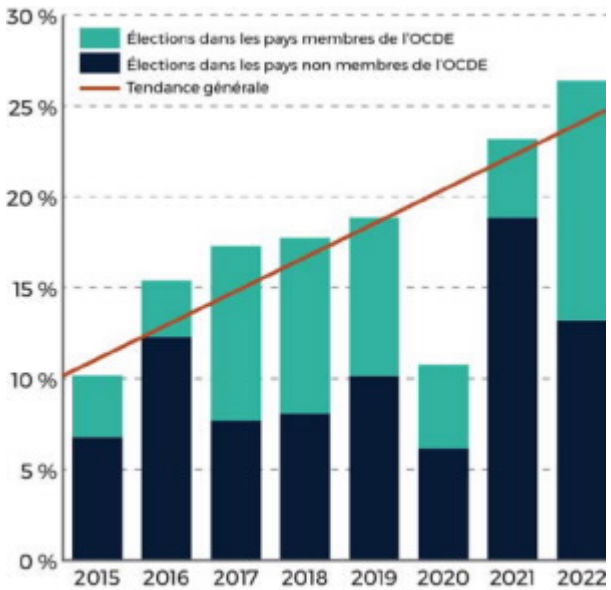


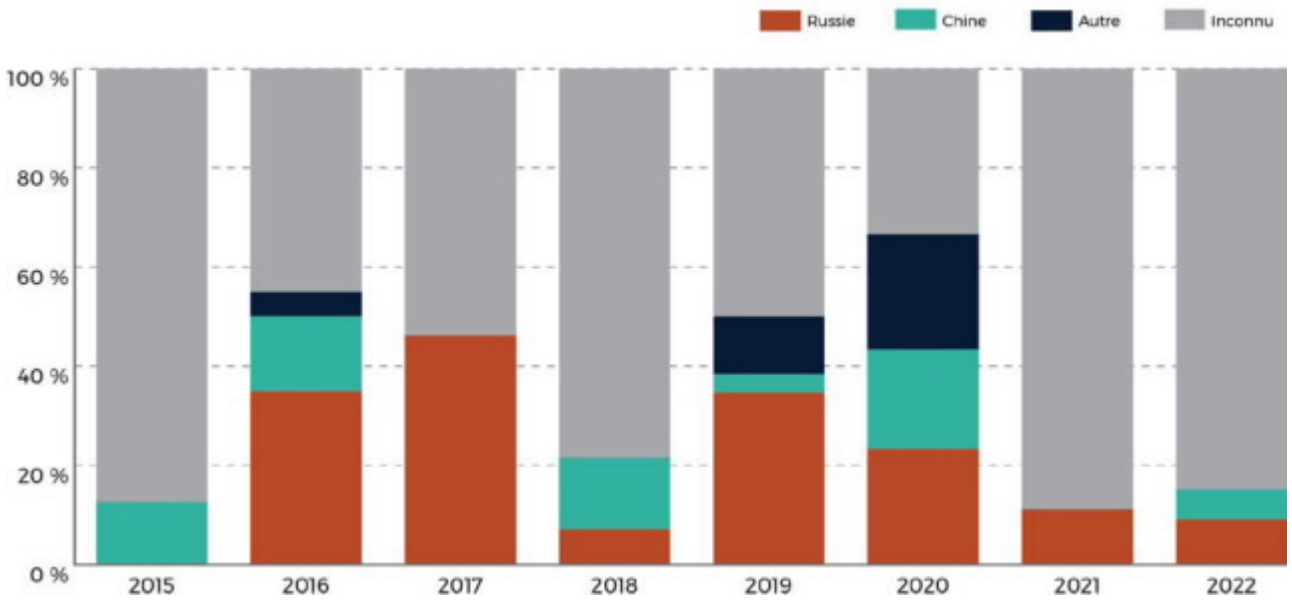
Figure 1b



Tendance nº 2 : La Russie et la Chine continuent de mener la plupart des activités de cybermenace visant les élections nationales étrangères

Nous constatons que les auteures et auteurs de cybermenace étatiques ayant des liens avec la Russie et la Chine continuent d'être à l'origine de la plupart des activités de cybermenace visant les élections étrangères depuis 2021. La Russie est constamment responsable d'activités de cybermenace observées faisant de l'interférence dans des élections étrangères depuis 2016, et des cyberactivités ont été attribuées à la Chine chaque année depuis 2015, à l'exception de 2017 et de 2021 (figure 2). Les activités de cybermenace de la Russie et de la Chine comprennent entre autres des tentatives d'attaque par DDoS contre les sites Web des organismes électoraux, d'accès aux renseignements personnels des électrices et électeurs ou à l'information électorale et d'analyse des vulnérabilités sur les modes de scrutin électronique.

Figure 2 : Proportion de cyberincidents attribués à des pays visant des élections nationales étrangères par année



Nous évaluons que les activités de cybermenace attribuée visent presque certainement à influencer les élections dans le but d'atteindre des objectifs stratégiques dans les régions géopolitiques d'intérêt pour la Russie et la Chine. Dans certains cas, les cyberactivités sont motivées par des fins politiques et cibleront les processus démocratiques d'un pays comme forme de représailles. Par exemple, des auteures et auteurs de cybermenace prorusses affiliés à un État ont ciblé les élections de pays ayant porté assistance à l'Ukraine. Nous estimons qu'il est très probable que la Russie et la Chine soient encore responsables de la plupart des activités de cybermenace attribuées visant les élections étrangères, particulièrement contre les pays ayant une importance stratégique pour elles. Nous soulignons que les prochaines élections européennes en 2023 et en 2024 pourraient être une cible importante pour la Russie en raison de l'importance de l'aide militaire et économique de l'Europe à l'Ukraine.

Tendance nº 3 : La majorité des activités de cybermenace visant les élections demeurent non attribuées

Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[15] », l'origine de plus de la moitié des activités de cybermenace visant les élections nationales est inconnue. En 2022, 85 % des activités de cybermenace ciblant les élections n'étaient pas attribuées, c'est-à-dire que ces cyberincidents n'étaient pas imputés à une ou un auteur de cybermenace parrainé par un État. Nous sommes d'avis qu'il est fort probable que les auteures et auteurs de cybermenace utilisent plus de techniques de camouflage et/ou l'externalisation des cyberactivités dans le but de masquer leur identité ou leurs liens avec un gouvernement étranger.

Le fait d'externaliser les activités de cybermenace malveillantes permet aux adversaires étrangers d'éviter de se les voir attribuer publiquement et d'éviter les conséquences diplomatiques subséquentes. Les adversaires étrangers utilisent davantage les groupes de cybermenace non étatiques afin d'éviter que les cyberactivités soient attribuées à leur gouvernement. Ces groupes font moins l'objet d'une surveillance par les gouvernements, ne respectent pas les mêmes conventions et normes et peuvent organiser des cyberactivités rapidement et sans préavis, comme des attaques par DDoS. Les adversaires étrangers utilisent aussi les services d'entreprise d'influence onéreuse pour mener des opérations d'influence qui passent inaperçues. Depuis 2011, au moins 27 opérations d'information en ligne ont été partiellement et entièrement attribuées à des services commerciaux de relations publiques ou à des entreprises de marketing[16]. Les services liés à l'ingérence électorale représentent un marché en pleine croissance, et, si l'utilisation de mandataires tiers se poursuit, nous estimons que, dans les deux prochaines années, les gouvernements auront probablement de la difficulté à associer les activités de cybermenace visant les processus électoraux aux adversaires étrangers qui en sont responsables [17].

Tendance nº 4 : L'IA générative toujours plus utilisée pour influencer des élections

Les auteures et auteurs de cybermenace utilisent les technologies d'IA générative pour influencer l'avenir des débats démocratiques en ligne. En août 2019, des chercheuses et chercheurs ont découvert une augmentation des activités sur le Web clandestin, ainsi qu'une augmentation de la publicité d'offres personnalisées de services d'hypertrucage[18]. Depuis la publication de notre rapport « Cybermenaces contre le processus démocratique du Canada : Mise à jour de juillet 2021[19] », nous avons détecté une augmentation du contenu synthétique (p. ex. hypertrucages) en lien avec les élections, presque certainement en raison de l'accès accru à un grand nombre de ces technologies. Toutefois, nous avons noté que le nombre de cas signalés quant à du contenu synthétique utilisé à des fins de désinformation au sujet d'élections demeure relativement bas, comparativement à la quantité de contenu synthétique détecté en ligne. Nous croyons que la production de contenu synthétique par l'IA en lien avec des élections nationales augmentera presque certainement au cours des deux prochaines années, alors que cette technologie deviendra accessible à un public plus large. Comme la génération de contenu synthétique augmente et devient plus répandue, il sera certainement de plus en plus difficile de détecter ce type de contenu, et les Canadiennes et Canadiens auront plus de difficultés à se fier à l'information sur les politiciennes, les politiciens et les élections disponible en ligne.

ACTIVITÉS DE CYBERMENACE CONTRE LES INFRASTRUCTURES ÉLECTORALES

Partout dans le monde, les processus électoraux dépendent de plus en plus des technologies numériques, c'est-à-dire que les cyberattaques contre les infrastructures électorales sont une menace croissante. Les auteures et auteurs de cybermenace ciblent les infrastructures électorales dans le but d'influencer directement le processus électoral. Par exemple, ils peuvent mener des attaques par DDoS, couper l'accès au site Web d'une commission électorale, obtenir l'accès non autorisé à des bases de données électorales par l'entremise d'un courriel d'hameçonnage ou s'en prendre aux infrastructures électorales, comme les machines à voter.

Figure 3 : Infrastructures électorales

Contrairement aux campagnes d'influence qui visent à influencer le comportement de l'électorat, les auteures et auteurs de cybermenace ciblant les infrastructures électorales cherchent à s'en prendre directement aux processus électoraux, à modifier les résultats ou à restreindre l'accès au vote. Les auteures et auteurs de cybermenace peuvent cibler les infrastructures électorales à trois moments : lors de l'inscription des électrices et électeurs, lors du vote et lors de la comptabilisation des votes. Une compromission qui survient à l'une de ces périodes du processus électoral peut mettre en péril l'intégrité d'une élection.

Inscription des électrices et électeurs

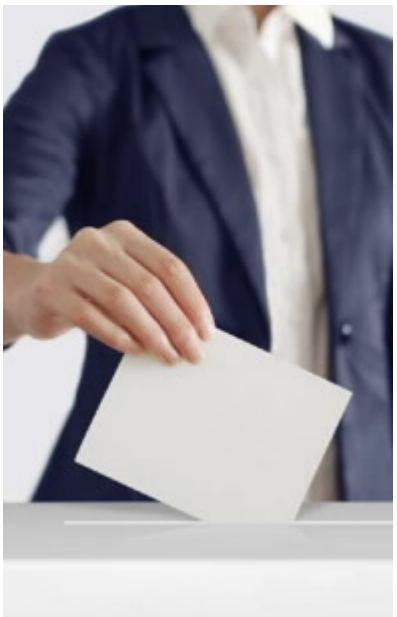
Dans presque tous les pays, les électrices et les électeurs doivent s'inscrire. Au Canada, une personne peut s'inscrire pour voter aux élections nationales au bureau de vote ou en ligne[20]. L'inscription en ligne peut accélérer le processus électoral, et des mesures de sécurité protègent les registres des électrices et électeurs, comme le contrôle de l'accès aux registres, la protection physique du matériel connexe et la fourniture de mesures de sécurité des technologies de l'information (TI) additionnelles. Ces registres contiennent toutefois des données précieuses que les auteures et auteurs de cybermenace malveillants pourraient vouloir cibler. Par exemple, ils pourraient tenter de modifier les dossiers d'électrices et électeurs, d'effacer ou de chiffrer des données, de rendre inaccessible l'inscription ou d'afficher de l'information trompeuse au sujet de l'inscription. Ils pourraient également tenter de contourner les mesures de sécurité pour accéder aux bases de données électorales et utiliser les renseignements personnels qui s'y trouvent pour cibler les électrices et électeurs. Par exemple, le 22 octobre 2022, le Federal Bureau of Investigation (FBI) et la Cybersecurity and Infrastructure Security Agency (CISA) ont dénoncé publiquement une campagne iranienne ayant pour but d'obtenir l'information de l'électorat américain et d'envoyer des messages menaçants afin d'intimider les électrices et les électeurs et de propager de la désinformation sur l'élection[21].

Dépôt du bulletin de vote

Une fois que leur identité est confirmée, les électrices et électeurs peuvent inscrire leur vote sur papier ou en sélectionnant une option sur un écran. Au Canada, les élections fédérales n'acceptent que les bulletins de vote papier. Dans d'autres pays, comme les États-Unis, la France et le Brésil, se servent de machines de vote direct par voie électronique (machines DRE pour *direct-recording electronic*), communément appelées « machines à voter », lors de leurs élections[22]. Les machines DRE peuvent être trafiquées par des auteures et auteurs de menace malveillants, et les spécialistes de la cybersécurité ont démontré par le passé que ces systèmes ont plusieurs vulnérabilités[23]. Depuis 2023, 11 pays ont abandonné le vote électronique en raison de préoccupations liées à la sécurité des votes et à la confiance envers le vote[24]. Certaines machines DRE n'enregistrent pas le choix des électrices et électeurs sur papier, ce qui crée des complications au moment de recompter les voix[25].

Comptabilisation des votes et trace écrite

La plupart des pays utilisent une quelconque forme de technologie pour traiter et comptabiliser les votes. Une des technologies les plus courantes pour comptabiliser les votes est une machine à lecture optique. Au Canada, certaines élections municipales ou provinciales se servent de ces machines, mais, au fédéral, le comptage des voix se fait à la main[26]. Les machines à lecture optique analysent les bulletins de vote papier, enregistrent la marque laissée par l'électrice ou l'électeur et stockent les résultats par voie électronique. Ce système permet de comptabiliser rapidement les votes, tout en veillant à ce que les bulletins papier puissent être comparés au dépouillement de la machine. Comme tout autre type de technologie informatique, les lecteurs optiques ne sont pas immunisés contre les compromissions, c'est pourquoi l'accès physique à ces machines doit être protégé de sorte à garantir l'intégrité du logiciel[27]. Sans trace écrite de secours, il devient difficile de détecter les erreurs ou les compromissions des logiciels ou du matériel des machines à voter.

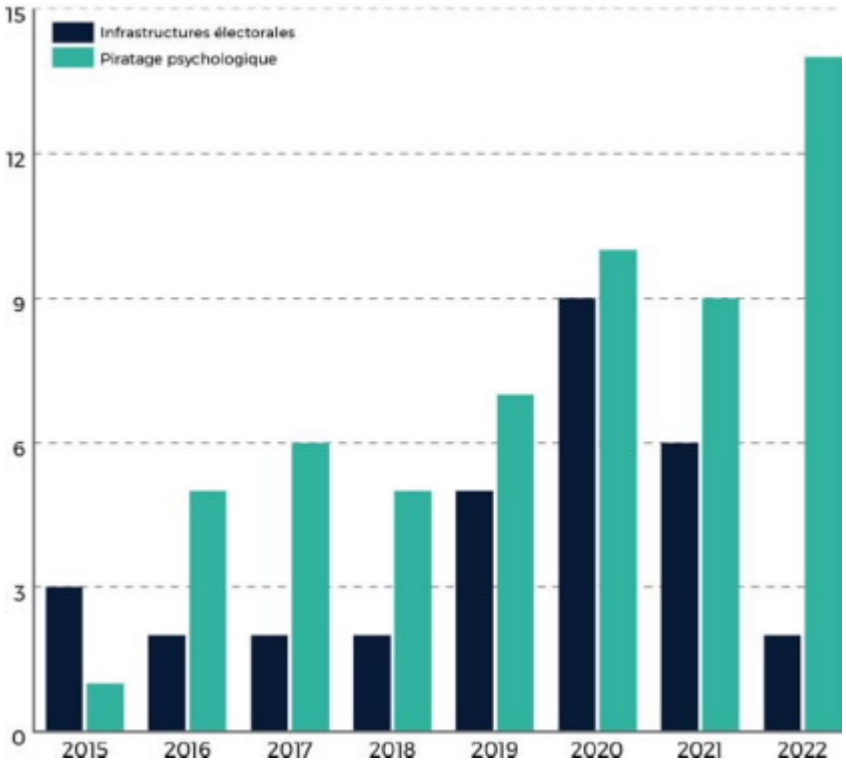


ACTIVITÉS DE CYBERMENACE ET CAMPAGNES D'INFLUENCE

Les activités de cybermenace peuvent produire de la désinformation qui influence les électrices et les électeurs avant les élections. Cette désinformation est un des éléments d'une campagne d'influence électorale de plus grande envergure, dans le cadre de laquelle des auteures et auteurs de cybermenace utilisent des tactiques et des techniques de piratage psychologique pour manipuler les émotions et les comportements de l'électorat[28]. L'accès non autorisé à des informations privilégiées peut influencer le discours public en ligne et, possiblement, affecter l'opinion et les choix électoraux du public. Ce type d'activité de cybermenace peut comprendre le piratage et la divulgation d'information sensible obtenue dans la base de données d'un parti, le piratage d'un compte de média social d'une figure politique afin de publier de la désinformation ou la défiguration du site Web d'un parti politique en y apposant de la désinformation. Au lieu de cibler les infrastructures électorales directement, les auteures et auteurs de cybermenace se serviront de leurs cybercapacités pour influencer ou manipuler l'électorat.

Les cyberactivités ciblant les processus démocratiques dans le monde visent plus souvent à influencer l'électorat avant des élections qu'à s'attaquer aux infrastructures électorales (figure 4). Selon ces constations, nous évaluons que les auteures et auteurs de cybermenace visant les élections préfèrent, en moyenne, manipuler l'environnement d'information plutôt que de tenter d'avoir un impact direct sur le processus électoral.

Figure 4 : Nombre d'incidents observés ciblant des élections nationales par l'entremise des infrastructures électorales et du piratage psychologique par année



Il y a plusieurs raisons qui expliquent la préférence de passer par le piratage psychologique au lieu de cibler des infrastructures électorales, notamment :

- choisir parmi un plus grand ensemble de cibles;
- avoir besoin de moins de tactiques, de techniques et de procédures (TTP) sur mesure pour accéder à de l'information privilégiée;
- cibler de sources d'information qui ne sont pas protégées par une équipe de TI (par exemple, obtenir de l'information en accédant au compte de courriel personnel d'une ou d'un membre du personnel politique);
- justifier le piratage et la divulgation comme geste altruiste qui fournit au public de l'information importante qu'il « devrait connaître »;
- faire en sorte qu'une firme de marketing ou de relations publiques prenne en charge des activités d'influence;
- pouvoir nier de façon plausible, c'est-à-dire que le fait de cibler l'électorat est moins direct et plus difficile à retracer.

Adversaires étrangers menant des campagnes d'influence

Les activités de cybermenace des adversaires étrangers tenteront d'influencer les élections en créant de la désinformation, en la faisant circuler ou en l'amplifiant dans les espaces publics en ligne. L'objectif des adversaires est de manipuler la population d'un pays secrètement, en espérant que le résultat des élections correspondra à leurs objectifs stratégiques à l'étranger. Il est possible également que les adversaires considèrent que le fait de cibler l'électorat risque de moins faire escalader les tensions que le fait de cibler les infrastructures électorales d'un pays. Les adversaires étrangers tenteront tout de même de masquer leur implication dans les campagnes d'influence et les cyberactivités qui alimentent ces campagnes d'influence. La géomystification et les plateformes de messagerie chiffrée complexifient l'identification de l'origine de la désinformation[29]. Dans certains cas, c'est une partie tierce qui effectuera les campagnes d'influence visant les élections. Ces parties tierces, aussi appelées « entreprises d'influence onéreuses », font partie d'une industrie florissante en pleine croissance depuis 2019. Des chercheuses et chercheurs à l'Oxford Internet Institute ont découvert 48 situations où des États ont travaillé avec des entreprises d'influence onéreuses de 2019 à 2020, une augmentation de 128 % depuis la période entre 2017 et 2018[30]. Les adversaires étrangers utiliseront également des réseaux de zombies afin d'amplifier certains messages en ligne et d'acheminer du contenu aux électrices et électeurs ayant les mêmes opinions politiques, ce qui a pour effet d'accentuer les répercussions des chambres d'écho politiques et la polarisation politique avant des élections[31]. Selon nos observations, ces campagnes d'influence propagées par des auteures et auteurs de cybermenace parrainés par des États représentent presque certainement une menace constante et persistante pour la population canadienne.

Environnement de nouvelles en ligne

La *Loi sur les nouvelles en ligne* exige que les entreprises de technologie rémunèrent les médias canadiens pour le contenu de nouvelles qui apparaît sur leurs plateformes en ligne. Certaines entreprises de technologie refusent de se conformer à la Loi et bloqueront les nouvelles de source canadienne de leurs plateformes. En 2019, près de 50 % de la population canadienne âgée de 18 à 24 ans utilisait les médias sociaux comme principale source de nouvelles.[32] Nous estimons que, en l'absence de nouvelles de sources canadiennes, les jeunes Canadiennes et Canadiens risquent probablement beaucoup plus d'être exposés à du contenu de nouvelles trompeur, qui pourrait faire partie de campagnes de désinformation ou d'influence plus générales.

L'IA GÉNÉRATIVE MENACE LES PROCESSUS DÉMOCRATIQUES

L'IA générative peut produire divers types de contenus, dont des textes, des images, du contenu audio et des vidéos, parfois appelés « hypertrucages ». Ce contenu synthétique peut servir dans le cadre de campagnes d'influence pour manipuler secrètement l'information en ligne et, du même coup, influencer les opinions et les comportements des électrices et des électeurs. Malgré les avantages possibles sur le plan créatif, la capacité de l'IA générative à polluer l'écosystème d'information par la désinformation menace les processus démocratiques partout dans le monde.

Récemment, l'IA générative a gagné en popularité, car sa capacité de production de contenu synthétique (textes, images ou vidéos) est rendue accessible par l'entremise de grandes entreprises de technologie telles que Meta, Google et OpenAI. Malheureusement, les auteures et auteurs de cybermenace se servent aussi de ces capacités afin de générer ou d'amplifier la désinformation en ligne. Entre août 2019 et janvier 2021, la surveillance de parties tierces a relevé une augmentation des activités sur le Web clandestin liées à l'hypertrucage, de même qu'une augmentation de la publicité d'offres personnalisées de services d'hypertrucage[33]. Nous estimons qu'il est très probable que les auteures et auteurs de cybermenace se serviront de plus en plus de l'IA générative dans le cadre de campagnes d'influence visant les processus électoraux.

L'apprentissage automatique

L'IA générative est une forme de mise en application de l'apprentissage automatique. L'apprentissage automatique permet aux ordinateurs d'apprendre comment effectuer une tâche à partir des données fournies sans avoir à programmer explicitement une solution étape par étape. Les programmes d'apprentissage automatique ont tellement progressé qu'il est souvent presque impossible de discerner le contenu qu'ils produisent du contenu créé par un humain.[34]

Figure 5 : Types de contenu synthétique créé par IA générative

Dans la plupart des cas, la source de désinformation générée par IA est inconnue. Cependant, nous estimons qu'il est très probable que les adversaires étrangers ou les hacktivistes se serviront de l'IA générative pour influencer le vote lors des prochaines élections fédérales du Canada. Nous avons observé que les auteures et auteurs de cybermenace utilisent déjà cette technologie dans le but de faire avancer leurs objectifs politiques à l'étranger. Par exemple, des auteures et auteurs de cybermenace prorusses ont utilisé l'IA générative pour créer un hypertrucage qui met en scène le président ukrainien Zelensky annonçant la reddition de l'Ukraine à la suite de l'invasion du pays par la Russie[35]. Nous évaluons que les adversaires étrangers et les hacktivistes utiliseront probablement l'IA générative comme d'une arme au cours des deux prochaines années, et ce, dans le but de créer des vidéos et des images hypertruquées où figurent des politiciennes et politiciens et des représentantes et représentants du gouvernement, en plus d'amplifier et d'automatiser les réseaux de zombies non authentiques au moyen de générateurs de textes et d'images.

Vidéos hypertruquées influençant les élections

Le terme « hypertrucage » fait référence à des modèles d'apprentissage automatique qui utilisent des techniques de synthèse d'images et de contenu audio pour générer de fausses vidéos qui semblent réalistes et authentiques. L'IA générative utilise la rétro-ingénierie de véritables contenus vidéo ou audio d'une personne pour imiter de manière convaincante son image et sa façon de s'exprimer et produire une vidéo d'événements qui n'ont jamais eu lieu[36]. Les vidéos hypertruquées de figures politiques risquent de tromper l'électorat et de susciter une polarisation politique accrue. Par exemple, en février 2023, un hypertrucage a circulé sur les médias sociaux dans lequel le Joe Biden faisait des remarques désobligeantes contre les personnes transgenres, en dépit de l'appui public de son administration pour la communauté LGBTQ[37]. Cet exemple, et les milliers d'autres qui circulent sur les médias sociaux, rend difficile la tâche de l'électorat de distinguer les messages politiques réels des faux[38]. La compréhension du public quant à la prévalence des vidéos hypertruquées en ligne peut également faire en sorte qu'il remette en question les sources d'information légitimes. Par exemple, les débats politiques sont une source d'information décisive pour l'électorat dans la période qui précède les jours de scrutin, car ils présentent les plateformes électorales des partis et ont tendance à faire changer les préférences de candidates et candidats des électrices et électeurs[39]. Si des auteures ou auteurs de cybermenace font circuler des hypertrucages modifiant le contenu des débats, il est possible de tromper les électrices et électeurs. Même si la vérité est rétablie par après, le dommage est fait et l'électorat peut remettre en question la légitimité des débats politiques à l'avenir. Bien que les plateformes de médias sociaux, telles qu'Instagram, Facebook et YouTube, fassent l'effort de signaler et de supprimer les hypertrucages de leur plateforme, elles ne sont pas toujours en mesure de détecter et de retirer ce contenu avant qu'il ne soit largement circulé.

La capacité des entreprises de médias sociaux à détecter et à retirer les hypertrucages est complexifiée par les considérations en matière de créativité et de liberté d'expression. Les partis politiques eux-mêmes utilisent des capacités d'IA générative dans le cadre de leurs campagnes, par exemple, pour créer des vidéos illustrant des « scénarios futurs » si leur adversaire politique remporte les élections[40]. Même si des mentions indiquent qu'une vidéo est un hypertrucage, il existe actuellement très peu de réglementations au Canada et aux États-Unis qui établissent la mesure dans laquelle l'IA générative peut être utilisée dans la publicité politique[41].

Réseaux de zombies accentués par les capacités d'IA

Les auteures et auteurs de cybermenace utilisent de faux profils de médias sociaux pour propager ou amplifier la désinformation en prévision des élections[42]. Un groupe de faux profils exploités par des robots logiciels, ou un « réseau de zombies », peut contrôler des comptes de médias sociaux et imiter les actions de véritables utilisatrices et utilisateurs[43]. Les réseaux de zombies peuvent influencer ou mal représenter l'opinion populaire, et les chercheuses et chercheurs concluent que les robots représentent jusqu'à 10 % des comptes participant à des conversations portant sur certains sujets, comme les crises[44]. Il est également connu que les réseaux de zombies amplifient les faussetés sur le plan national ou la désinformation afin d'attiser la polarisation politique au sein du pays. Par conséquent, ils font souvent partie de campagnes d'influence de plus grande envergure, et plusieurs entreprises d'influence onéreuses indiquent offrir ces services[45].

Nous estimons que l'IA générative servira presque certainement de plus en plus à automatiser et à accroître les fonctions des réseaux de zombies au cours des deux prochaines années. Les générateurs de texte par IA, tels que ChatGPT et Bard, sont capables de produire des paragraphes de texte cohérent qu'il est presque impossible de distinguer d'une rédaction humaine[46]. Ces capacités d'IA générative peuvent se transposer aux réseaux de zombie afin d'améliorer les publications et de faire en sorte qu'elles aient l'air d'être écrites par une personne[47]. De plus, les générateurs d'image par IA, tels que GAN Lab, Midjourney ou DALL-E, peuvent fabriquer de fausses images qui sont, dans certains cas, impossibles à distinguer de véritables images[48]. Ces capacités peuvent servir à générer de fausses images de profil pour les comptes de médias sociaux ou du contenu trompeur à publier. Par exemple, en mars 2023, une campagne d'influence gouvernementale prochinoise a utilisé plusieurs images générées par IA pour appuyer des messages qui représentaient négativement des dirigeantes et dirigeants aux États-Unis[49]. Au fur et à mesure que les réseaux de zombies évoluent et que les capacités d'IA générative deviennent plus largement accessibles, il sera plus difficile pour les électrices et électeurs de distinguer la vérité du contenu généré par l'IA.

Nous évaluons qu'il est très probable que la capacité de générer des hypertrucages surpasse notre capacité à les détecter. Les modèles actuels de détection accessibles au public ont du mal à distinguer les hypertrucages du contenu réel. Étant donné l'inefficacité des modèles de détection des hypertrucages et la disponibilité accrue de l'IA générative, il est probable que les campagnes d'influence se servant de l'IA générative pour cibler l'électorat passeront de plus en plus inaperçues dans le grand public. Nous estimons également qu'il est très probable que la technologie, en évoluant, sera mieux en mesure de tromper les modèles de détection, ce qui aura pour effet d'entraver la capacité des entreprises de médias sociaux à détecter et à retirer automatiquement le contenu synthétique avant que l'électorat en prenne connaissance.

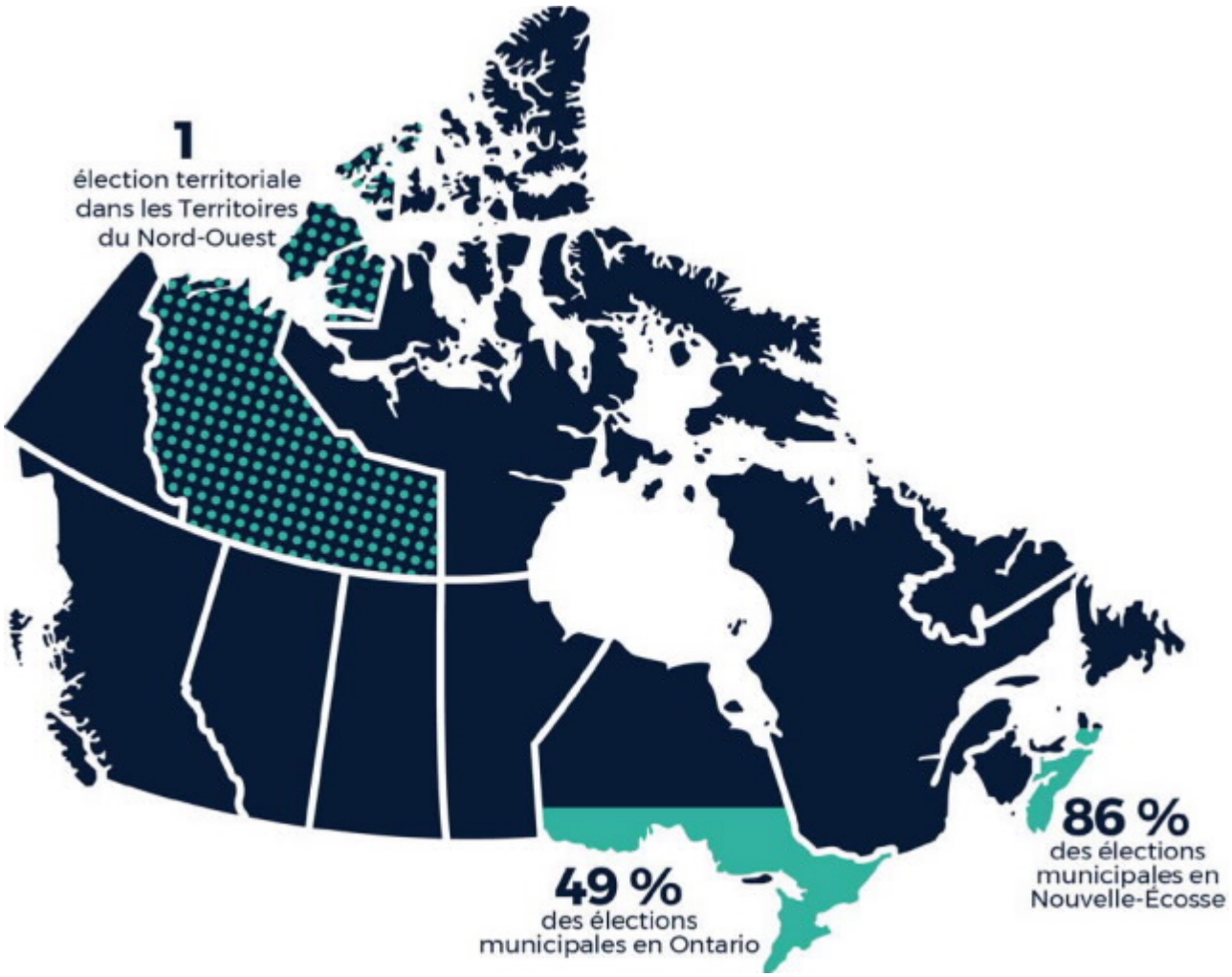
CONSÉQUENCES POUR LE CANADA

Selon nos observations, nous évaluons que de la désinformation à propos des prochaines élections fédérales circulera presque certainement en ligne et que les adversaires étrangers utiliseront probablement l'IA générative pour cibler les élections fédérales canadiennes dans les deux prochaines années. Nous estimons que, dans l'ensemble, le Canada représente une cible d'activités de cybermenace de plus faible priorité que certains de ses alliés, comme les États-Unis et le Royaume-Uni. Cependant, le Canada ne se trouve pas en vase clos, et les cyberactivités qui touchent les processus démocratiques de ses alliés entraîneront probablement des répercussions au Canada aussi. Par exemple, un grand pourcentage de la population canadienne utilise des plateformes américaines de médias sociaux et est souvent exposé aux mêmes hypertrucages et campagnes d'influence étrangère qui ciblent la population américaine[50].

Nous notons également que les quatre tendances mondiales que nous avons relevées auront des conséquences pour le Canada. Le pourcentage de processus électoraux ciblés par des activités de cybermenace a augmenté dans le monde, et, selon cette tendance, nous évaluons que les cyberincidents risquent plus probablement de survenir lors des prochaines élections fédérales canadiennes qu'auparavant. Comme il est indiqué dans l'Évaluation des cybermenaces nationales 2023-2024[51], les activités de cybermenace sont maintenant un outil important pour les États qui souhaitent influencer des événements tout en restant sous le seuil du conflit. Nous jugeons que les activités de cybermenace ciblant les processus démocratiques sont probablement perçues par les adversaires étrangers, tels que la Chine et la Russie, comme une façon obscure et peu risquée d'influencer les résultats politiques au Canada. Nous notons également que l'identification de l'origine des activités de cybermenace visant les élections est de plus en plus difficile, puisque les techniques de camouflage et l'externalisation des activités chez des tiers sont plus répandues. En conséquence, nous estimons qu'il est probable qu'il sera de plus en plus difficile pour le Canada d'attribuer les activités de cybermenace visant ses processus démocratiques à leur origine.

Au Canada, la technologie est utilisée dans tout le processus électoral national et est importante pour assurer l'efficacité et la précision du processus; toutefois, l'absence de bulletins de vote papier comporte des risques. Se fier uniquement aux équipes de criminalistique numérique pour évaluer l'ingérence électorale présente des défis, notamment le signalement d'anomalies comme fraudes dans le vote non frauduleux sans être en mesure de distinguer les cybercompromissions des défectuosités du système. À l'heure actuelle, les élections nationales canadiennes exigent toujours l'utilisation de bulletins papier; toutefois, certaines administrations municipales et certains gouvernements autochtones, provinciaux et territoriaux réfléchissent aux avantages et aux inconvénients du vote électronique[52]. Les Territoires du Nord-Ouest ont utilisé le vote électronique lors des élections territoriales de 2019 et une forte proportion de municipalités en Ontario et en Nouvelle-Écosse adoptent des pratiques de vote électronique. En date du 15 septembre 2023, nous avons relevé que 217 des 444 municipalités de l'Ontario (49 %) et 42 des 49 municipalités de la Nouvelle-Écosse (86 %) ont utilisé le vote électronique lors d'au moins une élection passée. (Figure 6)

Figure 6 : Carte représentant l'utilisation du vote électronique au Canada



Une potentielle ingérence électorale et la suspicion du trafiquage des résultats d'une élection peut venir semer le doute sur la légitimité d'une élection et déclencher des enquêtes sur le processus électoral. Il est difficile d'infirmer les faux messages sur l'ingérence électorale : les aspects techniques des activités de cybermenace ne sont pas toujours faciles à comprendre pour les électrices et électeurs et la portée des cybercompromissions peut être mécomprise ou mésinterprétée.

À L'AVENIR...

Les activités de cybermenace continuent de cibler les processus démocratiques partout dans le monde, et le gouvernement du Canada, le CST et le Centre pour la cybersécurité fournissent des avis et des conseils pour renseigner les Canadiennes et les Canadiens à propos des cybermenaces qui visent les élections canadiennes.

Le Centre pour la cybersécurité offre des avis et des conseils en matière de cybersécurité à tous les partis politiques majeurs, entre autres au moyen de publications comme le Guide de cybersécurité à l'intention des équipes chargées des campagnes électorales[53] et les Conseils en matière de cybersécurité pour les intervenants politiques[54].

Voici d'autres publications du Centre pour la cybersécurité :

- Conseils en matière de cybersécurité à l'intention des organismes électoraux[55]
- Conseils en matière de cybersécurité sur l'intelligence artificielle générative[56]
- Guide sur les facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation[57]

De plus, le Centre pour la cybersécurité collabore étroitement avec Élections Canada afin de protéger les infrastructures de l'organisme, y compris par la publication du rapport « Facteurs à considérer en matière de sécurité pour les systèmes de registre électronique du scrutin[58] ».

Nous encourageons les Canadiennes et les Canadiens à consulter les ressources du Centre pour la cybersécurité, dont les publications « Évaluation des cybermenaces nationales 2023-2024[59] », « Repérer les cas de mésinformation, désinformation et malinformation[60] », ainsi que « Fiche de renseignements à l'intention des électeurs canadiens[61] ». Dans le cadre de sa campagne Pensez cybersécurité[62], 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 EN FIN DE TEXTE

1 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

2 Ces chiffres ne tiennent compte que des activités de cybermenace, et non des activités d'influence étrangère en ligne.

3 Une attaque par déni de service (DoS pour *denial of service*) limite ou bloque l'accès à une ressource précise, comme un site Web. « Lors d'une attaque DoS, la capacité de bande passante de la connexion réseau à un système est épuisée en raison du volume de trafic malveillant ciblant la ressource ou les connexions réseau et les périphériques réseau qui permettent à la ressource de fonctionner. Ce trafic peut être généré par un seul système ou plusieurs systèmes sur Internet, communément appelé attaque par DDoS. » [Traduction] Voir MITRE ATT&CK. « Network Denial of Service » . Octobre 2023.
https://attack.mitre.org/techniques/T1498/ (en anglais seulement)

4 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

5 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

6 https://www.cyber.gc.ca/fr/orientation

7 https://www.pensezcybersecurite.gc.ca/fr/homepage

8 https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

9 https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces

10 https://www.cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

11 La grande majorité des Canadiennes et Canadiens utilise des plateformes de médias sociaux pour obtenir et transmettre de l'information concernant les politiciennes et politiciens, les partis politiques et les élections. En 2022, environ 74 % des personnes âgées de plus de 15 ans utilisaient les médias sociaux et environ 77 % accédaient aux nouvelles en ligne. En 2019, près de la moitié des personnes âgées de 18 à 24 ans consultaient les médias sociaux comme source principale de nouvelle et, de nos jours, ce chiffre est probablement plus élevé.

12 Stephanie Kirchgaessner, Manisha Ganguly, David Pegg, Carole Cadwalladr et Jason Burke. « Revealed: the hacking and disinformation team meddling in elections ». *The Guardian*, 15 février 2023.
https://www.theguardian.com/world/2023/feb/15/revealed-disinformation-team-jorge-claim-meddling-elections-tal-hanan (en anglais seulement)

13 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

14 Ces chiffres ne tiennent compte que des activités de cybermenace, et non des activités d'influence étrangère en ligne.

15 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

16 Craig Silverman, Jane Lytvynenko et William Kung. « Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online ». *Buzz Feed News*. 6 janvier 2020.
https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms (en anglais seulement)

17 Jacob Wallis, Ariel Bogle, Albert Zhang, Hillary Mansour, Tim Niven, Elena Yi-Ching Ho, Jason Liu, Jonathan Corpus Ong et Ross Tapsell. « Influence for hire: The Asia-Pacific's online shadow economy. ». *Australian Strategic Policy Institute - International Cyber Policy Centre*. Août 2021.
https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-08/Influence for hire_0.pdf (en anglais seulement)

18 Recorded Future. « The Business of Fraud: Deepfakes, Fraud's Next Frontier ». 29 avril 2021; Shamani Joshi. « They Follow You on Instagram, Then Use Your Face to Make Deepfake Porn in This Sex Extortion Scam ». *Vice News*. 7 septembre 2021.
https://www.recordedfuture.com/deepfakes-frauds-next-frontier (en anglais seulement)
https://www.vice.com/en/article/z3x9yj/india-instagram-sextortion-phishing-deepfake-porn-scam (en anglais seulement)

19 https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-le-processus-democratique-du-canada-mise-jour-de-juillet-2021

20 Organisation des Nations Unies, « Women and Elections: Basic elements of voter registration ». Mars 2005; Élections Canada. « Le système électoral du Canada ». 17 octobre 2022.
https://www.un.org/womenwatch/osagi/wps/publication/Chapter4.htm (en anglais seulement)
https://www.elections.ca/content.aspx?section=res&dir=ces&document=part5&lang=f

21 Federal Bureau of Investigations Most Wanted. « Iranian Interference in 2020 US Elections. ».

Notes en fin de texte

20 octobre 2021.
https://www.fbi.gov/wanted/cyber/iranian-interference-in-2020-us-elections (en anglais seulement)

22 International Institute for Democracy and Electoral Assistance. « Use of E-Voting Around the World. ». 6 février 2023.
https://www.idea.int/news-media/media/use-e-voting-around-world (en anglais seulement)

23 Sue Halpern. « Election-Hacking Lessons from the 2018 Def Con Hackers Conference ». *The New Yorker*. 23 août 2018; Shaun Nichols. « Expert gives Congress solution to vote machine cyber-security fears: Keep a paper backup ». *The Register*. 1er décembre 2017; Shaun Nichols. « US voting hardware maker's shock discovery: Security improves when you actually work with the community. ». *The Register*. 6 août 2020; Cyberscoop. « DEF CON Voting Village takes on election conspiracies, disinformation ». 17 août 2022.
https://www.newyorker.com/news/dispatch/election-hacking-lessons-from-the-2018-def-con-hackers-conference (en anglais seulement)
https://www.theregister.com/2017/12/01/us_voting_machine_security_hearing/ (en anglais seulement)
https://www.theregister.com/2020/08/06/black_hat_ess_bugs/ (en anglais seulement)
https://cyberscoop.com/defcon-voting-village-harri-hursti-election-fraud/ (en anglais seulement)

24 International Institute for Democracy and Electoral Assistance. « Use of E-Voting Around the World, International Institute for Democracy and Electoral Assistance ». 6 février 2023.
https://www.idea.int/news-media/media/use-e-voting-around-world (en anglais seulement)

25 Certaines machines DRE peuvent laisser une trace écrite, ou un reçu imprimé du vote; toutefois, ce ne sont pas toutes les machines qui peuvent réaliser cette tâche. Voir Raj Karan Gambhir et Jack Karsten. « Why paper is considered state-of-the-art voting technology ». *The Brookings Institution*. 14 août 2019.
https://www.brookings.edu/articles/why-paper-is-considered-state-of-the-art-voting-technology/ (en anglais seulement)

26 International Institute for Democracy and Electoral Assistance. « ICTs in Elections Database ». 29 avril 2019; Paul Laronde. « Les technologies dans le processus de vote : Un aperçu des tendances et initiatives émergentes (Note de recherche) ». *Élections Canada*. Mai 2012; Élections Canada. « Mesures de protection liées au dépouillement du scrutin et à la communication des résultats ». 13 mai 2023.
https://www.idea.int/news-media/media/use-e-voting-around-world (en anglais seulement)
https://www.elections.ca/content.aspx?section=res&dir=rec/tech/note&document=index&lang=f
https://www.elections.ca/content.aspx?section=vot&dir=int/cou&document=index&lang=f

27 En septembre 2007, la secrétaire d'État Debra Bowen a examiné un grand nombre des systèmes de vote certifiés en Californie. Voir California Secretary of State. « Top-to-Bottom Review ». 20 juillet 2007.
https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review (en anglais seulement)

28 IBM. « Qu'est-ce que l'ingénierie sociale? ». 20 novembre 2020.
https://www.ibm.com/fr-fr/topics/social-engineering

29 La géomystification est un processus consistant à modifier ou à cacher l'emplacement d'un appareil sur Internet en simulant que l'appareil se trouve ailleurs. Voir Justin Schamotta. « How to change your location online using geo-spoofing ». *Bleeping Computers*. 20 juin 2023.
https://www.bleepingcomputer.com/vpn/guides/location-geo-spoofing/ (en anglais seulement)

30 Samantha Bradshaw, Hannah Bailey et Philip N. Howard. « Industrialized Disinformation 2020 Global Inventory of Organized Social Media Manipulation ». *Oxford Internet Institute*. 13 janvier 2022.
https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf (en anglais seulement)

31 Emilio Ferrara, Herbert Chang, Emily Chen, Goran Muric et Jaimin Patel. « Characterizing social media manipulation in the 2020 U.S. presidential election ». *First Monday*. Novembre 2020.
https://doi.org/10.5210/fm.v25i11.11431 (en anglais seulement)

32 Sebastien Charlton et Kamille Leclair. « Digital News Report: Canada 2019 Data Overview ». *Centre d'études des médias - Université Laval*. Février 2019.
https://www.cem.ulaval.ca/wp-content/uploads/2019/06/dnr19_can_eng.pdf (en anglais seulement)

33 Recorded Future. « The Business of Fraud: Deepfakes, Fraud's Next Frontier ». 29 avril 2021; Shamani Joshi. « They Follow You on Instagram, Then Use Your Face to Make Deepfake Porn in This Sex Extortion Scam ». *Vice News*. 7 septembre 2021.
https://www.recordedfuture.com/deepfakes-frauds-next-frontier (en anglais seulement)
https://www.vice.com/en/article/z3x9yj/india-instagram-sextortion-phishing-deepfake-porn-scam (en anglais seulement)

34 Thanh Thi Nguyena, Quoc Viet Hung Nguyenb, Dung Tien Nguyena, Duc Thanh Nguyena, Thien Huynh-Thec, Saeid Nahavandid, Thanh Tam Nguyene, Quoc-Viet Phamf et Cuong M. Nguyen. « Deep Learning for Deepfakes Creation and Detection: A Survey ». 26 avril 2021; Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville et Yoshua Bengio. « Generative Adversarial Nets ». Université de Montréal. 10 juin 2014.
https://arxiv.org/pdf/1909.11573.pdf (en anglais seulement)
https://arxiv.org/pdf/1406.2661.pdf (en anglais seulement)

35 Bobby Allyn. « Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn ». *NPR*. 16 mars 2022.
https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia
(en anglais seulement)

36 Adrian Tijie Xu. « AI, Truth, and Society: Deepfakes at the front of the Technological Cold War ». *Medium*. 2 juillet 2019; Christian Vaccari et Andrew Chadwick. « Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception ». *SAGE Journals*. Février 2020.
https://medium.com/gradientcrescent/ai-truth-and-society-deepfakes-at-the-front-of-the-technological-cold-war-86c3b5103ce6 (en anglais seulement)
https://journals.sagepub.com/doi/full/10.1177/2056305120903408 (en anglais seulement)

37 Reuters. « Fact Check-Video does not show Joe Biden making transphobic remarks ». 10 février 2023.
https://www.reuters.com/article/factcheck-biden-transphobic-remarks-idUSL1N34Q1IW (en anglais seulement)

38 Alexandra Ulmer et Anna Tong. « Deepfaking it: America's 2024 election collides with AI boom ». *Reuters*. 30 mars 2023
https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/ (en anglais seulement)

39 John G Geer. « The effects of Presidential debates on the electorate's preferences for candidates ». *American Politics Quarterly*. Octobre 1988.
https://journals.sagepub.com/doi/10.1177/004478088016004005 (en anglais seulement)

40 Ali Swenson. « FEC moves toward potentially regulating AI deepfakes in campaign ads ». *PBS*. 10 août 2023.
https://www.pbs.org/newshour/politics/fec-moves-toward-potentially-regulating-ai-deepfakes-in-campaign-ads (en anglais seulement)

41 Fredreka Schouten. « Federal regulators inch a bit closer to regulating AI in political ads ». *CNN*. 10 août 2023; Paola Ramirez et Pablo Tseng. « What Has the Law Done About "Deepfake"? ». 10 mai 2023.
https://www.cnn.com/2023/08/10/politics/fec-deepfakes-political-ads-regulation/index.html (en anglais seulement)
https://mcmillan.ca/insights/what-has-the-law-done-about-deepfake/ (en anglais seulement)

42 Roberto Rocha et Jeff Yates. « Twitter trolls stoked debates about immigrants and pipelines in Canada, data show ». *CBC News*. 12 février 2019.
https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750 (en anglais seulement)

43 Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, et Matei Ripeanu. « Design and analysis of a social botnet ». *Computer Networks*. 27 juin 2012.
https://doi.org/10.1016/j.comnet.2012.06.006 (en anglais seulement)

44 Shashank Yadav. « Political Propagation of Social Botnets: Policy Consequences ». *Cornell University*, 10 mai 2022; Conrad Nied, Leo Stewart, Emma Spiro, et Kate Starbird. « Alternative Narratives of Crisis Events: Communities and Social Botnets Engaged on Social Media ». *Companion of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Février 2017.
https://arxiv.org/ftp/arxiv/papers/2205/2205.04830.pdf (en anglais seulement)
https://dl.acm.org/doi/10.1145/3022198.3026307 (en anglais seulement)

45 Lena Frischlich, Niels Göran Mede et Thorsten Quandt. « The Markets of Manipulation: The Trading of Social Bots on Clearnet and Darknet Markets ». *Disinformation in Open Online Media*. 29 janvier 2020.
https://link.springer.com/chapter/10.1007/978-3-030-39627-5_8 (en anglais seulement)

46 OpenAI. « Better Language Models and Their Implications ». 14 février 2019.
https://openai.com/research/better-language-models (en anglais seulement)

47 Alex Newhouse, Jason Blazakis et Kris McGuffie. « The industrialization of Terrorist Propaganda; Neural Language Models and the Threat of Fake Content Generation ». *Middlebury Institute of International Studies Center on Terrorism, Extremism and Counterterrorism*. Octobre 2019.
https://www.middlebury.edu/institute/sites/www.middlebury.edu.institute/files/2019-11/The Industrialization of Terrorist Propaganda - CTEC.pdf (en anglais seulement)

48 Ian, J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville et Yoshua Bengio. « Generative Adversarial Nets ». *Université de Montréal*. 10 juin 2014.
https://arxiv.org/pdf/1406.2661.pdf (en anglais seulement)

49 Michelle Cantos, Sam Riddell et Alice Revelli. « Threat Actors are Interested in Generative AI, but Use Remains Limited ». *Mandiant*. 17 août 2023.
https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited (en anglais seulement)

Notes en fin de texte

50 La plupart des Canadiennes et des Canadiens ont vu une forme quelconque de contenu synthétique dans les médias sociaux en raison 1) du volume important de contenu synthétique circulant dans les médias sociaux et 2) de leur grande consommation de contenu de médias sociaux. Les chercheuses et chercheurs de la Queensland University of Technology ont découvert que, en moyenne, plus de 3,2 milliards de photos et 720 000 heures de vidéos sont créées chaque jour et mises en ligne. Ils ont remarqué qu'une grande partie de ce contenu en ligne consistait en des médias synthétiques partagés dans les médias sociaux. En 2018, 78 % de la population canadienne a utilisé au moins un compte de réseautage social et, depuis janvier 2021, on estime que 67,1 millions d'utilisatrices et d'utilisateurs canadiens utilisent les plateformes de médias sociaux Facebook, Instagram, Twitter, TikTok, WeChat et YouTube. Voir Sebastien Charlton et Kamille Leclair. « Digital News Report: Canada, 2019 Data Overview ». Université Laval. 11 juin 2019; Christoph Schimmele, Jonathan Fonberg et Grant Schellenberg. « Évaluations que font les Canadiens des médias sociaux dans leur vie ». Statistique Canada. 24 mars 2021; T.J. Thompson, Daniel Angus, Paula Dootson, Edward Hurcombe et Adam Smith. « Visual Mis/disinformation in Journalism and Public Communications: Current Verification Practices, Challenges, and Future Opportunities ». *Journalism Practice*. Octobre 2020.
https://www.cem.ulaval.ca/wp-content/uploads/2019/06/dnr19_can_eng.pdf (en anglais seulement)
https://www150.statcan.gc.ca/n1/pub/36-28-0001/2021003/article/00004-fra.htm
https://www.researchgate.net/publication/344778089_Visual_Misdisinformation_in_Journalism_and_Public_Communications_Current_Verification_Practices_Challenges_and_Future_Opportunities (en anglais seulement)

51 https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

52 Chelsea Gabel et Nicole Goodman. « Indigenous Experiences with Online Voting ». *First Nation Digital Democracy*. Mai 2021; Nicole Goodman, Jon H. Pammett et Joan DeBardeleben. « Une analyse comparative du vote électronique ». *Élections Canada*. Février 2010; Paul Laronde. « Les technologies dans le processus de vote : Un aperçu des tendances et initiatives émergentes (Note de recherche) ». *Élections Canada*. Mai 2012
http://www.digitalimpactfn.com/wp-content/uploads/2021/05/FN_DIGITAL_REPORT_DIGITAL_FNL6.pdf (en anglais seulement)
https://www.elections.ca/res/rec/tech/ivote/comp/ivote_f.pdf
https://www.elections.ca/content.aspx?section=res&dir=rec/tech/note&document=index&lang=f

53 https://cyber.gc.ca/fr/orientation/guide-de-cybersecurite-lintention-des-equipes-chargees-des-campagnes-electorales

54 https://www.cyber.gc.ca/fr/orientation/conseils-en-matiere-de-cybersecurite-pour-les-intervenants-politiques

55 https://www.cyber.gc.ca/fr/orientation/conseils-en-matiere-de-cybersecurite-lintention-des-organismes-electoraux-itsm10020

56 https://www.cyber.gc.ca/fr/orientation/lintelligence-artificielle-generative-itsap00041

57 https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-lors-de-lutilisation-des-medias-sociaux-dans-votre-organisation

58 https://www.cyber.gc.ca/fr/orientation/facteurs-considerer-en-matiere-de-securite-pour-les-systemes-de-registre-electronique

59 https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024

60 https://www.cyber.gc.ca/fr/orientation/reperer-les-cas-de-mesinformation-desinformation-et-malinformation-itsap00300

61 https://www.cyber.gc.ca/fr/orientation/fiche-de-renseignements-lintention-des-electeurs-canadiens

62 https://www.pensezcybersecurite.gc.ca/fr