ISSN 2564-1395
CAT D95-10F-PDF

Cybermenaces contre le processus démocratique du CANADA

Mise à jour de 2025

Centre de la sécurité des télécommunications Canada
Communications Security Establishment Canada

Canada

Centre de la cybersécurité des télécommunications Canada
1929, chemin Ogilvie
Ottawa (Ontario) 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 Canada (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 pourraient avoir besoin de 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 les menaces extérieures, en vue d'aider à assurer la prospérité, la stabilité et la sécurité du pays. Parmi ces menaces figurent le terrorisme d'origine étrangère, l'espionnage étranger, les cybermenaces, l'enlèvement de Canadiennes et Canadiens à l'étranger et les attentats contre les ambassades canadiennes.

SOMMAIRE

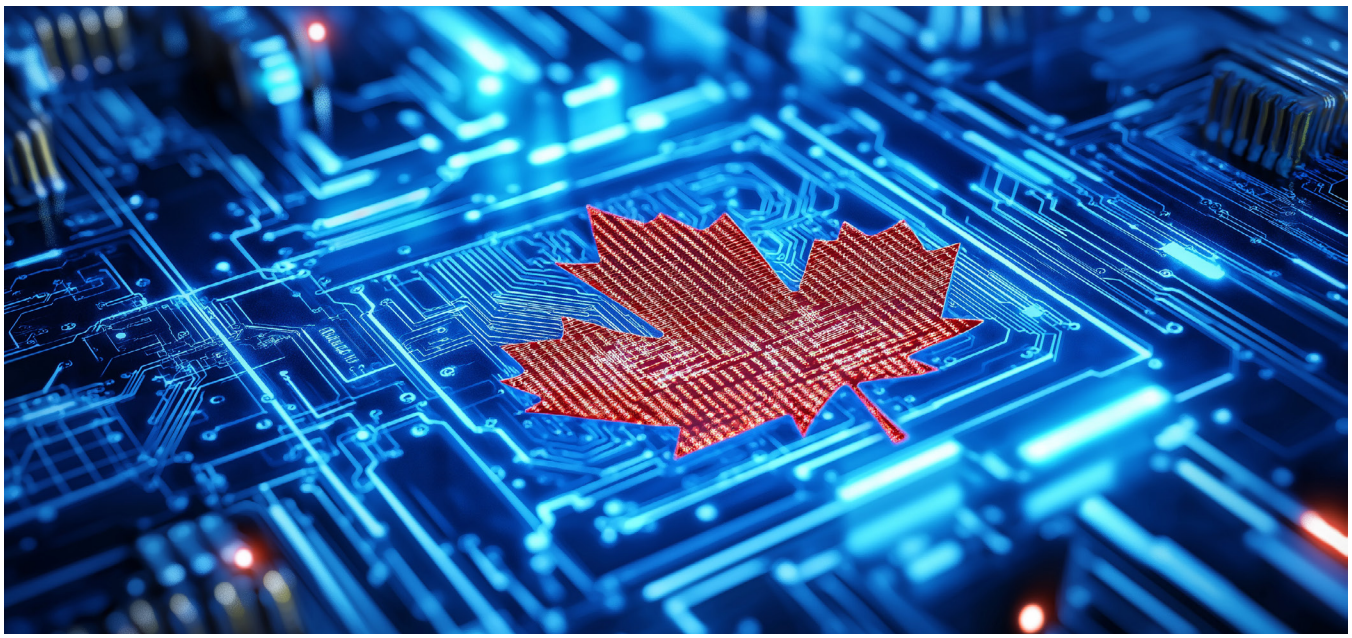
Les auteurs de menace hostiles tirent de plus en plus parti des outils d'intelligence artificielle (IA) pour tenter de s'ingérer dans les processus démocratiques, notamment les élections, partout dans le monde. Ces outils sont devenus plus puissants et plus faciles à utiliser au cours des deux dernières années. Ils jouent maintenant un rôle prépondérant dans la désinformation politique et le harcèlement de personnalités politiques. Ils peuvent également permettre aux auteurs de menace hostiles de se livrer à des activités malveillantes, dont le cyberespionnage.

Le présent rapport se veut une mise à jour de la publication Cybermenaces contre le processus démocratique du Canada : Mise à jour de 2023[1] (CPD de 2023). Bien que les évaluations contenues dans ce rapport demeurent pertinentes, les avancées technologiques rapides réalisées au cours des deux dernières années dans le domaine de l'IA posent un nouveau défi. Par conséquent, cette mise à jour porte exclusivement sur les auteurs de menace et leur utilisation de l'IA pour cibler les processus démocratiques au Canada et ailleurs. Même s'il est difficile de prévoir quelles campagnes de désinformation ou d'influence gagneront en popularité, nous croyons qu'il est très peu probable (c.-à-d. environ 10 % à 30 %) que la désinformation, ou toute cyberactivité facilitée par l'IA, porte fondamentalement atteinte à l'intégrité des processus démocratiques du Canada lors des prochaines élections générales. Parallèlement à l'évolution des technologies d'IA et à la maîtrise de l'IA par les adversaires dans le cyberespace, la menace contre les futures élections générales au Canada risque d'augmenter.

Principales conclusions et tendances mondiales

- Au cours des deux dernières années, les auteurs de menace hostiles ont davantage utilisé l'IA générative pour cibler des élections tenues ailleurs, notamment en Europe, en Asie et dans les Amériques. Alors que le rapport CPD de 2023 a fait état d'un seul cas où l'on a utilisé l'IA générative pour cibler une élection entre 2021 et 2023, nous avons relevé 102 cas signalés d'IA générative utilisée pour entraver ou influencer 41 élections, soit 27 % des élections tenues entre 2023 et 2024. Ces cas concernaient l'utilisation de l'IA pour créer de la désinformation, diffuser activement de la désinformation en ligne et harceler des politiciennes et politiciens. Cette évolution ressort des améliorations au chapitre de la qualité, du coût, de l'efficacité et de l'accessibilité des technologies d'IA.
- Même si nous n'avons pas été en mesure d'associer la majorité des campagnes facilitées par l'IA contre les élections tenues à l'étranger à des auteurs de menace particuliers, notre recherche nous a permis de relever un grand nombre d'activités de menace menées par la Russie et la République populaire de Chine (RPC). Selon nous, il est presque certain que ces États, et de nombreux auteurs de menace non étatiques, tirent parti de l'IA générative pour diffuser de la désinformation, en particulier pour attiser la discorde et la méfiance au sein des sociétés démocratiques. Il est fort probable, selon nous, que la Russie et la RPC continueront d'être les pays auxquels sont associées la plupart des activités de cybermenace et de désinformation facilitées par l'IA ciblant les processus démocratiques des États-nations.

- Un grand nombre d'auteurs de menace utilisent l'IA générative pour polluer l'environnement de l'information. Sur 151 élections tenues dans le monde entre 2023 et 2024, 60 campagnes de désinformation synthétique générées par l'IA et 34 cas connus et probables de réseaux de zombies facilités par l'IA ont été signalés. L'utilisation accrue de l'IA générative représente un changement dans la façon dont la désinformation est créée et diffusée, mais pas dans les motifs sous-jacents et les effets escomptés des campagnes de désinformation. Selon nous, il est probable que de telles campagnes continueront de prendre de l'ampleur à mesure que les technologies d'IA facilitant la désinformation synthétique seront de plus en plus accessibles.
- Selon nous, il est probable que, conformément aux formes de désinformation non facilitées par l'IA, la plupart des contenus créés à l'étranger et générés par l'IA n'acquièrent pas une visibilité importante dans les sociétés démocratiques. Toutefois, l'information qui gagne en visibilité est habituellement amplifiée volontairement ou involontairement par des commentatrices et commentateurs nationaux et transnationaux populaires. De plus, des auteurs de menace étrangers ont démontré la capacité de créer et de faire de la désinformation virale au moyen de l'IA générative. Il est probable, selon nous, que plus les auteurs de menace étrangers perfectionneront leurs méthodes facilitées par l'IA, plus la désinformation qu'ils créent sera visible en ligne. Néanmoins, il demeure difficile de prévoir quel élément de désinformation gagnera en visibilité ou fera écho en ligne.
- L'Évaluation des cybermenaces nationales de 2025-2026[2] (ECMN de 2025-2026) a établi que les cybercriminelles et cybercriminels et les auteurs de menace parrainés par des États utilisent l'IA générative pour accroître le caractère personnel et le pouvoir de persuasion des attaques par piratage psychologique. Nous estimons qu'au cours des deux prochaines années, il est fort probable que les auteurs de menaces intégreront l'IA générative dans les attaques par piratage psychologique contre des personnalités politiques et publiques et contre des administrations électorales. Bien que nous n'ayons pas vu un auteur de menace utiliser l'IA générative pour cibler les élections de cette manière, nous ne pouvons pas exclure la possibilité que cette situation se soit déjà produite.
- Nous estimons également qu'au cours des deux prochaines années, il est probable que les auteurs de menace qui ciblent le Canada recourront à diverses technologies d'IA pour accroître la furtivité et l'efficacité des maliciels qu'ils cherchent à déployer contre des électrices et électeurs, des politiciennes et politiciens, des personnalités publiques et des institutions électorales cibles.



- Les États-nations, en particulier la RPC, mènent de vastes campagnes de collecte de données, recueillant des milliards de points de données sur des politiciennes et politiciens démocratiques, des personnalités publiques et des gens du monde entier. Les percées en IA prédictive permettent aux analystes humaines et humains de rechercher et d'analyser rapidement ces données. Nous sommes d'avis que de tels États comprendront vraisemblablement mieux les environnements politiques démocratiques en conséquence. Dotés des profils détaillés des principales cibles, des réseaux sociaux et des caractéristiques psychographiques des électrices et électeurs, les auteurs de menace améliorent sans doute leur capacité de mener des campagnes d'influence et d'espionnage ciblées.
- Les cybercriminelles et cybercriminels et les auteurs de menace non étatiques utilisent l'IA générative pour créer des hypertrucages pornographiques de politiciennes et politiciens et de personnalités publiques — les personnes ciblées étaient presque toutes des femmes. Bien que la plupart des cas ne semblent pas avoir fait partie d'une campagne d'influence délibérée, les hypertrucages pornographiques dissuadent les personnes ciblées de participer au processus démocratique. De plus, nous croyons que, à au moins une occasion, ce contenu a vraisemblablement été créé dans le but de saboter délibérément la campagne d'une candidate ou d'un candidat. Nous estimons que, compte tenu de l'accès répandu à ces modèles, le nombre d'attaques personnelles facilitées par l'IA augmentera sûrement.

Principaux termes

Apprentissage automatique : Méthodes ou modèles qui permettent aux machines d'apprendre comment effectuer une tâche à partir des données fournies sans avoir à programmer explicitement une solution étape par étape.

IA générative : Branche de l'apprentissage automatique qui génère du nouveau contenu à partir de modèles extraits de grandes quantités de données d'entraînement. L'IA générative peut créer du contenu dans divers formats, comme du texte, des images, des fichiers audio ou vidéo et du code de logiciel.

IA prédictive : Branche de l'apprentissage automatique qui consomme des données d'entrée, mais qui, au lieu de produire une image ou un texte, relève des schémas de données pour classer de nouvelles données, comme des images dans la reconnaissance d'objets ou des mots dans la reconnaissance vocale.

À PROPOS DU PRÉSENT RAPPORT

Le rapport se veut une mise à jour au rapport CPD de 2023, publié en décembre 2023. Compte tenu de l'évolution de l'IA et des technologies d'apprentissage automatique depuis, le rapport porte sur la menace que représentent les auteurs de menace hostiles qui utilisent ces technologies pour cibler le processus démocratique du Canada en 2025. Les principales constatations présentées dans le rapport CPD de 2023 demeurent pertinentes dans l'environnement de menace actuel.

Portée

Le présent rapport traite des cybermenaces facilitées par l'IA qui touchent les processus démocratiques à l'échelle mondiale. Une activité de cybermenace (p. ex. harponnage, maliciel) est une activité facilitée par l'IA qui intègre des composants intelligents (IA générative ou autres méthodes d'apprentissage automatique) pour 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. Le rapport traite également des campagnes d'influence facilitées par l'IA, qui se produisent lorsque les auteurs de cybermenace utilisent l'IA générative et l'IA prédictive pour effectuer des recherches sur les cibles de renseignement et pour manipuler secrètement l'information en ligne.

Enfin, le rapport 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 générales au Canada, prévues en 2025. La prestation de conseils sur l'atténuation des menaces ne s'inscrit pas dans la portée du présent rapport.

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.

Information supplémentaire

Des ressources se trouvent sur la page de conseils sur la cybersécurité du Centre pour la cybersécurité[3] et sur le site Web de Pensez cybersécurité[4].

Pour en savoir plus sur les cyberoutils et le contexte en évolution des cybermenaces, veuillez consulter les publications suivantes :

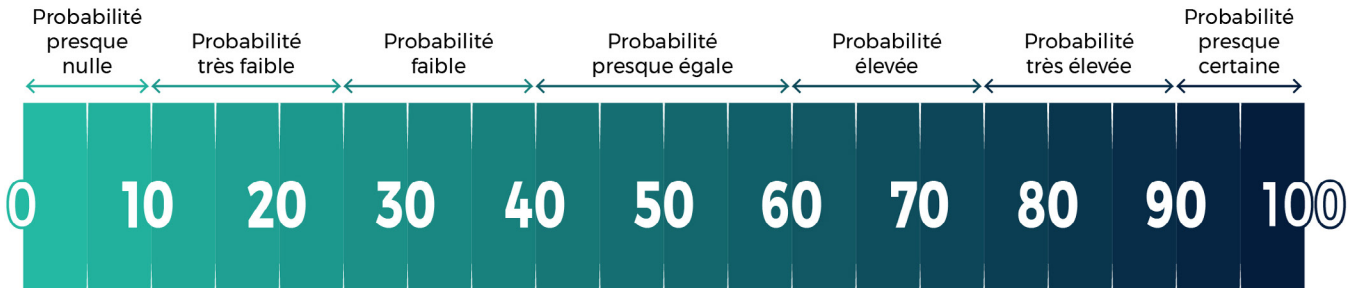
- Évaluation des cybermenaces nationales 2025-2026[5]
- Introduction à l'environnement de cybermenaces[6]
- Repérer les cas de mésinformation, désinformation et malinformation[7]

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. Le Centre pour la cybersécurité utilise 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 présent rapport est basé sur des renseignements disponibles en date du **27 janvier 2025**.

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

Comparativement aux versions précédentes du rapport « Cybermenaces contre le processus démocratique du Canada », lesquelles portaient sur la cybermenace générale ciblant les élections nationales, cette mise à jour porte exclusivement sur la menace posée par l'IA. Elle présente des renseignements sur la façon dont les auteurs de cybermenace utilisent les percées percutantes dans le domaine de l'IA, en particulier l'IA générative et l'IA prédictive, pour cibler le processus électoral, nuire aux protagonistes démocratiques, et tromper et désinformer les électrices et électeurs.

Les élections au Canada : Une cible de choix pour les auteurs de menace étrangers

Les auteurs de menace étrangers souhaitent cibler les élections au Canada pour de nombreuses raisons. Le Canada est membre de l'Organisation du Traité de l'Atlantique Nord (OTAN) et de l'alliance du renseignement de la collectivité des cinq. De plus, l'économie et la culture du pays sont liées à celles des États-Unis.

En tant qu'intervenant jouant un rôle actif au sein de la communauté internationale, le Canada participe à des institutions clés comme l'Organisation des Nations Unies (ONU), l'Organisation de coopération et de développement économiques (OCDE), l'Organisation mondiale du commerce (OMC), le Fonds monétaire international (FMI) et la Banque mondiale. En tant que grande puissance économique, le Canada est membre de l'Accord de partenariat transpacifique global et progressiste (PTPGP) et de forums multilatéraux comme le Groupe des 20 (G20) et le Groupe des 7 (G7). Les décisions du gouvernement du Canada sur des questions militaires et en matière de commerce, d'investissement et de migration ont toutes des répercussions sur la collectivité mondiale, tout comme les produits de la culture et de la science du pays. Il est presque certain, selon nous, que les auteurs étrangers ciblent les élections au Canada pour influencer la façon dont ces décisions sont prises, ainsi que pour affaiblir complètement notre capacité à prendre des décisions.

Les cybermenaces facilitées par l'IA contre le processus démocratique du Canada

L'utilisation malveillante de l'IA est une menace croissante qui pèse sur les élections au Canada, un fait soulevé pour la première fois dans la publication Le point sur les cybermenaces contre le processus démocratique du Canada en 2019[8]. À l'époque, l'IA générative était coûteuse et nécessitait des connaissances techniques. Elle est depuis moins coûteuse et plus accessible aux utilisatrices et utilisateurs non spécialisés. Des interfaces Web conviviales, des invites faciles et peu de règlements ou de mesures de protection permettent à un plus grand nombre d'auteurs de menace de se livrer à des cyberactivités malveillantes[9]. La qualité des modèles d'IA générative produits, et la vitesse à laquelle ces modèles sont produits, se sont également nettement améliorées; par exemple, du premier transformateur génératif pré-entraîné (GPT-1) au quatrième transformateur génératif pré-entraîné (GPT-4) auquel on recourt maintenant pour générer du contenu synthétique de haute qualité[10]. Ces technologies et les technologies connexes ont permis aux auteurs antagonistes de générer des hypertrucages persuasifs et de créer des agents conversationnels convaincants à même de faire de la désinformation adaptée à leur public cible. On a également recouru à la personnalisation du contenu en fonction de cibles précises à partir de l'IA générative pour améliorer les attaques par hameçonnage et pour permettre de nouvelles formes de harcèlement numérique, de cybercriminalité et d'espionnage.

L'analyse prédictive permet le traitement des données à un niveau de sophistication et à un volume impossibles à atteindre par des méthodes non facilitées par l'IA, ce qui permet aux analystes humaines et humains d'identifier rapidement des cibles pour des opérations de piratage potentielles ou des populations susceptibles d'être inondées de propagande ciblée[11].

Un meilleur accès à l'IA générative accroît le risque pour des pays comme le Canada, dont la population et l'infrastructure sont très branchées. Selon le rapport de DataReportal, 94,3 % des Canadiennes et Canadiens sont des utilisateurs inscrits d'Internet, tandis que 80 % d'entre eux utilisent activement les médias sociaux[12]. Les données d'enquête de Statistique Canada indiquent que la majorité de la population canadienne tire ses nouvelles et ses informations d'Internet ou des médias sociaux, ce qui accroît son exposition aux campagnes d'influence malveillantes facilitées par l'IA[13].

Bien que les élections générales au Canada se déroulent par bulletin de vote papier, une grande partie de l'infrastructure électorale est numérisée, notamment les systèmes d'inscription des électrices et électeurs, les sites Web consacrés aux élections et les communications entre les administrations électorales et leur personnel. Cette situation crée une exposition aux menaces sensible aux cyberactivités malveillantes visant à compromettre la confidentialité, l'intégrité ou la disponibilité du système sous-jacent avant ou pendant une période électorale. Les auteurs de cybermenace peuvent utiliser l'IA générative pour créer rapidement des courriels d'hameçonnage ciblés et convaincants, ce qui pourrait leur permettre d'accéder illégalement à cette infrastructure, où ils peuvent installer des maliciels ou exfiltrer et exposer des renseignements de nature délicate[14].

La population canadienne et ses données, ainsi que les organisations publiques et politiques, sont toutes des cibles potentielles des opérations d'influence facilitées par l'IA. Les politiciennes et politiciens, les candidates et candidats et les personnalités des médias ont pratiquement tous une présence en ligne à partir de laquelle des données peuvent être extraites et utilisées pour créer du faux contenu. Les partis politiques du Canada détiennent des téraoctets* de données d'importance politique sur les électrices et électeurs canadiens, tout comme les courtières et courtiers en données commerciales[15].

* Un téraoctet équivaut à environ 500 heures de vidéo HD ou 6,5 millions de pages d'information stockées en format PDF.

Des auteurs de menace affiliés à la RPC volent les données des registres électoraux au Royaume-Uni

En juillet 2024, le gouvernement britannique a indiqué que des auteurs de menace affiliés à la RPC étaient à l'origine d'un piratage de la commission électorale du Royaume-Uni. Les pirates informatiques ont eu accès aux courriels de la commission et à des copies des registres électoraux contenant le nom et l'adresse des personnes inscrites pour voter entre 2014 et 2021[16]. Les auteurs de cybermenaces facilitées par l'IA peuvent utiliser de telles données pour mettre en place des campagnes de propagande adaptées à certains auditoires.

Selon nous, des auteurs de menace étrangers tentent presque assurément d'acquérir ces données, qu'ils peuvent ensuite utiliser contre les processus démocratiques canadiens. Les auteurs de cybermenace peuvent combiner des données achetées ou volées et des données publiques sur les Canadiennes et Canadiens pour créer des campagnes de propagande ciblées fondées sur l'analyse prédictive et le contenu généré par l'IA[17]. Les auteurs de cybermenace malveillants ont également utilisé des réseaux de zombies pour tirer parti d'algorithmes de recommandation dans les médias sociaux, amplifier les campagnes de désinformation et même communiquer directement avec les électrices et électeurs d'autres pays[18]. En fonction de cette capacité, nous croyons que les auteurs de cybermenace peuvent presque certainement cibler les électrices et électeurs canadiens de la même façon.

Nous estimons que les pays qui adoptent des stratégies antagonistes contre le Canada et ses alliés possèdent presque certainement les capacités décrites ci-dessus. Selon nous, il est fort probable que la RPC utilisera ces capacités pour promouvoir des discours favorables à ses intérêts et faire de la désinformation chez les électrices et électeurs canadiens. En ce qui concerne la Russie et l'Iran, nous sommes d'avis que les élections canadiennes sont presque certainement moins prioritaires que les élections américaines ou britanniques. Nous croyons également que, si ces États ciblent le Canada, ils sont plus susceptibles de mener des opérations de cybermenace ou d'influence à faible effort.

Les auteurs de menace du pays, ainsi que les membres de groupes militants et les adeptes de sensations fortes à l'étranger, ont également accès à des outils d'IA générative commerciaux. Nous estimons que de tels auteurs de menace utiliseront presque certainement ces outils pour faire de la désinformation avant une élection nationale. Nous croyons que les tensions géopolitiques accrues entre le Canada et d'autres États inciteront sûrement des auteurs de cybermenace, y compris des auteurs non étatiques, à utiliser des outils facilités par l'IA pour cibler le processus démocratique du Canada. Avant les élections générales de 2021, par exemple, des auteurs qui ont ou auraient des liens avec la RPC ont fait de la désinformation sur les politiciennes et politiciens qui briguaient les suffrages, qu'ils considéraient comme étant anti-RPC[19].

ÉVOLUTION DES TECHNOLOGIES D'IA

L'IA générative est un type d'intelligence artificielle qui génère du nouveau contenu en modélisant les caractéristiques des données tirées des grands jeux de données. L'IA générative peut créer du nouveau contenu sous de nombreuses formes, comme du texte, des images, des fichiers audio ou du code machine. Tout comme l'IA générative, l'IA prédictive consomme des données d'entrée, mais au lieu de produire des images ou du texte, elle applique les modèles découverts afin de faire des prévisions éclairées pour classer de nouvelles données. Par conséquent, les logiciels peuvent évaluer rapidement de grandes réserves de données afin de dégager des modèles et d'effectuer des analyses qui autrement exigeraient qu'une annotation soit faite manuellement par des humains, ce qui serait long et coûteux. Les deux types d'IA reposent sur l'apprentissage automatique, un processus par lequel les machines apprennent à effectuer une tâche à partir des données fournies sans avoir à programmer explicitement une solution étape par étape.

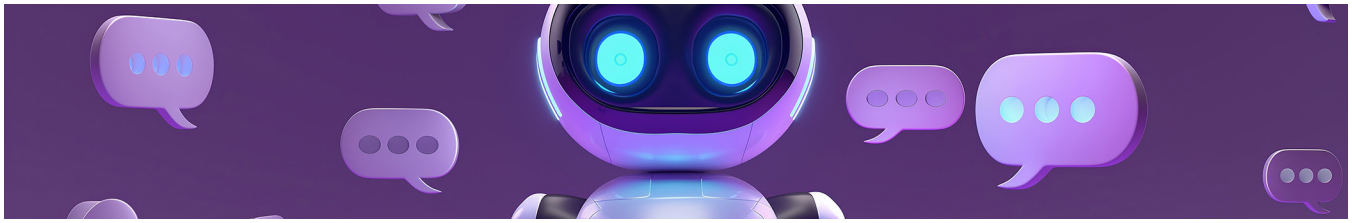
Modèles de langage de grande taille

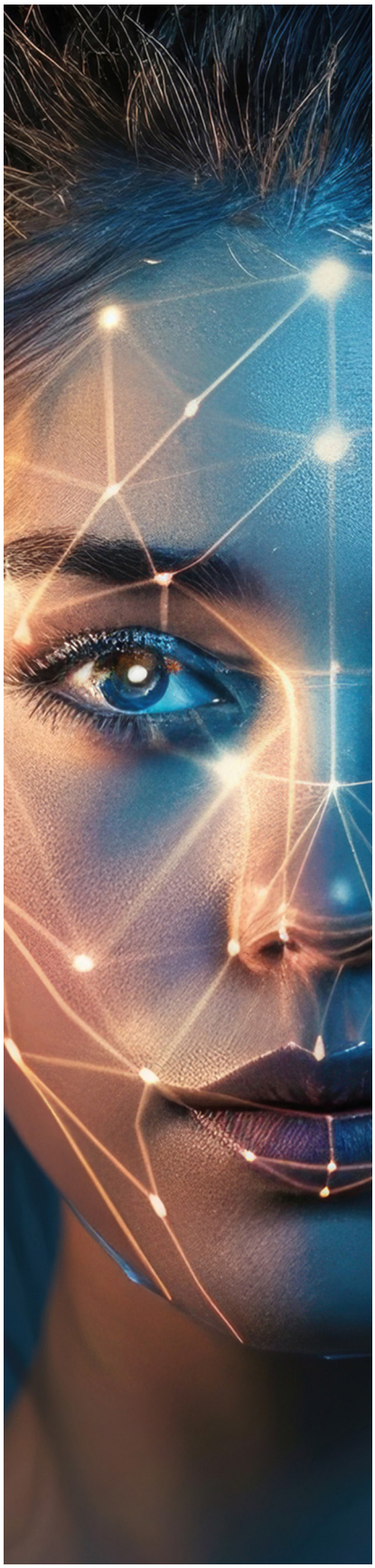
Les modèles de langage de grande taille (LLM pour *large language model*) sont des modèles d'apprentissage automatique qui sont entraînés sur de très grands jeux de données linguistiques utilisant l'apprentissage autosupervisé ou semi-supervisé. Les premiers modèles de langage généraient du texte en prédisant le mot suivant, mais les plus récents modèles se sont grandement appuyés sur cette fonction — en apprenant de très grands jeux de données textuelles et d'une modélisation sophistiquée — afin de permettre aux utilisatrices et utilisateurs de taper du texte dans des applications comme ChatGPT à l'invite pour produire des phrases complètes ou générer des documents complets sur un sujet donné, selon un style donné[20].

L'accessibilité croissante et le coût réduit de ces technologies ont permis leur utilisation à des fins de cybercriminalité et de désinformation et dans les attaques contre l'infrastructure démocratique[21]. Au moyen d'un faux compte ou d'un compte compromis, un auteur de menace peut utiliser un LLM pour rédiger une communication plausible qui amène la personne ciblée à cliquer sur un lien malveillant ou à transmettre par inadvertance ses justificatifs d'identité ou des renseignements sensibles.

Les LLM peuvent produire rapidement des produits d'hameçonnage personnalisés

Pour démontrer la menace potentielle, un chercheur de l'Université d'Oxford a utilisé ChatGPT et d'autres LLM pour rédiger (mais pas envoyer) des courriels de harponnage personnalisés à plus de 600 députées et députés du Parlement britannique[22]. La recherche a montré que les LLM peuvent produire ces courriels beaucoup plus rapidement que les chercheuses et chercheurs humains et sont capables de persuader les personnes ciblées de cliquer sur des liens malveillants à des taux comparables aux courriels d'hameçonnage créés par des humains[23].





Montée des hypertrucages

Les hypertrucages désignent le contenu pictographique, vidéo et audio qui a été produit ou modifié au moyen d'un modèle d'apprentissage automatique. On peut les distinguer des « piètres copies », qui sont également conçues pour la tromperie, mais qui, parce qu'elles sont produites à partir d'un logiciel moins sophistiqué, sont de moindre qualité et sont plus faciles à identifier[24].

La technologie d'hypertrucage, qui existe depuis 2014, était difficile à utiliser et nécessitait des ressources informatiques considérables, jusqu'à ce que des modèles de génération d'images comme GPT, DALL-E et Midjourney soient lancés en 2021-2022[25]. Aujourd'hui, on peut créer un hypertrucage convaincant à partir de quelques secondes de vidéo ou d'audio seulement, ce qui nécessite peu d'expertise technique de la part de l'utilisatrice ou utilisateur[26].

Les hypertrucages sont utilisés contre des élections à l'échelle mondiale, principalement pour diffuser de la désinformation[27]. Un auteur de menace malveillant peut également utiliser une voix ou un appel vidéo hypertruqué pour amener une personne ciblée à transmettre de l'information sensible. Bien que nous n'ayons pas encore observé cette situation dans le contexte d'une élection, les cybercriminelles et cybercriminels ont utilisé l'IA générative efficacement de cette façon pour commettre des fraudes de plusieurs milliards de dollars[28].

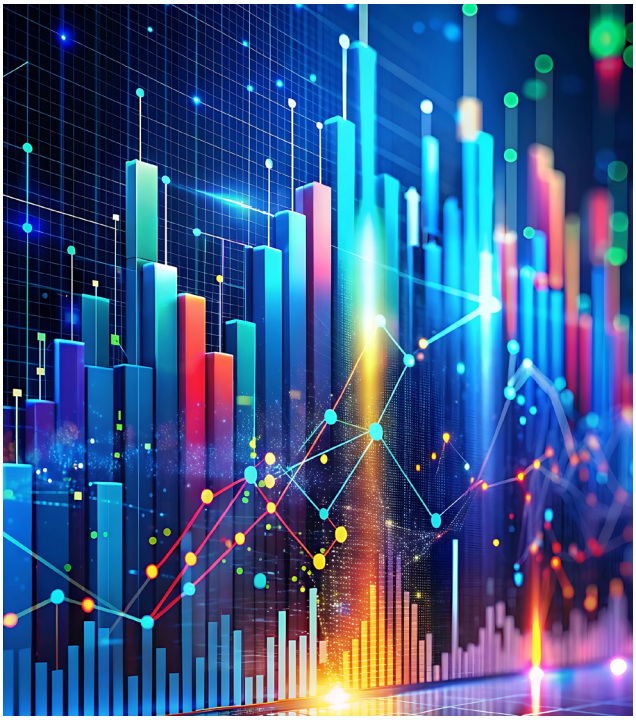
Des fraudeurs utilisent l'IA pour voler 35 millions de dollars

En 2024, des pirates informatiques ont utilisé un hypertrucage pour se faire passer pour la dirigeante principale ou le dirigeant principal des finances d'une entreprise à Hong Kong. Au cours d'un appel vidéo avec une employée ou un employé des services financiers, les pirates informatiques ont amené cette personne à transférer près de 35 millions de dollars canadiens dans leurs comptes bancaires[29].

Analyse basée sur l'apprentissage automatique et exploitation des mégadonnées

Les modèles d'apprentissage automatique sont des outils d'analyse de mégadonnées puissants. Les jeux de données principaux sont créés par la collecte, l'achat ou l'acquisition d'énormes quantités de données mesurées en pétaoctets ou exaoctets*. Le stockage, l'interrogation et l'analyse de ces données exigent des ordinateurs puissants. Les progrès réalisés dans les domaines de la conception des puces, de l'architecture logicielle et de la puissance de traitement ont permis d'effectuer des analyses avancées; par conséquent, les mégadonnées peuvent être traitées plus rapidement et plus précisément[30].

Les entreprises de médias sociaux recourent à l'analyse basée sur l'apprentissage automatique pour repérer et promouvoir le contenu jugé le plus susceptible de capter et de retenir l'attention d'une utilisatrice ou un utilisateur. Les plateformes de médias sociaux ont conçu leurs algorithmes de recommandation basés sur l'apprentissage automatique pour favoriser un contenu polémique et chargé d'émotivité pouvant servir à désinformer, à radicaliser et diviser les utilisatrices et utilisateurs[31]. Les auteurs de menace malveillants peuvent exploiter ces algorithmes pour promouvoir leurs discours politiques privilégiés avant des élections. On note également que certaines plateformes amplifient le contenu biaisé[32].



Entre les mains des auteurs de menace antagonistes, les mégadonnées peuvent être exploitées par apprentissage automatique afin de fournir du renseignement qui permet à ces auteurs d'influencer des personnes ciblées, notamment au moyen d'opérations nécessitant une intervention humaine et de propagande ciblée[33]. L'exploitation statistique des données, par exemple, peut produire des profils d'utilisatrices et utilisateurs — ou de l'information psychographique personnalisée pour chaque électrice ou électeur ou groupe d'électrices et électeurs, reflétant leurs attitudes, leurs aspirations, leurs valeurs et leurs craintes[34]. De même, l'analyse de données en temps réel, capable de recueillir et de traiter des données dès leur création, permet de la rétroaction instantanée et des rapports de renseignement sur demande[35].

Des organes de propagande russes achètent de la publicité ciblée pour cibler les élections fédérales américaines

Selon le Federal Bureau of Investigation (FBI) des États-Unis, à l'automne 2023, les organes de propagande russes ont acheté les services de publicité de Meta, qui s'appuient sur l'IA prédictive, pour diriger la propagande vers des groupes que les organismes russes avaient jugés réceptifs à leur interprétation de certains faits[36].

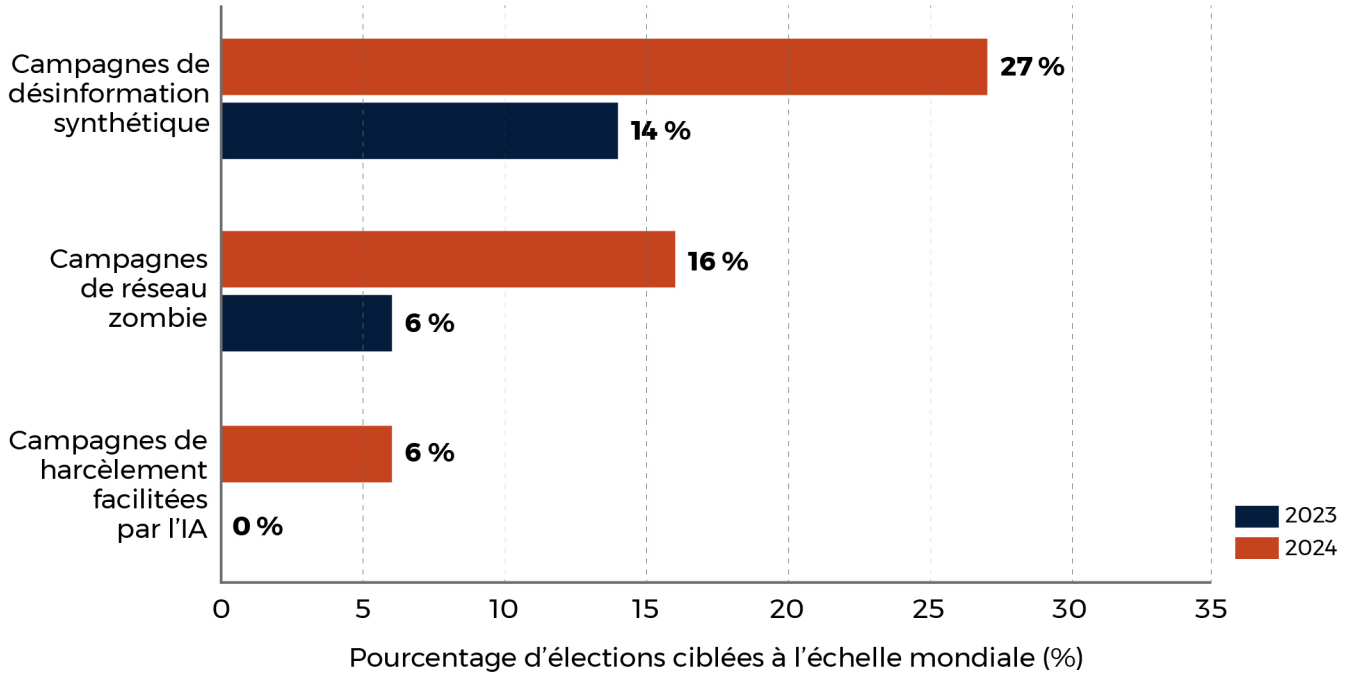
* Un pétaoctet correspond à 1 000 téraoctets, ou l'équivalent de 11 000 films HD. L'unité correspondant à 1 000 pétaoctets se nomme un exaoctet.

TENDANCES MONDIALES

Le Centre pour la cybersécurité analyse les activités de cybermenace ciblant les élections nationales depuis 2015. La présente mise à jour porte principalement sur les menaces facilitées par l'IA et se fonde sur des données qui remontent jusqu'à 2023, année à laquelle nos recherches ont commencé à indiquer que les auteurs de menace faisaient appel à l'IA générative pour cibler un processus démocratique.

Depuis 2023, nous avons constaté une augmentation du nombre d'activités de cybermenace facilitées par l'IA ciblant des élections dans le monde. Cependant, nous estimons que les données représentent presque certainement une sous-évaluation du nombre total d'événements menés contre des processus démocratiques dans le monde, car les cyberactivités ne sont pas toutes signalées ou détectées. De même, il peut être difficile de repérer les hypertrucages et les textes générés par LLM ou de les différencier du contenu créé par des humains. Nos observations réalisées entre 2023 et 2024 nous ont permis de dégager quatre grandes tendances.

Figure 1 : Augmentation des menaces facilitées par l'IA pour les processus démocratiques de 2023 à 2024



Types de menaces facilitées par l'IA

Campagne de désinformation synthétique : Utilisation de l'IA pour créer de la désinformation qui soit sera répandue en ligne en insistant sur un message ou un thème constant, soit servira de façon sporadique et désorganisée contre une candidate ou un candidat.

Campagne de réseau zombie : Réseau de zombies automatisés qui se caractérise par l'utilisation de LLM pour générer du contenu ou des profils créés par l'IA.

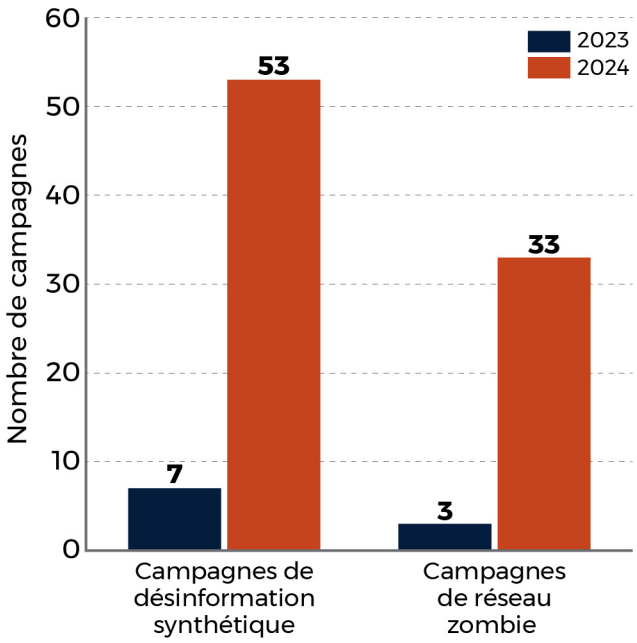
Campagne de harcèlement facilitée par l'IA : Utilisation de l'IA pour exercer de la pression sur une politicienne ou un politicien participant à un processus démocratique ou pour l'intimider.

Tendance 1 : L'IA générative est utilisée pour polluer l'écosystème d'information

En 2023 et 2024, il y a eu 124 élections nationales dans le monde, en plus des élections législatives de l'Union européenne de 2024 qui se sont déroulées dans les 27 États membres. Selon les recherches du Centre pour la cybersécurité, 40 de ces 151 élections avaient été ciblées par des auteurs qui ont utilisé l'IA générative pour **créer** ou **diffuser** de la désinformation au moins une fois au cours des 12 mois précédant l'élection. Comme certains pays ont été ciblés plus d'une fois, nous avons repéré 60 campagnes de désinformation synthétique, ce qui veut dire que des auteurs hostiles se sont servis de l'IA générative pour créer de la désinformation et la répandre en ligne. Soit ces campagnes réitéraient un message ou un thème constant, soit elles s'inscrivaient dans un effort sporadique et désorganisé visant à créer de la désinformation contre une candidate ou un candidat. Dans certains cas, des images, du contenu audio ou des textes générés par l'IA ont servi à semer la confusion et à transmettre la désinformation au sein de l'électorat.

Nous avons également décelé 36 cas confirmés ou soupçonnés d'utilisation de réseaux de zombies automatisés pour propager de la désinformation. Ces réseaux se caractérisaient souvent par leur utilisation de photos de profil générées par l'IA. Pour leur part, les ordinateurs zombies en tant que tels étaient en mesure de publier des liens, d'amplifier du contenu et d'interagir avec de véritables utilisatrices et utilisateurs. À plusieurs occasions, des équipes de recherche et des comités de surveillance indépendants ont observé des réseaux de zombies qui tentaient de manipuler les algorithmes de recommandation dans les médias sociaux. Parmi les plateformes touchées, citons X, Facebook, TikTok, WeChat, Telegram ainsi que des plateformes propres à un pays, comme PTT de Taïwan[37].

Figure 2 : Campagnes de désinformation facilitées par l'IA ciblant les processus démocratiques



Tendance 2 : Le doute plane quant à l'utilisation de l'IA dans des tentatives d'hameçonnage contre des institutions électorales

De 2023 à 2024, nous avons observé trois cas signalés de campagnes d'hameçonnage lancées par des auteurs de menace qui voulaient mettre la main sur des justificatifs d'identité ou se livrer à des opérations de piratage et de divulgation afin de nuire à des organisations politiques et gouvernementales[38]. Bien qu'il nous soit impossible de confirmer si l'IA générative a été utilisée dans les cas susmentionnés, nous avons constaté que la fréquence à laquelle les auteurs de menace ont eu recours à des LLM pour bonifier leurs attaques par hameçonnage dans d'autres contextes a connu une augmentation rapide ces deux dernières années[39].

De plus, au cours de la même période, la technologie de l'IA servant à améliorer et à accélérer les campagnes d'hameçonnage s'est répandue sur le Web clandestin parallèlement à la découverte de nouvelles techniques permettant de contourner les contrôles antihameçonnages intégrés à la technologie légitime[40].

Les LLM permettent également aux auteurs de menace de créer rapidement du contenu qui est non seulement dans la langue de la cible, mais qui reflète la « voix » et les particularités du groupe ou de la plateforme. Nous considérons que les attaques par hameçonnage facilitées par l'IA menées contre des cibles démocratiques augmenteront presque certainement au cours des deux prochaines années.

Tendance 3 : Le ciblage avancé qui repose sur une analyse basée sur l'apprentissage automatique

Il est difficile d'observer, dans chaque cas, la façon dont les États-nations utilisent l'apprentissage automatique pour analyser des mégadonnées. Toutefois, nous avons constaté que la RPC et, dans une moindre mesure, la Russie mènent d'énormes campagnes de collecte de données; elles se procurent habituellement les données dans les sources ouvertes, les achètent en secret ou les volent[41]. Les ensembles de données qui suscitent leur intérêt comprennent l'information de nature politique, comme les registres électoraux ou les données sur les campagnes, ainsi que l'information précise sur une personne qui comprend, par exemple, ses habitudes d'achat, son dossier médical et son historique de navigation ou de médias sociaux[42].

Comme l'indique l'ECMN de 2025-2026, les États-nations dotés de ressources importantes comptent fort probablement sur l'IA pour traiter et analyser ces ensembles de données, ce qui leur donne de l'information pour mener des opérations de renseignement subséquentes, entre autres contre les élections[43]. Les auteurs hostiles exploitent aussi ces données pour accroître la surveillance qu'ils exercent sur les groupes de diaspora et leurs représentantes ou représentants politiques ou encore pour mener des opérations en ligne contre eux[44]. Dans un autre ordre d'idées, selon un affidavit du FBI, la Russie a secrètement utilisé des produits de publicité ciblée vendus par les médias sociaux et les moteurs de recherche pour mener ses efforts de propagande[45].

Tendance 4 : Les auteurs de menace ont recours à l'IA générative pour harceler des personnalités publiques

Des 151 élections étudiées en 2023 et 2024, au moins 6 ont été marquées par l'utilisation d'hypertrucages pour harceler ou intimider des personnalités politiques. Les hypertrucages ainsi utilisés sont exclusivement de nature sexuelle et ciblent principalement les politiciennes ou les personnes de la communauté 2SLGBTQI+ qui œuvrent en politique. Cette observation cadre avec une tendance qui se dessine en lien avec l'IA : de toutes les vidéos hypertruquées qui se trouvent en ligne, 98 % sont de nature pornographique et de ce nombre, 99 % ciblent des femmes[49].

Dans ces cas, l'IA sert à humilier et à intimider les personnes ciblées et à les exclure d'une participation politique. Même si la plupart des cas ne semblent pas faire partie de campagnes d'influence délibérées, nous estimons que dans au moins un cas, le contenu a probablement été publié pour saboter intentionnellement la campagne d'une personne qui avait posé sa candidature dans une élection[50].

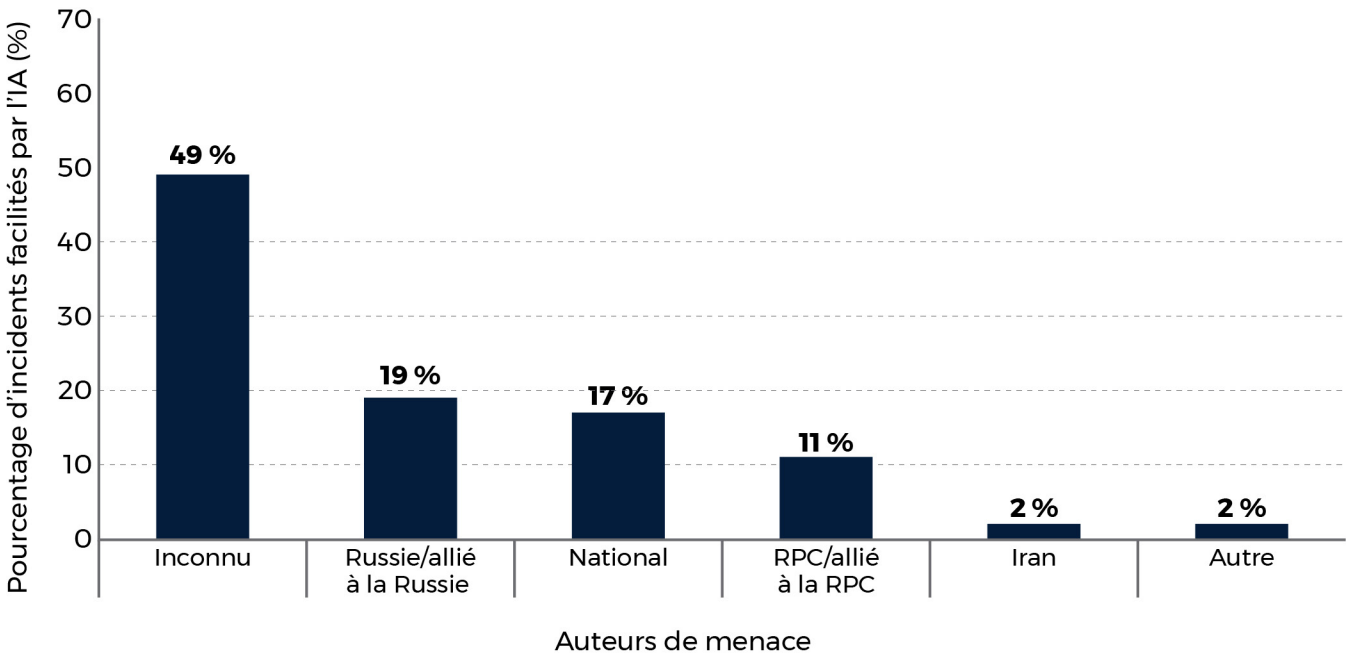
Les femmes sont ciblées de façon disproportionnelle

En juin 2024, un média britannique a fait savoir qu'on avait trouvé en ligne 400 photos pornographiques modifiées par des moyens numériques dans lesquelles on voyait plus de 30 politiciennes connues[46]. En Grèce, l'IA avait été utilisée pour créer une photo d'un chef de parti nu, ce qui a engendré des commentaires homophobes dénigrants[47]. À la veille des élections de 2024 au Bangladesh, des photos montrant faussement une politicienne en bikini ont circulé en ligne[48].

LES PRINCIPAUX AUTEURS DE MENACE QUI SE SERVENT DE L'IA POUR CIBLER LES PROCESSUS DÉMOCRATIQUES

De toutes les activités facilitées par l'IA que nous avons observées — qui avaient toutes pour objectif de propager de la désinformation ou de harceler des politiciennes ou politiciens — environ 49 % ne pouvaient pas être attribuées de façon crédible à un auteur en particulier. Nos recherches indiquent que la majorité des activités de cybermenace facilitées par l'IA qui ont été **attribuées** avaient été perpétrées par des auteurs parrainés par des États ayant un lien avec la Russie, la RPC et l'Iran. Nous considérons que leur objectif est presque certainement de briser des alliances démocratiques et de semer la division au sein d'États démocratiques et entre ceux-ci en plus de servir leurs objectifs géopolitiques[51]. Nous avons aussi constaté que des partis politiques ont eu recours à l'IA à mauvais escient dans leurs propres pays, généralement pour propager de la désinformation.

Figure 3 : Attribution des menaces pour les processus démocratiques



Russie

Comme l'indiquaient les statistiques présentées dans le rapport CPD de 2023, parmi les auteurs à qui on a attribué des activités ciblant des élections dans le monde, les plus agressifs sont ceux de la Russie et ceux qui agissent en sa faveur, mais qui ne relèvent pas d'elle. Nous considérons que la Russie mène presque certainement ses activités de cybermenace dans le but de nuire aux visées électorales des partis ou des candidates ou candidats qui ont, selon elle, une idéologie et une orientation en matière de politique étrangère favorables à l'Occident. Ces deux dernières années, au moins quatre réseaux russes importants ont employé l'IA pour propager de la désinformation de façon distincte.

Même si nous n'avons pas observé de façon définitive des auteurs russes se servir de l'IA pour améliorer leurs efforts d'hameçonnage ou de piratage et de divulgation contre des élections, nous sommes d'avis qu'ils possèdent presque certainement les moyens de le faire. Cette évaluation est fondée sur des activités similaires entreprises par des groupes criminels et d'autres États-nations[52]. Ainsi, nous croyons que la Russie a fort probablement la capacité de se servir de l'IA pour améliorer l'efficacité et la furtivité des maliciels déployés contre ses cibles[53].

En ce qui concerne la désinformation facilitée par l'IA, un réseau connu sous le nom de Doppelganger, créé en avril 2022, est exploité par deux entreprises établies en Russie qui ont des liens connus avec le Kremlin[54]. Doppelganger recourt à l'IA pour mystifier des sites Web de nouvelles légitimes, comme *Der Spiegel* ou *The Guardian*, et utilise les LLM pour générer des articles qui contiennent de la désinformation[55]. Un réseau similaire, CopyCop, se sert de LLM pour créer des articles de désinformation et les publier sur des sites Web qui ont l'air d'appartenir à des organes d'information occidentaux[56].

Pour sa part, Storm-1679, un troisième réseau qui est en activité depuis 2023, tire parti de l'IA générative pour surcharger des organisations médiatiques ainsi que des communautés de recherche et de vérification de faits, c'est-à-dire qu'il les bombarde de demandes de vérification dans le but de saturer leurs ressources de lutte contre la désinformation[57]. Chacun de ces réseaux a eu recours à l'IA générative pour produire du contenu et à des réseaux de zombies pour amplifier la désinformation dans divers médias en ligne.

Hypertrucage pour nuire à la candidature de Tim Walz au poste de vice-président des États-Unis

Dans cette vidéo d'hypertrucage, M. Walz était accusé d'avoir commis des abus sexuels dans le cadre de son ancien poste d'enseignant au secondaire. Même si la vidéo était fausse, la personne qui y figurait semblait avoir véritablement étudié à l'école à laquelle M. Walz enseignait. Pour créer cet hypertrucage, Storm-1516 a probablement fait des recherches sur la population étudiante de l'école en question, utilisé l'IA pour créer une fausse vidéo qui intègre les particularités de cette population, puis déployé la vidéo pour qu'elle nuise à M. Walz[58].

Bien que la qualité de la désinformation russe ait été en dents de scie, la Russie et les auteurs non étatiques favorables à ce pays ont démontré qu'ils peuvent créer du contenu de propagande sur mesure qui est conçu pour augmenter sa viralité et son impact politique dans l'État visé. En octobre 2024, Storm-1516 a publié une vidéo d'hypertrucage personnalisée dans laquelle une personne prétend avoir subi des abus sexuels de la part du candidat au poste de vice-président des États-Unis, Tim Walz[59]. Cette attaque alliait la désinformation à la dégradation sexuelle et n'avait aucune considération pour la victime intermédiaire.

Nous estimons qu'en dépit de ces efforts, il est probable que les campagnes de la Russie n'obtiennent généralement pas une grande visibilité sans que des intervenants du pays cible ne les amplifient sciemment ou inconsciemment[60]. En effet, selon le renseignement allemand, les 700 sites Web frauduleux créés dans le cadre des campagnes de Doppelganger n'ont été consultés que 800 000 fois* de novembre 2023 à août 2024[61]. Un autre chercheur a fait remarquer que la plupart des liens partagés par Doppelganger ont très peu été utilisés, sinon pas du tout[62]. Pour ce qui est des allégations d'abus visant Tim Walz, la population n'y a prêté attention qu'après que des commentateurs américains influents en ont parlé[63].

La contre-attaque des pays visés, qui ont riposté à la désinformation en supprimant l'infrastructure en ligne qui supporte les sites Web en question, ainsi que les opérations de déplateformisation menées par les entreprises de médias sociaux ont privé les campagnes de toute visibilité[64]. Malgré tout, nous sommes d'avis que la Russie a presque certainement encore l'intention et les moyens de continuer à exploiter l'IA générative pour polluer l'environnement informationnel des démocraties. De plus, la récente tendance des entreprises de médias sociaux à délaisser la vérification de faits professionnelle aura probablement pour effet d'exposer davantage le public à du contenu trompeur[65].

République populaire de Chine

La RPC représente une menace complexe et envahissante dans le cyberespace. Par des moyens numériques, entre autres, elle a mené une campagne hostile d'influence malveillante contre l'élection présidentielle de 2024 à Taïwan[66]. En ce qui a trait à l'IA, des équipes de recherche à Taïwan ont repéré un probable réseau de zombies composé de plus de 14 000 comptes Facebook, X, YouTube, TikTok et PTT, une plateforme de média social taïwanaise[67]. Certains avatars de profil des zombies étaient créés par l'IA générative alors que les zombies en tant que tels affichaient un comportement coordonné et des similarités dans leurs commentaires. Les comptes servaient à reprendre des messages diffusés par les médias d'État de la RPC et souvent à tenter de dénigrer la relation américano-taïwanaise et à nuire à la candidature de Lai Ching-Te, chef du Parti progressiste démocratique[68]. Le réseau de zombies a aussi partagé et amplifié du contenu qui dénigrait diverses personnalités politiques taïwanaises, faisant entre autres couler une vidéo à caractère sexuel soi-disant hypertruquée publiée sur un site Web pornographique[69].

De façon similaire, Spamouflauge Dragon, une campagne de propagande probablement menée par la Chine qui a déjà ciblé le Canada par le passé s'est servi de l'IA générative pour créer de la désinformation et exercer de l'influence sur l'électorat de divers pays dans le monde à la veille d'élections démocratiques dans ces pays[70]. Même si ces efforts n'ont pas suscité beaucoup d'attention, des organes de recherche indépendants ont signalé que la RPC peaufine ses tactiques de propagande qui commencent à mobiliser davantage les membres des électorats ciblés[71].

Spamouflage Dragon

En 2023, le réseau Spamouflauge a propagé de la désinformation sur des dizaines de députées et députés, dont le premier ministre, le chef de l'opposition et plusieurs membres du Cabinet. Il a aussi eu recours à l'IA générative pour cibler des personnalités mandarinophones au Canada[72].

* À titre de comparaison, le *Frankfurter Allgemeine Zeitung*, un journal allemand populaire, reçoit généralement plus de neuf millions de visionnements par mois.

Comme nous l'avons mentionné plus haut, la RPC mène des opérations de collecte de données massives contre les populations occidentales. Les données ainsi recueillies sont utilisées à différentes fins, mais nous croyons que la RPC a probablement la capacité et l'intention de recourir à l'apprentissage automatique pour les analyser et produire des profils de renseignement détaillés sur d'éventuelles cibles liées à des processus démocratiques[73]. Ces cibles peuvent être des membres du public votant et des médias, des personnalités politiques, des fonctionnaires et des activistes[74]. La RPC collabore avec des entreprises sur son territoire qui se spécialisent dans la technologie pour exploiter ces données à des fins de renseignement, entre autres :

- pour éclairer la prise de décisions;
- pour cerner des occasions de recrutement;
- pour améliorer ses opérations d'influence[75].

Selon nos observations, il est presque certain que la RPC continuera de récolter de l'information politique pertinente dans les sociétés occidentales.

Nous croyons que la RPC a probablement instrumentalisé TikTok, une plateforme de média social appartenant à la société chinoise ByteDance, pour contrôler les messages à son égard dans des États démocratiques, c'est-à-dire faire circuler les messages qui sont favorables à la RPC et censurer ceux qui ne le sont pas[76]. La Network Contagion Research Institute a d'ailleurs signalé que la RPC « a recours à la manipulation d'algorithmes et à des opérations d'information prolifiques pour influencer les croyances et les comportements des utilisatrices et utilisateurs à très grande échelle » [traduction][77]. Selon nous, il est probable que ces opérations aient, au moins une fois, ciblé des électrices et électeurs à la veille d'un scrutin[78].

Iran

D'après le FBI en 2024, le Corps des Gardiens de la révolution islamique (CGRI) a eu recours au harponnage pour s'introduire dans les systèmes liés à une campagne présidentielle américaine et pour tenter de s'introduire dans ceux liés à une autre campagne[79]. Nous ignorons encore si le CGRI a employé l'IA dans cette opération. Toutefois, nous savons qu'il a utilisé des LLM à d'autres occasions pour générer des courriels ciblés et convaincants qui incitaient une cible à cliquer sur un lien (ou à ouvrir une pièce jointe) pour l'amener à naviguer sur une page Web malveillante ou à télécharger un maliciel[80].

Selon nos observations, il est très probable qu'un auteur hostile comme le CGRI intègre l'IA à une cyberattaque similaire lancée contre une infrastructure électorale. Le CGRI a également trafiqué des pages de connexion pour récolter les justificatifs d'identité de ses victimes. Les technologies de l'IA peuvent être mises à profit pour faciliter cette tâche et les opérations de l'hameçonnage[81]. Il est aussi probable que le CGRI ait employé des LLM pour améliorer le code de maliciel, désactiver des antivirus et échapper à la détection[82].

Le CGRI se livre à du piratage contre une campagne présidentielle aux États-Unis

Lors d'une opération de piratage menée contre une campagne présidentielle aux États-Unis en 2024, le CGRI a mis la main sur de l'information sensible de sa cible et a transmis cette information à des médias et à des personnes qui étaient, à son avis, associés à des campagnes rivales. Ces derniers ont toutefois coupé court à cette opération et minimisé ses effets, car ils ont signalé la situation aux services d'application de la loi[83]. Nous ignorons encore si le CGRI a utilisé l'IA dans cette opération, mais nous savons qu'il a déjà eu recours à des LLM dans le cadre d'activités similaires.

Cybercriminelles et cybercriminels et auteurs de menace non étatiques

Il est presque certain que les cybercriminelles et cybercriminels et les auteurs de menace non étatiques sont responsables de la vaste majorité des hypertrucages pornographiques non consensuels qui ciblent les personnalités politiques, publiques et médiatiques. Les cybercriminelles et cybercriminels mènent des opérations de piratage et de divulgation en grand volume contre des bases de données commerciales et publiques, y compris celles d'États démocratiques[84]. Le Centre pour la cybersécurité définit la cybercriminalité comme étant une activité de cybermenace motivée par le gain financier, mais il ne faut pas oublier que les États-nations sont des acheteurs connus de données volées[85]. Les données volées peuvent servir à plusieurs fins, mais nous croyons que certaines d'entre elles sont probablement utilisées par des États-nations pour perfectionner leurs opérations facilitées par l'IA et l'apprentissage automatique et ciblant des processus démocratiques.

En outre, il est établi que les cybercriminelles et cybercriminels profitent des événements qui suscitent une importante couverture médiatique, comme des élections, pour commettre des escroqueries et de la fraude contre les électrices et électeurs[86]. Nous estimons donc qu'au cours des deux prochaines années, des cybercriminelles et cybercriminels utiliseront fort probablement l'hypertrucage et l'hameçonnage facilité par l'IA pour déployer une série de cyberattaques contre des processus démocratiques. Cela s'applique également aux méthodes plus destructrices employées dans la cybercriminalité, comme les rançongiciels[87].

Des auteurs non étatiques et des personnes influentes au pays peuvent, sciemment ou inconsciemment, amplifier la désinformation étrangère facilitée par l'IA. Étant donné qu'ils entretiennent habituellement des liens plus étroits et de confiance avec les réseaux sociaux nationaux, l'effet qu'ils ont sur l'amplification de la désinformation est plus grand que celui des usagers réguliers. En effet, comme nous l'avons dit précédemment, les tentatives d'auteurs liés à la Russie de véhiculer des histoires salaces sur Tim Walz sont restées vaines jusqu'à ce que des influenceurs américains s'emparent du contenu et l'amplifient sur leurs plateformes[88].

RÉPERCUSSIONS SUR LES ÉLECTIONS AU CANADA

Selon nos observations, il est très probable que la RPC, la Russie et l'Iran utilisent des outils facilités par l'IA pour tenter de s'ingérer dans le processus démocratique du Canada avant ou pendant la période électorale de 2025. De plus, nous estimons que les cybercriminelles et cybercriminels profiteront probablement des occasions que représentent des élections au Canada pour se livrer à des escroqueries et à de la fraude sans pour autant se concentrer sur les élections en tant que telles.

Il est fort probable que les auteurs de menace, lorsqu'ils ciblent des élections au Canada, se servent de l'IA générative pour créer et diffuser de la désinformation dans le but de diviser la population canadienne et de véhiculer une vision favorable aux intérêts d'États étrangers. Nous croyons qu'il est très probable que des auteurs affiliés à la RPC continueront de cibler précisément les communautés de la diaspora chinoise du Canada et de transmettre des messages à l'avantage des intérêts de la RPC sur les plateformes de médias sociaux[89]. Comme le Canada partage un écosystème informationnel avec les États-Unis, les Canadiennes et Canadiens ont déjà été exposés à de la désinformation facilitée par l'IA qui ciblait la population américaine[90]. Il est presque certain que cette tendance se poursuivra. Toutefois, il est impossible de prévoir la mesure dans laquelle un élément donné de désinformation gagnera de la visibilité ou trouvera un écho parmi la population canadienne.

Les personnalités et les partis politiques du Canada seront probablement la cible d'auteurs de menace qui cherchent à mener des opérations de piratage et de divulgation. Comme nous l'avons observé dans d'autres contextes, nous estimons que les auteurs de menace mettront probablement à profit des LLM pour s'en prendre à leurs cibles dans le cadre d'une opération d'hameçonnage de longue durée. Toutefois, selon nos constatations, il est très peu probable que des auteurs hostiles lancent une cyberattaque destructrice contre les infrastructures électorales, comme tenter de paralyser les systèmes de télécommunications le jour du scrutin, sauf en cas de conflit armé imminent ou direct.

Qui plus est, les personnalités publiques canadiennes, surtout les femmes et les membres de la communauté 2SLGBTQI+, sont plus susceptibles d'être la cible de vidéo pornographique hypertruquée. Malheureusement, nous estimons que sans mise à jour des lois et règlements, du contenu de ce genre continuera fort probablement de se répandre avec autant d'intensité.

À L'AVENIR

Des activités de cybermenace servent toujours à cibler des processus démocratiques à l'échelle planétaire. Le Centre pour la cybersécurité, qui fait partie du CST, fournit des avis et des conseils pour renseigner les Canadiennes et Canadiens sur les cybermenaces qui pèsent sur les élections au Canada[91].

Il 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[92] et les Conseils en matière de cybersécurité pour les intervenants politiques[93]. Des représentantes et représentants du CST font partie du Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections[94].

Le CST collabore étroitement avec Élections Canada pour protéger son infrastructure et défendre les processus électoraux du pays contre les cybermenaces. Il est d'ailleurs autorisé par le ministre de la Défense nationale à mener des cyberopérations défensives pour protéger le gouvernement du Canada, y compris Élections Canada. Cette autorisation donne au CST les moyens de perturber les cyberactivités malveillantes qui menacent les systèmes du pays. Le CST est également autorisé à protéger les systèmes d'importance pour le gouvernement, comme ceux qui sont liés à une élection générale.

De plus, le programme de capteurs du Centre pour la cybersécurité[95] contribue à défendre l'infrastructure d'Élections Canada en surveillant et en atténuant les éventuelles cybermenaces. Le Centre pour la cybersécurité aide aussi les organismes électoraux à renforcer leurs mesures de cybersécurité en leur transmettant des conseils d'expert par l'entremise de publications telles que Facteurs à considérer en matière de sécurité pour les systèmes de registre électronique du scrutin[96] et Conseils en matière de cybersécurité à l'intention des organismes électoraux[97].

Pour accroître davantage la protection des institutions démocratiques du Canada, le Bureau du Conseil privé a publié des ressources pour aider la population à lutter contre la désinformation et l'ingérence étrangère[98]. Ces ressources comprennent des trousses d'outils pour les dirigeantes et dirigeants communautaires, les titulaires d'une charge publique et les fonctionnaires.

Les Canadiennes et Canadiens sont invités à consulter les ressources suivantes qui portent sur des thèmes abordés dans la présente évaluation :

- Conseils en matière de cybersécurité sur l'intelligence artificielle générative[99]
- Guide sur les facteurs à considérer lors de l'utilisation des médias sociaux dans votre organisation[100]
- Conseils sur la cybersécurité pour reconnaître et contrer la désinformation en ligne[101]
- Conseils sur l'utilisation sécuritaire des médias sociaux[102]
- Évaluation des cybermenaces nationales 2025-2026[103]
- Repérer les cas de mésinformation, désinformation et malinformation[104]
- Fiche de renseignements à l'intention des électeurs canadiens[105]

Dans le cadre de sa campagne Pensez cybersécurité[106], le CST continuera de publier, tout au long de l'année, 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-processus-democratique-canada-mise-jour-2023

2 https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

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

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

5 https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

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

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

8 https://www.cyber.gc.ca/sites/default/files/cyber/publications/tdp-2019-report-f_0.pdf

9 Nicas, Jack et Lucía Cholakian Herrera. « Is Argentina the First A.I. Election? » (en anglais seulement), *The New York Times*, 15 novembre 2023. https://www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html.

10 « History of Generative AI » (en anglais seulement), Toloka, 22 août 2023. https://toloka.ai/blog/history-of-generative-ai/.

11 Scharre, Paul. *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W.W. Norton and Company, 2023); « Émirats : Edge Group et G42 accélèrent sur le développement du traitement automatique des langues – 22/03/2023 », Intelligence Online, 17 décembre 2024. https://www.intelligenceonline.fr/surveillance--interception/2023/03/22/edge-group-et-g42-accelerent-sur-le-developpement-du-traitement-automatique-des-langues,109925056-art?__cf_chl_tk=Bj.7oDYpCYGgyJlJLRVP7EnvU9eyYJGRP0xTHfmSQw-1739840261-1.0.1.1-OIy6_cWIAAsdV5S0KtXIasJBFjrhrrCWoMGvx_3mRiM.

12 « Digital 20 :4: Canada » (en anglais seulement), DataReportal – Global Digital Insights, 22 février 2024. https://datareportal.com/reports/digital-2024-canada.

13 Statistique Canada. « Enquête sociale canadienne – Qualité de vie, soins de santé virtuels et confiance, 2023 », 10 novembre 2023. https://www150.statcan.gc.ca/n1/daily-quotidien/231110/dq231110b-fra.htm.

14 Lin, Belle. « Welcome to the Era of BadGPTs » (en anglais seulement), *The Wall Street Journal*, 28 février 2024. https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8; National Cyber Security Centre. « The Near-Term Impact of AI on the Cyber Threat » (en anglais seulement), 24 janvier 2024. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

15 Judge, Elizabeth et Michael Pal. « Voter Privacy and Big-Data Elections », *Osgoode Hall Law Journal*, vol. 58, n 1 (9 mars 2021), p. 1-55.

16 National Cyber Security Centre. « UK Calls out China State-Affiliated Actors for Malicious Cyber Targeting of UK Democratic Institutions and Parliamentarians » (en anglais seulement), 25 mars 2024. https://www.ncsc.gov.uk/news/china-state-affiliated-actors-target-uk-democratic-institutions-parliamentarians.

17 Milmo, Dan. « Hacked UK Voter Data Could Be Used to Target Disinformation, Warn Experts » (en anglais seulement), *The Guardian*, 9 août 2023. https://www.theguardian.com/politics/2023/aug/09/hacked-uk-electoral-commission-data-target-voter-disinformation-warn-expert.

18 Linvill, Darren et Patrick Warren. « Digital Yard Signs: Analysis of an AI Bot Political Influence Campaign on X » (en anglais seulement), Clemson University Media Forensics Hub, 30 septembre 2024. https://open.clemson.edu/mfh_reports/7/; Yang, Kai-Cheng et Filippo Menczer. « Anatomy of an AI-Powered Malicious Social Botnet » (en anglais seulement), *Journal of Quantitative Description: Digital Media*, vol. 4 (29 mai 2024).

19 « Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux », Commission sur l'ingérence étrangère, 3 mai 2024, p. 150-157. https://commissioningerenceetrangere.ca/fileadmin/user_upload/Commission_sur_l_ingerence_etrangere_-_Rapport_initial__mai_2024__-_Digitale.pdf.

20 « Better Language Models and Their Implications » (en anglais seulement), Open AI, 14 février 2019. https://openai.com/index/better-language-models/.

21 Lin, Belle. « Welcome to the Era of BadGPTs » (en anglais seulement), *The Wall Street Journal*, 28 février 2024. https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8.

22 Hazell, Julian. « Spear Phishing with Large Language Models » (en anglais seulement), Oxford Internet Institute, 14 décembre 2023. https://cdn.governance.ai/Spear_Phishing_with_Large_Language_Models.pdf.

23 Heiding, Fredrik, Bruce Schneier et Arun Vishwanath. « AI Will Increase the Quantity — and Quality — of Phishing Scams » (en anglais seulement), *Harvard Business Review*, 30 mai 2024. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams.

24 Pour obtenir un sommaire de la technologie d'hypertrucage et de la menace qu'elle pourrait représenter pour le Canada, consulter le rapport intitulé Évolution de la désinformation : Un avenir « hypertruqué » du Service canadien du renseignement de sécurité, octobre 2023. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/evolution-de-la-desinformation-un-avenir-hypertruque.html.

25 Service canadien du renseignement de sécurité. Évolution de la désinformation : Un avenir « hypertruqué », octobre 2023. https://www.canada.ca/fr/service-renseignement-securite/organisation/publications/evolution-de-la-desinformation-un-avenir-hypertruque.html.

26 Nelson, Nate. « Deepfake-Generating Apps Explode, Allowing Multimillion-Dollar Corporate Heists » (en anglais seulement), 5 février 2024. https://www.darkreading.com/threat-intelligence/deepfake-apps-explode-multimillion-dollar-corporate-heists.

27 « AI Deepfakes Can Sway Voters and Disrupt Elections » (en anglais seulement), *Financial Times*, 7 juillet 2024. https://www.ft.com/video/4f473456-ca0e-4f0b-a9aa-9bac1e3220a6.

28 Lalchand, Satish et coll. « Generative AI Is Expected to Magnify the Risk of Deepfakes and Other Fraud in Banking » (en anglais seulement), Deloitte, 29 mai 2024. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html.

29 Mannie, Kathryn. « Company out $35M after Scammers Stage Video Call with Deepfake CFO, Coworkers » (en anglais seulement), 5 février 2024. https://globalnews.ca/news/10273167/deepfake-scam-cfo-coworkers-video-call-hong-kong-ai/.

30 « Top Trends in Big Data for 2024 and Beyond » (en anglais seulement), TechTarget, 12 janvier 2024. https://www.techtarget.com/searchdatamanagement/feature/Top-trends-in-big-data-for-2021-and-beyond; Our World in Data. « Computation Used to Train Notable Artificial Intelligence Systems, by Domain » (en anglais seulement), 2023. https://ourworldindata.org/grapher/artificial-intelligence-training-computation.

31 Brady, William J. et coll. « Algorithm-Mediated Social Learning in Online Social Networks » (en anglais seulement), *Trends in Cognitive Sciences*, vol. 27, n 10 (1 octobre 2023), p. 947-60.

32 Milli, Smitha et coll. « Engagement, User Satisfaction, and the Amplification of Divisive Content on Social Media » (en anglais seulement), Columbia University, 3 janvier 2024. https://knightcolumbia.org/content/engagement-user-satisfaction-and-the-amplification-of-divisive-content-on-social-media; BÄR, Dominik, et coll. « Systematic Discrepancies in the Delivery of Political Ads on Facebook and Instagram » (en anglais seulement), *PNAS Nexus*, vol. 3, n 7 (1juillet 2024). https://academic.oup.com/pnasnexus/article/3/7/pgae247/7695718; Finkelstein, Joel, et coll. « The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States » (en anglais seulement), Network Contagion Research Institute, août 2024. https://networkcontagion.us/reports/the-ccps-digital-charm-offensive/; Hao, Karen. « Troll Farms Reached 140 Million Americans a Month on Facebook before 2020 Election, Internal Report Shows » (en anglais seulement), *MIT Technology Review*, 16 septembre 2021. https://www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election/.

33 Mcmillan, Robert, Dustin VOLZ, et Aruna Viswanatha. « China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says » (en anglais seulement), *The Wall Street Journal*, 25 décembre 2023. https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594.

34 Chatterjee, Mohar. « What AI Is Doing to Campaigns » (en anglais seulement), Politico, 15 août 2024. https://www.politico.com/news/2024/08/15/what-ai-is-doing-to-campaigns-00174285.

35 Shubladze, Sandro. « Empowering Decision-Making With Real-Time Data Analytics » (en anglais seulement), *Forbes*, 30 avril 2024. https://www.forbes.com/councils/forbestechcouncil/2024/04/30/empowering-decision-making-with-real-time-data-analytics/.

36 « US FBI Affidavit in Support of Seizure Warrant » (en anglais seulement), United States District Court for the Eastern District of Pennsylvania, 9 septembre 2024, 30-31, 219. https://www.justice.gov/archives/opa/media/1366261/dl.

37 Voir par exemple : « Disrupting deceptive uses of AI by covert influence operations » (en anglais seulement), Open AI, 30 mai 2024. https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/; « 2024 Taiwan Presidential Election Information Manipulation AI Observation Report » (en anglais seulement), AI Labs, 2024. https://ailabs.tw/wp-content/uploads/2024/01/2024-Taiwan-Presidential-Election-Information-Manipulation-AI-Observation-Report-2.pdf; Wack, Morgan, Darren Linvill et Patrick Warren. « Old Despots, New Tricks - An AI-Empowered Pro-Kagame/RPF Coordinated Influence Network on X » (en anglais seulement), Media Forensics Hub Reports, juin 2024. https://open.clemson.edu/mfh_reports/5/.

38 Les trois cas observés étaient des campagnes d'hameçonnage menées contre les campagnes présidentielles de Trump et de Harris aux États-Unis ainsi que contre des représentantes ou représentants lors d'une élection en Moldavie à l'automne de 2024. Antoniuk, Daryna. « Google: Iranian Hackers Targeting Affiliates of Both US Presidential Campaigns » (en anglais seulement), 15 août 2024. https://therecord.media/iran-targets-us-election; « Operation MiddleFloor: Disinformation Campaign Targets Moldova Ahead of Presidential Elections and EU Membership Referendum » (en anglais seulement), Check Point Research, 9 octobre 2024. https://research.checkpoint.com/2024/disinformation-campaign-moldova/.

39 Desai, Deepen et Rohit Hedge. « Phishing Attacks Rise: ThreatLabz 2024 Phishing Report » (en anglais seulement), ZScaler, avril 2024. https://www.zscaler.com/blogs/security-research/phishing-attacks-rise-58-year-ai-threatlabz-2024-phishing-report.

40 Lin, Belle. « Welcome to the Era of BadGPTs » (en anglais seulement), *The Wall Street Journal*, 28 février 2024. https://www.wsj.com/articles/welcome-to-the-era-of-badgpts-a104afa8; POIREAULT, Kevin. « The Dark Side of Generative AI: Five Malicious LLMs Found on the Dark Web » (en anglais seulement), *Infosecurity Europe*, 10 août 2023. https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/generative-ai-dark-web-bots.html.

41 Cadell, Cate. « China Harvests Masses of Data on Western Targets, Documents Show » (en anglais seulement), Washington Post, 31 décembre 2021. https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html; Silverman, Craig. « Google Allowed a Sanctioned Russian Ad Company to Harvest User Data for Months » (en anglais seulement), ProPublica, 1 juillet 2022. https://www.propublica.org/article/google-russia-rutarget-sberbank-sanctions-ukraine.

42 Landler, Mark et Stephen Castle. « U.K. Accuses China of Cyberattacks Targeting Voter Data and Lawmakers » (en anglais seulement), *The New York Times*, 25 mars 2024. https://www.nytimes.com/2024/03/25/world/europe/uk-china-cyberattack-hacking.html; Balding, Christopher. « Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua » (en anglais seulement), SSRN Scholarly Paper (Rochester, NY : Social Science Research Network, 13 septembre 2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999.

43 Tucker, Patrick. « How China Used TikTok, AI, and Big Data to Target Taiwan's Elections » (en anglais seulement), 8 avril 2024. https://www.defenseone.com/technology/2024/04/how-china-used-tiktok-ai-and-big-data-target-taiwans-elections/395569/.

44 Voir, par exemple : « Press Release: Eastern District of New York | 34 Officers of People's Republic of China National Police Charged with Perpetrating Transnational Repression Scheme Targeting U.S. Residents » (en anglais seulement), United States Attorney's Office, 17 avril 2023. https://www.justice.gov/usao-edny/pr/34-officers-peoples-republic-china-national-police-charged-perpetrating-transnational. Voir l'acte d'accusation au complet « Complaint and Affidavit in Support of Application for Arrest Warrant » (en anglais seulement), mais surtout les pages 8 et 9. https://web.archive.org/web/20250204065726/https:/www.justice.gov/d9/2023-04/squad_912_-_23-mj-0334_redacted_complaint_signed.pdf.

45 « US FBI Affidavit in Support of Seizure Warrant » (en anglais seulement), United States District Court for the Eastern District of Pennsylvania, 9 septembre 2024, 30, 216–20. https://www.justice.gov/archives/opa/media/1366261/dl.

46 Newman, Kathy. « Exclusive: Top UK Politicians Victims of Deepfake Pornography » (en anglais seulement), Channel 4, 1 juillet 2024. https://www.channel4.com/news/exclusive-top-uk-politicians-victims-of-deepfake-pornography.

47 Epachtitis, Thanos Sitistas. « Κατασκευασμένη με λογισμικό AI η φωτογραφία που "δείχνει" τον Σ. Κασσελάκη και τον Τ. Μακμπέθ γυμνούς σε παραλία » (en grec seulement), Security Hero, 3 avril 2024. https://www.factchecker.gr/2024/04/03/ai-generated-image-of-kasselakis-and-tyler-naked-on-a-beach/.

48 The Tribune. « Pakistanis, Bangladeshi Politicians Are New Targets of Deepfake, 90 per Cent of Videos Online Are Pornographic » (en anglais seulement), 14 décembre 2023. https://www.tribuneindia.com/news/science-technology/from-rashmika-mandanna-to-bangladeshi-politician-filmed-in-a-bikini-90-per-cent-of-deepfake-videos-online-are-pornographic-571782/.

49 « 2023 State Of Deepfakes: Realities, Threats, And Impact » (en anglais seulement), décembre 2023. https://www.securityhero.io/state-of-deepfakes/.

50 Hung, Chen-Ling, et coll. « AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election » (en anglais seulement), Thomson Foundation, avril 2024, 5. https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf.

51 Seddon, Max, Demetri Sevastopulo et Joe Leahy. « Vladimir Putin and Xi Jinping Vow to Co-Operate against 'Destructive and Hostile' US » (en anglais seulement), *Financial Times*, 16 mai 2024. https://www.ft.com/content/f77028c8-c960-4d10-b0eb-4c511924a4d5; RAUCH, Jonathan. « Confronting the Axis of Resistance » (en anglais seulement), *The Atlantic*, 1 juillet 2024. https://www.theatlantic.com/ideas/archive/2024/07/russia-china-nato-axis-resistance/678831/.

52 Rundle, James. « Generative AI Could Revolutionize Email—for Hackers » (en anglais seulement), *The Wall Street Journal*, 6 septembre 2023. https://www.wsj.com/articles/generative-ai-could-revolutionize-emailfor-hackers-5a8c725c.

53 Les observations ont permis de constater que d'autres auteurs étatiques comptent sur les LLM pour développer du code pour échapper aux antivirus. Voir Sécurité Microsoft, « Staying Ahead of Threat Actors in the Age of AI » (en anglais seulement), 14 février 2024. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.

54 « Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts » (en anglais seulement), U.S. Department of the Treasury, 20 mars 2024. https://home.treasury.gov/news/press-releases/jy2195; THUST, Sarah. « Doppelganger: CORRECTIV Investigations Bring Russian Propaganda Campaign to a Halt » (en anglais seulement), Correctiv, 15 novembre 2024. https://correctiv.org/en/fact-checking-en/2024/11/15/doppelganger-correctiv-investigations-bring-russian-propaganda-campaign-to-a-halt/.

55 Consulter le document suivant pour obtenir de l'information sur Doppelganger, y compris son utilisation de l'IA : « What Is the Doppelganger Operation? List of Resources » (en anglais seulement), EU DisinfoLab, 30 octobre 2024. https://www.disinfo.eu/doppelganger-operation/.

56 « Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale » (en anglais seulement), Insikt Group, 9 mai 2024. https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf.

57 « Operation Overload Impersonates Media to Influence 2024 US Election » (en anglais seulement), Insikt Group, 23 octobre 2024. https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf.

58 Gilbert, David. « Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims » (en anglais seulement), *Wired*, 21 octobre 2024. https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

59 Gilbert, David. « Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims » (en anglais seulement), *Wired,* 21 octobre 2024. https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

60 Leake, Matthew. « Are Fears about Online Misinformation in the US Election Overblown? The Evidence Suggests They Might Be » (en anglais seulement), Reuters Institute for the Study of Journalism, 24 octobre 2024. https://reutersinstitute.politics.ox.ac.uk/news/are-fears-about-online-misinformation-us-election-overblown-evidence-suggests-they-might-be. Pour consulter une étude sur la visibilité de contenu pro-russe (non lié à l'IA), voir : Allen, Jennifer. « Worried about the Russians Dividing America? The Call Is Coming from inside the House » (en anglais seulement), Media Bias Detector, 28 septembre 2024. https://mediabiasdetector.seas.upenn.edu/blog/worried-about-the-russians-dividing-america-the-call-is-coming/.

61 « „Doppelgänger" Interne Details Zu Russicher Desinformationaskampagne » (en allemand seulement), Bayerisches Landesamt für Verfassungsschutz, août 2024. https://www.verfassungsschutz.bayern.de/mam/anlagen/baylfv_vollanalyse_doppelgaenger.pdf.

62 Rid, Thomas. « The Lies Russia Tells Itself » (en anglais seulement), Foreign Affairs, 30 septembre 2024. https://www.foreignaffairs.com/united-states/lies-russia-tells-itself.

63 Gilbert, David. « Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims » (en anglais seulement), *Wired*, 21 octobre 2024. https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

64 Voir par exemple : « TAG Bulletin : Q3 2024, Google Threat Analysis Group, September 12, 2024 » (en anglais seulement). https://blog.google/threat-analysis-group/tag-bulletin-q3-2024/; Franklin, Margarita et coll. « Adversarial Threat Report » (en anglais seulement), Meta, mai 2024. https://md.teyit.org/file/meta-threat-report.pdf.

65 Chuai, Yuwei, et coll. « Did the Roll-Out of Community Notes Reduce Engagement With Misinformation on X/Twitter? » (en anglais seulement), *Proceedings of the ACM on Human-Computer Interaction 8*, no. CSCW2 (novembre 2024). https://dl.acm.org/doi/10.1145/3686967.

66 Lau, Stuart Lau. « China Bombards Taiwan with Fake News Ahead of Election » (en anglais seulement), Politico, 10 janvier 2024. https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/; Miller, Maggie, et Joseph Gedeon. « Taiwan Bombarded with Cyberattacks Ahead of Election » (en anglais seulement), Politico, 11 janvier 2024. https://www.politico.com/news/2024/01/11/taiwan-cyberattacks-election-china-00134841; Yu, Alan, Michael Clark, et Megan Shahi. « Taiwan's Election: PRC Interference and Its Implications for the 2024 Election Landscape » (en anglais seulement), Center for American Progress, 1 février 2024. https://www.americanprogress.org/article/taiwans-election-prc-interference-and-its-implications-for-the-2024-election-landscape/.

67 « 2024 Taiwan Presidential Election Information Manipulation AI Observation Report » (en anglais seulement), AI Labs, 2024. https://ailabs.tw/wp-content/uploads/2024/01/2024-Taiwan-Presidential-Election-Information-Manipulation-AI-Observation-Report-2.pdf.

68 « 2024 Taiwan Presidential Election Information Manipulation AI Observation Report » (en anglais seulement), AI Labs, 2024. https://ailabs.tw/wp-content/uploads/2024/01/2024-Taiwan-Presidential-Election-Information-Manipulation-AI-Observation-Report-2.pdf.

69 Cheng-Yu, Chen, et Liu Hsin-Han. « 2024 Elections : Cabinet Supports Probe of Deepfake Video of Legislator » (en anglais seulement), *Taipei Times*, 10 janvier 2024. https://www.taipeitimes.com/News/taiwan/archives/2024/01/10/2003811892; Hung, Chen-Ling, et coll. « AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election » (en anglais seulement), Thomson Foundation, avril 2024, 5. https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf

70 « The #Americans : Chinese State-Linked Influence Operation Spamoflage Masquerades as U.S. Voters to Divisive Narratives Ahead of 2024 Election » (en anglais seulement), Graphika, septembre 2024. https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf; « Une probable campagne par Spamouflage, de la RPC, vise des dizaines de députés canadiens dans le cadre d'une opération de désinformation », Affaires mondiales Canada, 23 octobre 2023. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=fra.

71 Gilbert, David. « Why China Is So Bad at Disinformation » (en anglais seulement), *Wired*, 29 avril 2024. https://www.wired.com/story/china-bad-at-disinformation/.

72 « Une probable campagne par Spamouflage, de la RPC, vise des dizaines de députés canadiens dans le cadre d'une opération de désinformation », Affaires mondiales Canada 23 octobre 2023. https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/2023-spamouflage.aspx?lang=fra.

73 « Évaluation des cybermenaces nationales 2025-2026 », Centre canadien pour la cybersécurité, novembre 2024. https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026; McMillan, Robert, Dustin Volz, et Aruna Viswanatha. « China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says » (en anglais seulement), *The Wall Street Journal*, 25 décembre 2023. https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594.

74 BALDING, Christopher. « Chinese Open Source Data Collection, Big Data, And Private Enterprise Work For State Intelligence and Security: The Case of Shenzhen Zhenhua » (en anglais seulement), SSRN Scholarly Paper (Rochester, NY : Social Science Research Network, 2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3691999.

75 McMillan, Robert, Dustin Volz, et Aruna Viswanatha. « China Is Stealing AI Secrets to Turbocharge Spying, U.S. Says » (en anglais seulement), *The Wall Street Journal*, 25 décembre 2023. https://www.wsj.com/tech/ai/china-is-stealing-ai-secrets-to-turbocharge-spying-u-s-says-00413594; Dorfman, Zach. « How China's Tech Giants Like Alibaba, Tencent, and Baidu Aid Spy Agencies » (en anglais seulement), *Foreign Policy*, 23 décembre 2020. https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/.

76 « TikTok Inc. and Bytedance Ltd. v. Merrick B. Garland, Amended Public Redacted Brief for the Respondent » (en anglais seulement), 16 septembre 2024, 35–44. https://storage.courtlistener.com/recap/gov.uscourts.cadc.40861/gov.uscourts.cadc.40861.1208648321.0.pdf.

77 Finkelstein, Joel, et coll. « The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States » (en anglais seulement), Network Contagion Research Institute, août 2024. https://networkcontagion.us/reports/the-ccps-digital-charm-offensive/; voir également « A Tik-Tok-Ing Timebomb : How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives » (en anglais seulement), Network Contagion Research Institute, décembre 2023. https://networkcontagion.us/reports/12-21-23-a-tik-tok-in-timebomb-how-tiktoks-global-platform-anomalies-align-with-the-chinese-communist-partys-geostrategic-objectives/.

78 Lau, Stuart. « China Bombards Taiwan with Fake News Ahead of Election » (en anglais seulement), Politico, 10 janvier 2024. https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/.

79 « Press Release: Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election » (en anglais seulement), Office of Public Affairs, U.S. Department of Justice, 27 septembre 2024. https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us.

80 Les tactiques, techniques et procédures du CGRI et d'autres auteurs liés à l'Iran recourant à l'IA sont décrites dans les documents suivants : « Staying Ahead of Threat Actors in the Age of AI » (en anglais seulement), Sécurité Microsoft, 14 février 2024. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/; « Influence and Cyber Operations: An Update » (en anglais seulement), Open AI, octobre 2024, 14–19. https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf.

81 « How to Protect against Iranian Targeting of Accounts Associated with National Political Organizations » (en anglais seulement), Cybersecurity and Infrastructure Security Agency, 8 octobre 2024. https://www.cisa.gov/news-events/alerts/2024/10/08/cisa-and-fbi-release-fact-sheet-protecting-against-iranian-targeting-accounts-associated-national.

82 « Staying Ahead of Threat Actors in the Age of AI » (en anglais seulement), Sécurité Microsoft, 14 février 2024. https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.

83 « Press Release: Three IRGC Cyber Actors Indicted for 'Hack-and-Leak' Operation Designed to Influence the 2024 U.S. Presidential Election » (en anglais seulement), Office of Public Affairs, U.S. Department of Justice, 27 septembre 2024. https://www.justice.gov/archives/opa/pr/three-irgc-cyber-actors-indicted-hack-and-leak-operation-designed-influence-2024-us. Pour consulter la mise en accusation complète : « United States of America vs Masoud Jalili, Seyyed Ali Aghamiri and Yasar Balagui » (en anglais seulement). https://www.justice.gov/archives/opa/media/1371191/dl.

84 « Global Malicious Activity Targeting Elections Is Skyrocketing » (en anglais seulement), Resecurity, 12 février 2024. https://www.resecurity.com/blog/article/global-malicious-activity-targeting-elections-is-skyrocketing; Leyden, John. « Hacked Iraqi Voter Information Found for Sale Online » (en anglais seulement), 20 février 2024. https://www.darkreading.com/endpoint-security/hacked-iraqi-voter-information-found-for-sale-online.

85 Hawkins, Amy. « Huge Cybersecurity Leak Lifts Lid on World of China's Hackers for Hire » (en anglais seulement), *The Guardian*, 23 février 2024. https://www.theguardian.com/technology/2024/feb/23/huge-cybersecurity-leak-lifts-lid-on-world-of-chinas-hackers-for-hire.

86 « Cyber Threats to Democracy: A Special Report on Phishing and Online Scams Targeting the 2024 Election » (en anglais seulement), Bolster AI, octobre 2024. https://bolster.ai/blog/phishing-online-scams-targeting-the-2024-election.

87 Lin, Belle, et Catherine Stupp. « Cyber Threats and the Election: What You Need to Know » (en anglais seulement), *The Wall Street Journal*, 1 novembre 2024. https://www.wsj.com/articles/cyber-threats-and-the-election-what-you-need-to-know-c9dcaa7d; Akartuna, Arda. « As the US Election Nears, AI Political Deepfake Scams Are Targeting Crypto Users » (en anglais seulement), 15 août 2024. https://www.elliptic.co/blog/as-the-us-election-nears-ai-political-deepfake-scams-are-targeting-crypto-users.

88 Gilbert, David. « Russian Propaganda Unit Appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims » (en anglais seulement), *Wired*, 21 octobre 2024. https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/.

89 « Sommaire du pays : République populaire de Chine », Commission sur l'ingérence étrangère, 2024. https://commissioningerenceetrangere.ca/fileadmin/commission_ingerence_etrangere/Documents/Preuves_et_Presentations/Preuves/CAN.SUM.000005.FR.pdf; Bridgman, Aengus, et coll. « Mis- and Disinformation during the 2021 Canadian Federal Election » (en anglais seulement), Media Ecosystem Observatory, 8 juin 2022, 60–64. https://osf.io/preprints/osf/ubfmx_v1.

90 À la veille de l'élection fédérale de 2021, de la désinformation non facilitée par l'IA émanant des États-Unis a été observée dans l'écosystème médiatique canadien. Voir : Bridgman, Aengus, et coll. « Mis- and Disinformation during the 2021 Canadian Federal Election » (en anglais seulement), Media Ecosystem Observatory, 8 juin 2022, 60–64. https://osf.io/preprints/osf/ubfmx_v1.

91 https://www.cyber.gc.ca/fr/orientation/cybermenaces-elections

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

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

94 https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/groupe-travail-securite.html

95 https://www.cse-cst.gc.ca/fr/reddition-de-comptes/transparence/rapports/rapport-annuel-centre-securite-telecommunications-2023-2024#9-1-1

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

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

98 https://www.canada.ca/fr/institutions-democratiques/services/proteger-institutions-democratiques.html

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

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

101 https://www.canada.ca/fr/campagne/desinformation-enligne.html

102 https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/reseaux-sociaux

103 https://www.cyber.gc.ca/fr/orientation/evaluation-cybermenaces-nationales-2025-2026

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

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

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