Renforcement de la résilience démocratique face à la désinformation étrangère au Canada

Rapport final | Juin 2024

Toronto Metropolitan University

the dais

DEMOCRACY XCHANGE

Remerciements

The Dais est une plateforme canadienne vouée à l'élaboration de politiques audacieuses et au développement de meilleures et meilleurs leaders. Nous sommes un laboratoire d'idées sur les politiques publiques et de leadership à l'Université Toronto Metropolitan qui fait des liens entre les personnes, les idées et les pouvoirs dont nous avons besoin pour édifier un Canada plus inclusif, plus novateur et plus prospère.

Pour obtenir de plus amples renseignements, consultez dais.ca. Notre adresse est la suivante : 20, rue Dundas O., bureau 921, Toronto (Ontario) M5G 2C2

@daisTMU
/daisTMU
The Dais at Toronto Metropolitan University

The Dais est fier d'engager un groupe diversifié de bailleurs de fonds pour appuyer et catalyser son travail, conformément à ses valeurs (en anglais) et sous réserve d'un examen interne approfondi. Comme groupe de réflexion non partisan et d'intérêt public, nous n'acceptons de fonds que d'organismes qui appuient notre mission et nous permettent d'entreprendre des travaux de manière indépendante, avec un contrôle rédactionnel total. Le nom de tous nos bailleurs de fonds est affiché publiquement et de manière transparente sur tous les documents en ligne et imprimés relatifs à chaque projet ou initiative.

Conception et illustration: Zaynab Choudhry

Travail éditorial: Suzanne Bowness

Collaboratrices et collaborateurs:
Tiffany Kwok, analyste politique, the Dais
André Côté, directeur de la politique et de la recherche, the Dais
Sam Andrey, directeur général, the Dais
Nina Rafeek Dow, responsable des communications et du marketing, the Dais
Marium Hamid, responsable des partenariats
Angus Lockhart, analyste politique principal
Jake Hirsch-Allen, conseiller principal

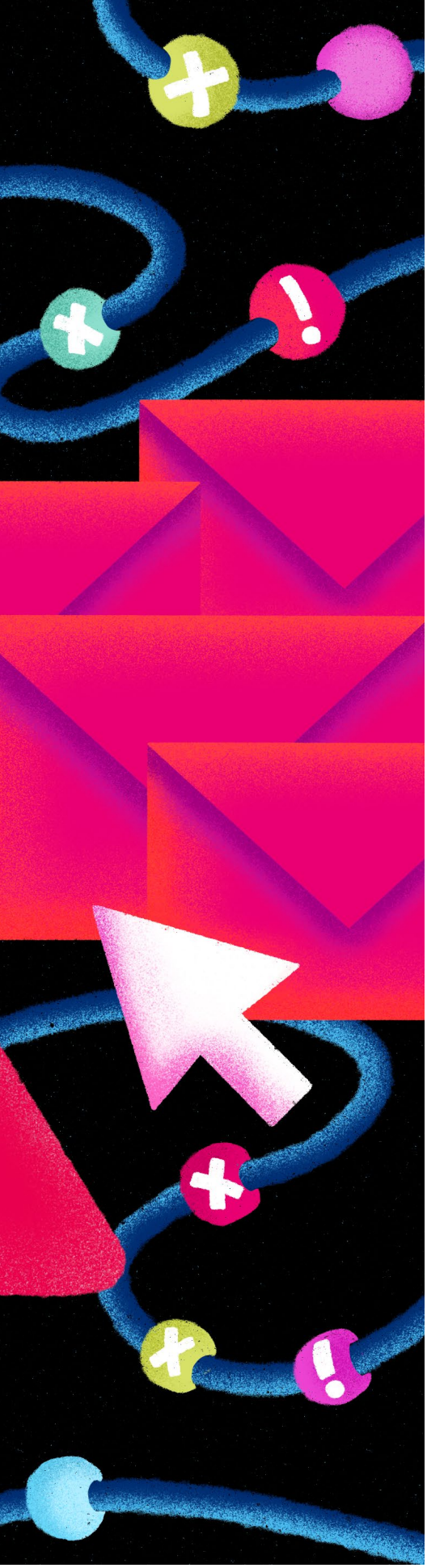
DemocracyXChange (en anglais), qui en est cette année à sa cinquième édition, est un sommet annuel qui vise à connecter, célébrer et équiper les personnes qui agissent pour renforcer la démocratie. Organisé conjointement par Dais de TMU, l'Université OCAD (en anglais) et l'Open Democracy Project (en anglais), DemocracyXChange vise à renforcer la communauté de pratique qui existe déjà au Canada et à fournir de nouvelles occasions pour renforcer la résilience démocratique au cours de trois jours de conférences, d'ateliers pratiques et d'occasions de réseautage sur place.

Funded by the Government of Canada | Canada

Cet ouvrage est appuyé en partie par le : gouvernement du Canada par l'intermédiaire du Secrétariat des institutions démocratiques du Bureau du Conseil privé

Les opinions et interprétations contenues dans ce rapport sont celles des auteurs et ne reflètent pas nécessairement celles du gouvernement du Canada.

Pour citer le présent rapport :
The Dais. Renforcement de la résilience démocratique face à la désinformation étrangère au Canada : Rapport final. Université Toronto Metropolitan, 2024.
https://dais.ca



Participantes et participants à l'atelier qui ont accepté que leur nom soit mentionné :

Le présent rapport a été largement inspiré par les différents points de vue des personnes participantes à l'atelier. Cela dit, les déclarations et les recommandations contenues dans le présent rapport n'engagent que la responsabilité de ses autrices et auteurs.

Aaron Shull, Centre for International Governance Innovation
Akaash Maharaj, Global Organization of Parliamentarians Against Corruption
Andrea Cecchetto, Bibliothèque publique de Markham
Anthony Seaboyer, Collège militaire royal du Canada
Bessma Momani, Université de Waterloo
Chris Russill, Université Carleton
Chris Tenove, Université de la Colombie-Britannique
Christina de Castell, Bibliothèque publique de Vancouver
Colette Brin, Université Laval
David Morin, Université de Sherbrooke
Diana Fu, Université de Toronto
Dianna English, Centre for International Governance Innovation
Elizabeth Dubois, University d'Ottawa
Emile Dirks, Citizen Lab
Emily Laidlaw, Université de Calgary
Erin Taylor, Meta
Ghayda Hassan, UQÀM
Helen A. Hayes, Université McGill
Isabelle Corriveau, Université McGill
Jean-Christophe Boucher, Université de Calgary
Jennie Phillips, Université McGill
Kathryn Ann Hill, HabiloMédias
Laurie Mulvey, Université Penn State, World in Conversation Center for Public Diplomacy
Lee Slinger, Munk School of Global Affairs & Public Policy
Marla Boltman, Les amis des médias canadiens
Mohammed Hashim, Fondation canadienne des relations raciales
Nicole Jackson, Université Simon Fraser
Renee Black, GoodBot
Sabiha Tursun, Université McGill, Projet de défense des droits des Ouïghours
Samantha Reusch, Apathy is Boring
Sam Richards, Université Penn State
Samantha Meyer, Université de Waterloo
Seher Shafiq, Mozilla
Shelly Ghai Bajaj, Université de Waterloo
Shlomit Broder, Digital Public Square
Steven Hassan, Freedom of Mind Resource Center
Viola Tian, Fondation canadienne des relations raciales
Wendy Chun, Université Simon Fraser
Wesley Wark, Centre for International Governance Innovation

Résumé

En mars et avril 2024, the Dais a organisé un atelier en deux parties avec plus de 40 personnes participants issues du monde universitaire, de la société civile, du gouvernement et de l'industrie. Cet atelier visait à réunir des spécialistes pour discuter de la menace que représente aujourd'hui la désinformation étrangère. Il a également examiné les possibilités d'avancer des solutions fondées sur des données probantes pour renforcer la résilience démocratique au Canada.

Dès le début de l'atelier, les personnes participantes ont débattu de la capacité à définir et à identifier la « désinformation étrangère », en soulignant la nécessité de faire la distinction entre un éventail d'activités, de tactiques et d'acteurs de la menace. Elles ont également reconnu la complexité du réseau d'interactions en ligne, qui brouille souvent l'origine du faux contenu. Ces défis ont préparé le terrain pour le reste des discussions, au cours desquelles les personnes participantes ont débattu des questions et des occasions associées à chaque niveau.

Les discussions de l'atelier ont été organisées en trois sections : la première pour traiter de l'expérience des Canadiennes et des Canadiens en matière de désinformation étrangère au niveau citoyen; la deuxième examine la manière dont la société civile et les entreprises sont impliquées dans la lutte contre la désinformation étrangère; et la troisième aborde les décisions que les gouvernements et les institutions doivent prendre lorsqu'ils luttent contre l'ingérence étrangère ainsi que les possibilités qu'ils peuvent avoir d'améliorer l'échange d'informations et de renforcer la confiance de la population.

Les personnes participants ont collectivement exprimé le besoin d'approches coordonnées et multi-niveaux au niveau citoyen, au niveau société civile et entreprises ainsi qu'au niveau gouvernements et institutions.

Parmi les occasions identifiées au niveau **citoyen**, on trouve les suivantes :

- Recueillir davantage de données au niveau individuel et communautaire, afin de mieux comprendre les expériences de désinformation étrangère par le biais des médias en ligne et hors ligne, y compris les nuances dans la sensibilité à la désinformation, et d'examiner de plus près tous les groupes vulnérables ciblés, en plus des seules communautés de la diaspora.
- Renforcer la résilience préventive, cultiver de l'information « bonne et exacte » et élargir les initiatives d'éducation civique fondées sur des données probantes sont autant de moyens d'autonomiser et de renforcer les capacités des communautés en matière de littératie numérique.
- Collaborer avec des acteurs de confiance comme des médecins, des scientifiques et des influenceurs en ligne, et concevoir les programmes d'éducation à la littératie numérique comme des occasions de renforcer d'autres compétences afin de rendre les initiatives citoyennes plus accessibles et mieux accueillies.

Parmi les occasions identifiées au niveau **société civile et entreprises**, on trouve les suivantes :

- Renforcer la protection des universitaires, des journalistes et de la société civile sous la forme d'un soutien juridique et des coûts connexes, d'une fonction de soutien ou de médiateur pour aider les victimes de harcèlement, et d'une approche renouvelée pour l'application de la loi afin de prendre plus au sérieux les menaces en ligne.
- Tirer les leçons des efforts de la société civile dans des pays plus avancés que le Canada dans le développement de leur résistance à l'ingérence étrangère. Il s'agit notamment des efforts déployés dans des pays comme l'Estonie, la Finlande et Taïwan.
- Exiger une plus grande transparence de la part des plateformes en ligne afin d'évaluer l'efficacité des mesures de gouvernance des plateformes visant à lutter contre la désinformation, comme les initiatives de vérification des faits et d'étiquetage, ou les restrictions sur le contenu automatisé et la publicité payante.

Parmi les occasions identifiées au niveau **gouvernements et institutions**, on trouve les suivantes :

- Revoir le seuil à partir duquel les gouvernements sont tenus de communiquer de l'information au public ou aux communautés touchées en cas d'attaque informatique, afin d'encourager un échange plus ouvert dans la mesure du possible
- Introduire une évaluation annuelle de la menace que représente la désinformation étrangère, afin de prévenir les problèmes émergents et de tenir les gouvernements et les institutions informés des menaces qui pèsent sur le pays.
- Examiner les vulnérabilités qui ont été exploitées par les campagnes de désinformation étrangères afin d'en tirer des enseignements pour le Canada.

Introduction

Aperçu du projet

Dans le contexte de l'enquête publique en cours sur l'ingérence étrangère qui a ciblé les élections fédérales de 2019 et de 2021 et de la désinformation continue dans l'écosystème d'information du Canada, nous avons vu une occasion de mobiliser les spécialistes et les intervenantes et intervenants dans le cadre d'une discussion vaste sur la nature de la menace de la désinformation étrangère aujourd'hui et sur les occasions de promouvoir des solutions fondées sur des données probantes dans le but de renforcer la résilience démocratique au Canada.

En mars et avril 2024, on a convié un échantillon représentatif d'expertes, d'experts, de praticiennes et de praticiens du gouvernement, de l'industrie, du milieu universitaire et de la société civile qui travaillent à l'intersection de la désinformation et de la démocratie à participer à un atelier en deux parties :

- Un pré-atelier virtuel de 90 minutes, le 26 mars 2024 afin d'offrir des présentations et des discussions initiales sur les enjeux et de présenter les thèmes clés ainsi que l'approche de l'atelier en personne qui suivrait.
- Un atelier en personne d'une journée, le 12 avril 2024, au sommet de DemocracyXChange, qui a mobilisé les personnes participantes dans le cadre d'une séance intensive animée visant à recueillir des commentaires et des suggestions sur les approches à privilégier dans la lutte contre la désinformation étrangère au Canada au niveau de la population, de la société civile et des gouvernements/institutions.

À la fin des ateliers, un sommaire des thèmes clés, des conclusions et des propositions découlant des discussions ont été intégrés dans le présent rapport final. Le rapport explore les possibilités de combattre et de traiter la désinformation étrangère au niveau citoyen, au niveau société civile et entreprises ainsi qu'au niveau gouvernements et institutions.

Contexte: Désinformation étrangère au Canada

La désinformation gangrène depuis longtemps l'écosystème d'information. Dans un écosystème d'information numérique qui évolue rapidement, les formes changeantes et ses méthodes de diffusion de désinformation de plus en plus insaisissables ont amplifié les difficultés relatives au traitement et à l'atténuation de cette désinformation.[1] Ce défi est devenu encore plus difficile étant donné les complexités géopolitiques des campagnes de désinformation étrangères, qui visent à miner la confiance du public et à menacer l'intégrité des institutions démocratiques.

La désinformation étrangère a récemment émergé en tant qu'enjeu important dans le débat public sur la sécurité nationale et l'intégrité démocratique, stimulée par son rôle prépondérant dans des événements mondiaux d'envergure, comme l'invasion de la Crimée par la Russie en 2014. Au Canada, les élections fédérales de 2019 ont vu plus de tentatives d'intervention, par les instances publiques, en vue d'essayer de lutter contre l'ingérence étrangère, y compris la désinformation. Des outils et des équipes, comme le Groupe de travail sur les menaces en matière de sécurité et de renseignements fédéral visant les élections et le mécanisme de réponse rapide du G7 (MRR), ont été mis sur pied, et la Loi sur la modernisation des élections de 2018 comprenait des mesures de protection contre la

désinformation, notamment par la transparence de la publicité numérique, ainsi que de l'influence étrangère par le biais de dons en période électorale.[2] Les efforts en matière d'éducation civique et d'éducation aux médias ont également été renforcés par des programmes comme l'Initiative de citoyenneté numérique et différents programmes d'organismes communautaires.[3] Plus récemment, les modifications proposées à la Loi électorale du Canada comprennent l'élargissement de l'interdiction empêchant une personne ou une entité étrangère d'influencer des électrices et des électeurs pendant la période électorale pour qu'ils votent ou s'abstiennent de voter pour une candidate, un candidat ou un parti en particulier pour aussi inclure les candidates et candidats potentiels et les partis et pour s'appliquer à tout moment pendant la période électorale. Les interdictions relatives à l'usurpation d'identité et aux fausses déclarations dans le but d'influer sur le processus électoral ou les résultats des élections ont également été clarifiées pour comprendre le contenu créé par intelligence artificielle (IA).[4]

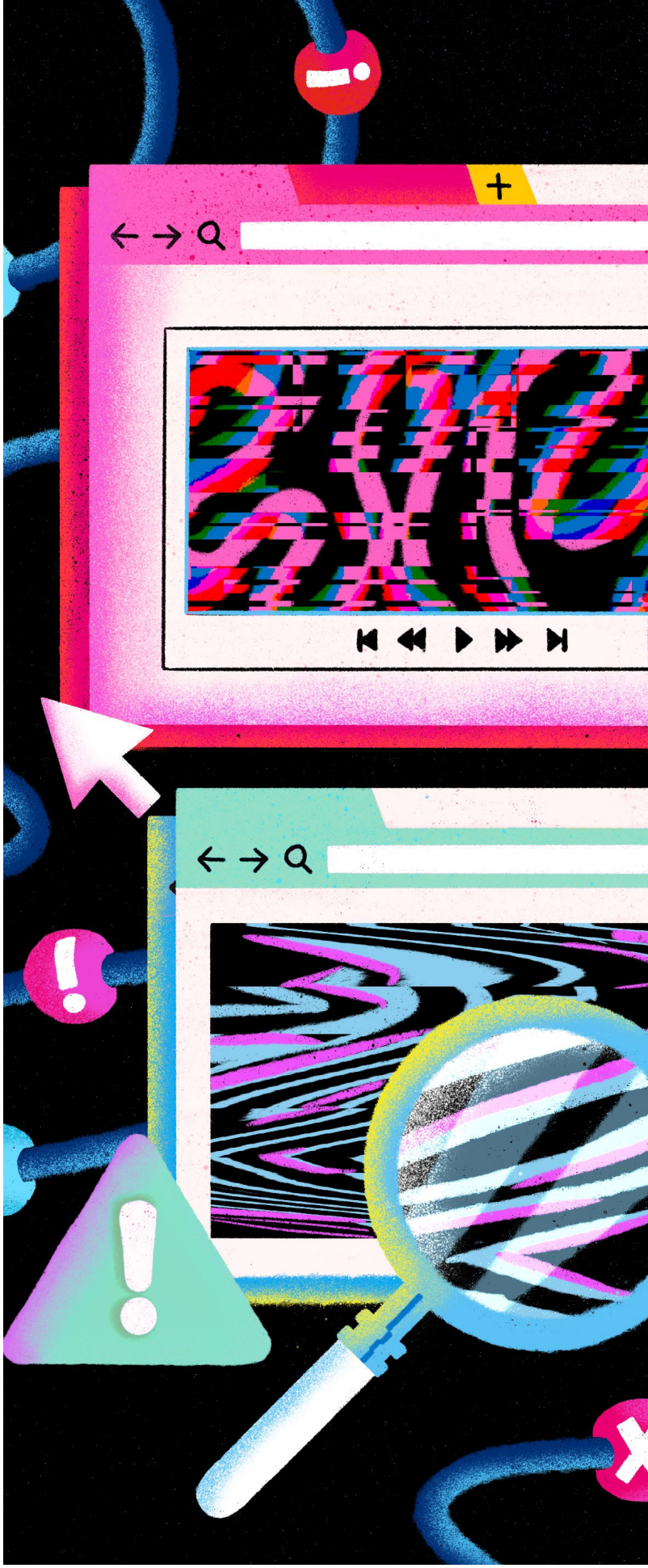
D'après l'Évaluation des cybermenaces nationales au Canada, les activités d'influence étrangère en ligne sont devenues la « nouvelle normalité », avec le déploiement de la désinformation comme une menace grandissante et complexe au Canada.[5] Dans certains cas, des acteurs étrangers malveillants cherchent à modifier les discours ou à accentuer les clivages à propos d'enjeux mondiaux au sein de nations démocratiques, comme ce fut récemment le cas avec des campagnes de désinformation sur la pandémie de COVID-19 et l'invasion de l'Ukraine par la Russie en 2022.[6] D'autres efforts ont été faits pour influencer directement les élections et les processus démocratiques, comme en témoignent les révélations récentes sur le ciblage de députées et députés canadiens et de candidates et candidats potentiels à une investiture politique. Des préoccupations ont également été suscitées par le ciblage des communautés de la diaspora, particulièrement par des avenues médiatiques avec des émissions dans leurs langues maternelles et les plateformes comme VKontakte (VK), Telegram et WeChat.[7]

Compte tenu du cadre et de la portée du présent rapport sur la désinformation étrangère, les personnes participantes à l'atelier ont souligné la difficulté de définir ce que l'on entend par « étrangère », en particulier dans le contexte des récits de désinformation qui circulent des États-Unis vers le Canada. Elles ont également discuté de la manière de différencier l'engagement diplomatique de l'ingérence étrangère, afin de comprendre et de définir correctement l'« ingérence étrangère ». La nature de la « désinformation étrangère » a également été contestée, compte tenu de la nature interconnectée de l'écosystème de l'information en ligne, qui brouille les frontières entre l'information étrangère et l'information nationale. Les discussions ont également porté sur les différences entre les campagnes d'influence menées par les différents acteurs étatiques étrangers, certains diffusant une désinformation spécifique à la fois à grande échelle et en ciblant les communautés de la diaspora, tandis que d'autres opèrent en cherchant à répandre le chaos par le biais de vastes opérations de dispersion ou en amplifiant la polarisation existante.

Le paysage international

Qu'il s'agisse de mobiliser la population ou de mener des actions coordonnées au niveau de l'état, d'autres pays ont adopté des approches variées à la lutte contre la désinformation étrangère. Jusqu'à récemment, les États-Unis ont privilégié une approche globale en communiquant directement avec les plateformes de médias sociaux et en les informant, en plus de lutter contre la désinformation à l'aide de plusieurs organismes, dont le Global Engagement Center, le Federal Bureau of Investigation et la Cybersecurity and Infrastructure Security Agency.[8] En raison des difficultés présentées par cette approche sur le plan juridique, les réunions d'information sur les plateformes de médias sociaux sont actuellement en veilleuse.[9] Un nouveau Cadre de lutte contre la manipulation de l'information par un État étranger dirigé par les États-Unis a été conjointement approuvé par le Royaume-Uni et le Canada en février 2024. Ce cadre vise en partie à aller au-delà des approches de type « surveillance et signalement » pour l'adoption d'autres approches qui intègrent des stratégies visant à contrer les menaces.[10]

L'Union européenne (UE) a également adopté une approche mixte en créant un cadre visant à contrer la manipulation de l'information par des acteurs étrangers et l'ingérence étrangère (FIMI), pour établir un code de bonnes pratiques contre la désinformation et déployer un système d'alerte rapide (RAS) afin de faire part des analyses, des pratiques exemplaires et des communications aux institutions, États membres et partenaires internationaux de l'UE.[11] Le site Web EUvsDisinfo mobilise les visiteuses et les visiteurs au niveau des citoyennes et citoyens en démystifiant les cas de désinformation, tandis que les États membres de l'UE ont également adopté leurs propres approches de lutte contre la désinformation.[12] La France, par exemple, a adopté en 2018 une loi visant à habiliter les juges à supprimer les « fausses nouvelles » pendant les campagnes électorales.[13] L'approche du Royaume-Uni comprend sa stratégie pour la littératie médiatique en ligne qui vise à augmenter le taux de littératie médiatique parmi le personnel enseignant, les personnes aidantes, les bibliothécaires et les personnes qui travaillent auprès des jeunes,[14] et son équipe d'information sur la sécurité nationale en ligne (NSOIT), qui cible la désinformation étrangère.



THÈME CLÉ 1

Niveau citoyen

Cette section se penche sur les expériences des Canadiennes et des Canadiens avec la désinformation étrangère et présente des moyens de lutter contre la désinformation et de développer de la résilience face à elle au niveau citoyen.

L'ENJEU :

La population canadienne est la cible de campagnes de désinformation étrangères.

RÉSUMÉ DES OCCASIONS POTENTIELLES :

- **Recueillir davantage de données pour mieux comprendre les expériences d'interférence étrangère au sein des communautés vulnérables comme les communautés de la diaspora.**
- **Mieux comprendre les résultats des organismes communautaires qui luttent contre la désinformation avec comme but d'améliorer les itérations futures du programme, y compris la traduction dans des langues autres que l'anglais et le français.**
- **Éduquer les membres de la population canadienne de tous les âges sur la désinformation étrangère afin de doter les personnes des outils et des capacités nécessaires pour faire preuve d'esprit critique et identifier la désinformation, notamment par le biais de programmes et d'initiatives d'éducation du public et de littératie numérique adaptés à la culture.**

Les diasporas au Canada sont depuis longtemps les cibles de campagnes d'ingérence étrangère par les acteurs étatiques. La désinformation, la popularisation des plateformes en ligne, et la méfiance historique à l'égard des autorités sont devenues des avenues pour l'ingérence d'acteurs étrangers pour créer des campagnes qui ciblent les communautés vulnérables. La forte dépendance de certaines communautés de la diaspora au contenu qui circule sur des chaînes de communication privées, comme WeChat et WhatsApp et leur degré de confiance élevé à leur égard, pose des défis particuliers en ce qui concerne l'identification de la désinformation et la lutte contre elle.[15]

Le développement de mesures pertinentes sur le plan culturel et visant à atteindre les communautés ciblées requiert une compréhension plus profonde de l'expérience des différentes communautés en matière d'ingérence étrangère. Des efforts pour aborder la désinformation doivent tenir compte des besoins et des expériences de ces communautés ou elles pourraient faire face à des conséquences négatives.

Comme dans le cas des campagnes de désinformation et de manipulation de l'information ciblant le député Michael Chong et l'ancien député Kenny Chiu, des acteurs étrangers malveillants cherchent à décourager les députés ciblés de la participation politique, à polluer le discours public et ultimement, à miner la participation démocratique.[16] En l'absence de sources d'information culturellement et linguistiquement pertinentes, les membres des communautés de la diaspora risquent d'avoir des difficultés à se forger une opinion politique juste et authentique et d'accepter les informations fausses comme étant la vérité, ce qui dissuade les citoyennes et les citoyens de participer aux élections et à d'autres processus démocratiques.

Les efforts de désinformation étrangère ont également cherché à influencer le discours politique et l'opinion publique au Canada dans la population générale. Un exemple de ces efforts est la longue campagne de désinformation entreprise par la Russie, qu'il s'agisse d'influencer le discours autour des réticences à l'égard de la vaccination et des messages anticonfinement durant la pandémie de

COVID-19 ou de la désinformation autour de l'invasion de l'Ukraine par la Russie.[17]

Nous avons déterminé trois occasions potentielles d'aborder la menace de désinformation étrangère au niveau citoyen.

Recueillir davantage de données pour comprendre les expériences d'interférence étrangère au sein des communautés.

Premièrement, mener des recherches et favoriser la mobilisation au niveau local afin d'avoir une meilleure compréhension des communautés confrontées à l'ingérence étrangère en plus d'explorer les facteurs sous-jacents qui contribuent à la propagation d'informations fausses et mensongères. Si la recherche existante fait ressortir une plus grande vulnérabilité potentielle en raison de facteurs comme les traumatismes historiques et contemporains et les appels basés sur l'identité, il faudra recueillir beaucoup plus de données pour comprendre les nuances de cette susceptibilité afin d'éclairer les approches futures à la lutte contre la désinformation.
Les personnes les participantes à l'atelier ont évoqué la nécessité d'explorer d'autres groupes vulnérables ciblés, en plus des communautés de la diaspora, à savoir ceux qui ont traditionnellement moins confiance dans les institutions. Les personnes participantes ont cité en exemple le Convoi de la liberté et les communautés de conspiration de la COVID-19 au Canada. Les personnes participantes ont aussi souligné l'importance de mieux comprendre le rôle des créateurs de contenu et des influenceuses et influenceurs sur les médias sociaux dans la diffusion de fausse information et de désinformation. Les études montrent que l'influence et l'engagement sont inégaux : les 10 % de comptes de médias sociaux les plus importants génèrent environ 93 % de l'engagement sur les principales plateformes.[18] Les résultats révèlent également que les médecins et les scientifiques sont les fournisseurs d'information les plus fiables, ce qui justifie une étude plus approfondie sur la manière de tirer parti de ces personnalités dignes de confiance.

Les personnes participantes ont également discuté de la disponibilité relative des données agrégées, par opposition aux données individuelles, pour souligner la nécessité de mieux comprendre les interactions des gens avec les médias sociaux et la désinformation. Tandis que les données agrégées peuvent fournir des renseignements généraux et de haut niveau sur les expériences des différents groupes communautaires sur les médias sociaux, les données individuelles peuvent mettre en évidence des nuances linguistiques, culturelles et habituelles au sein des communautés qui ne sont pas nécessairement prises en compte dans les données au niveau du groupe. La collecte et l'utilisation de données individuelles et agrégées permettraient de créer des solutions à plusieurs niveaux pour lutter contre la désinformation. Les personnes participante ont également discuté de comment le Projet de loi sur les préjudices en ligne crée de nouvelles obligations réglementaires pour les plateformes en ligne afin de fournir de l'information transparente et un accès aux données pour la recherche, mais dont le champ d'application est limité aux catégories étroites de contenu illégal, plutôt qu'à la désinformation.

Les personnes participantes ont aussi suggéré de consulter les sources d'information locales qui relient les communautés de la diaspora à leur pays d'origine afin de mieux comprendre le discours international sur les questions, bien que certaines aient souligné la nécessité de faire la distinction entre les interférences malveillantes et le simple engagement social entre les personnes. Les personnes participantes ont de plus recommandé d'aller plus loin que les plateformes de médias sociaux traditionnellement étudiées et de s'intéresser à des outils en ligne comme les plateformes de messagerie privée, les plateformes de jeux et les balados.

Suivre et analyser les résultats du travail des organismes communautaires en vue de lutter contre la désinformation.

Deuxièmement, chercher à mieux comprendre les résultats du travail des organismes communautaires en vue de lutter contre la désinformation. Cela peut être fait au moyen de programmes ou d'évaluations communautaires de ceux qui reçoivent du financement par l'entremise du Programme de contributions en matière de citoyenneté numérique

ou du Programme d'échange en matière de littératie numérique. Dans le cadre de ces occasions de financement, les organismes ont conçu une variété de matériel d'apprentissage, de programmes et d'outils de sensibilisation du public et de campagnes d'alphabétisation civique. L'évaluation des utilisatrices et utilisateurs de ces produits en vue d'améliorer leur compréhension et leur savoir-faire numérique peut être un moyen de déterminer si ces programmes et outils ont été efficaces et d'identifier les lacunes qui subsistent.

Une personne participante à l'atelier a fait part de la nécessité de recueillir les expériences réussies des programmes existants pour comprendre pourquoi ils ont fonctionné, afin de mettre en œuvre ces éléments dans les initiatives futures. D'autres ont souligné la difficulté de mettre en place un suivi de l'impact à long terme dans le cadre de subventions qui sont souvent d'une durée d'un an. D'autres ont exprimé la nécessité de protéger la vie privée des membres de la communauté comme une priorité absolue lors de l'analyse de tous les suivis et résultats. Cela a été mentionné spécifiquement en ce qui concerne les organismes qui travaillent dans des communautés qui ont moins confiance dans les gouvernements, car elles peuvent se sentir mal à l'aise à l'idée de faire part de leurs idées et de leurs données, même si les résultats permettent d'améliorer la programmation.

Des efforts peuvent aussi être faits pour identifier les organismes communautaires culturels qui n'ont peut-être pas reçu de financement, mais qui travaillent en vue de combattre la désinformation dans leurs communautés. La collecte de données fondées sur les résultats peut également contribuer à améliorer les itérations futures des interventions en vue de la désinformation et des programmes de littératie numérique pour les populations ciblées. Si la recherche a montré que l'amélioration de la culture numérique peut aider les utilisatrices et les utilisateurs à distinguer l'information exacte de la fausse, on ne sait toujours pas combien de temps dure cet effet, ni s'il empêche les utilisatrices et les utilisateurs de répandre de la fausse information en ligne.[19] Par conséquent, il convient également d'accorder une plus grande attention aux capacités des utilisatrices et utilisateurs et à leurs interactions en ligne au fil du temps.

Éduquer la population canadienne et lui donner les outils et les capacités nécessaires pour faire preuve d'esprit critique et identifier la désinformation.

Troisièmement, en appliquant les idées des efforts qui précèdent, élargir les communications avec les Canadiennes et les Canadiens de tous les âges au sujet de la désinformation étrangère, doter les gens des outils et de l'éducation nécessaires pour penser de façon critique et identifier la désinformation. Des initiatives d'éducation et de littératie numérique pertinentes sur le plan culturel et auxquelles le public peut s'identifier, en plus que dans des langues autres que l'anglais et le français, peuvent être particulièrement importantes pour atteindre les communautés vulnérables. Le soutien d'initiatives locales comme les sites communautaires Factchequeado et Auntie Betty, ainsi que d'organismes locaux, élargira la portée de l'éducation à la littératie numérique aux personnes qui se trouvent à l'extérieur du système éducatif formel.[20] Toutes les initiatives et tout le matériel devraient être créés conjointement avec les membres des communautés de la diaspora afin d'avoir un impact complet et de renforcer la confiance dans les institutions démocratiques. Les personnes participantes ont également suggéré la nécessité de présenter à la population des initiatives de programmes d'alphabétisation numérique comme des occasions de renforcer d'autres compétences, d'éviter les escroqueries et d'engager des acteurs de confiance comme des influenceuses et influenceurs et des vedettes pour renforcer la résilience des citoyennes et citoyens à une plus grande échelle.

Les personnes participantes à l'atelier ont souligné la nécessité de renforcer les capacités des communautés plutôt que de s'en remettre uniquement à la réglementation, en offrant la possibilité de prévenir et de neutraliser l'information erronée et la désinformation afin de former des citoyennes et citoyens compétents sur le plan numérique. Les discussions ont également mentionné le besoin ultime d'une éducation civique élargie et

d'une plus grande attention à la culture d'information « bonne et exacte », plutôt que de lutter uniquement contre la fausse information, afin de rétablir la confiance dans les institutions.

En revanche, certaines personnes participantes ont exprimé leur scepticisme quant à l'efficacité de l'éducation et de la communication élargie en tant qu'approche unique, en soulignant les tactiques de surcharge cognitive utilisées par certains acteurs étatiques étrangers sur les médias sociaux. Les personnes participantes ont expliqué que l'encombrement de l'espace d'information conduit à l'apathie et à la paralysie de l'information, et ont fait allusion à la manière dont les nouvelles et le contenu « sombres » et accrocheurs peuvent prendre le dessus sur les efforts d'éducation. D'autres ont pointé les racines de la surcharge cognitive par les concepts de guerre psychologique de quatrième et cinquième génération, visant à créer une méfiance à l'égard des spécialistes, des scientifiques et des institutions.

THÈME CLÉ 2

Niveau société civile et entreprises

Cette section examine les façons dont la société civile et les entreprises – y compris les plateformes de médias sociaux – s'impliquent dans la lutte contre la désinformation et offre des occasions potentielles de renforcer et de coordonner les efforts de la société civile et de l'industrie.

L'ENJEU :

Différents organismes et plateformes, comme les médias, les bibliothèques, les écoles, les organismes d'aide à l'établissement des personnes nouvellement immigrées, les groupes communautaires culturels et les plateformes en ligne, font des efforts pour prévenir les menaces qui pèsent sur les personnes et les communautés exposées à la désinformation.

RÉSUMÉ DES OCCASIONS POTENTIELLES :

- **Renforcer la protection des journalistes, des membres de la société civile, des chercheuses et des chercheurs contre le harcèlement et les menaces liés à leur travail de lutte contre la désinformation.**
- **Améliorer les outils qui permettent aux personnes dirigeantes et aux organismes communautaires d'accroître la résilience et de démystifier la désinformation étrangère au sein de leurs communautés.**
- **Lutter contre la propagation de la désinformation étrangère sur les plateformes en ligne par le biais d'initiatives de vérification des faits, de restrictions sur les outils comme les robots, de comportements inauthentiques coordonnés et de contenus générés par l'IA, et de l'application de politiques contre la désinformation par le biais de publicités payantes.**

Qu'il s'agisse de journalistes, de bibliothécaires ou de personnel enseignant, les membres de la société civile sont de plus exposés à la désinformation étrangère et touchés par elle. Néanmoins, en raison des changements rapides de la désinformation et de l'évolution de l'utilisation de l'IA pour générer et répandre de la désinformation, des tentatives coordonnées pour mettre fin à sa propagation et protéger l'écosystème d'information ont souvent échoué. Même s'il s'est avéré difficile d'empêcher la création de fausses informations et d'arrêter de façon préventive leur propagation, certaines mesures peuvent être prises de façon continue pour protéger et doter les membres de la société civile des outils et des capacités nécessaires pour éviter les menaces envers les personnes et les communautés qui sont exposées à la désinformation.

Il est devenu de plus en plus difficile pour les journalistes de trouver la vérité dans un écosystème d'information pollué, de signaler les événements récents avec précision et de se tenir au courant de l'actualité. Les journalistes, les chercheuses, les chercheurs et les membres de la société civile qui s'intéressent à des sujets comme la désinformation et l'examen des clivages sociaux sont devenus la cible de harcèlement et d'intimidation en ligne au Canada et à l'étranger.[21]

Les plateformes en ligne ont également, à des degrés divers, déployé des mesures pour lutter contre la désinformation. Par exemple, plusieurs plateformes ont mis en place des politiques et des mesures visant à atténuer les comportements coordonnés inauthentiques qui caractérisent souvent les campagnes de désinformation étrangère dans le but d'amplifier artificiellement de faux récits, avec un succès mitigé.[22] Certaines plateformes ont également

établi des partenariats avec des gouvernements, des organismes et des initiatives de vérification des faits pour s'assurer de l'exactitude de l'information diffusée en ligne, dans le cas des élections, ou des urgences de santé publique.

Nous avons déterminé trois occasions de renforcer le travail des organismes de la société civile et des entreprises.

Renforcer la protection et les ressources des journalistes, des membres de la société civile, des chercheuses et des chercheurs contre le harcèlement et les menaces liés à leur travail de lutte contre la désinformation.

Premièrement, accroître la protection contre le harcèlement en ligne, les menaces et le piratage contre des personnes comme les journalistes, les chercheuses, les chercheurs et les membres de la société civile. Le Projet de loi sur les préjudices en ligne du Canada offre des voies plus claires pour signaler les cas et recevoir du soutien dans les cas de haine ciblée, d'incitation à la violence et les abus par rapport aux images intimes, ainsi que d'assigner des nouvelles responsabilités pour les plateformes afin de minimiser les risques d'exposition à ce contenu.[23] Les Canada a également fait des investissements récents dans le renforcement de la cybersécurité des instituts de recherche afin d'atténuer le risque de menaces étrangères..[24] Les personnes participantes à l'atelier ont souligné le rôle des personnalités politiques dans la diffusion de la désinformation, et la nécessité d'une plus grande protection de la société civile pour qu'elle puisse interpeller les dirigeantes et les dirigeantes. Les personnes participantes ont fait référence à l'Election Amendment Act (Loi sur la modification des élections) de la Colombie-Britannique et à ses lois contre la désinformation sur le processus électoral, pour exprimer leur curiosité quant à l'application de la loi par l'administration des élections.

Les personnes participantes ont fait des suggestions pour mieux protéger les universitaires, les journalistes et la société civile qui s'adonnent à la recherche sur la désinformation, y compris un soutien juridique pour se défendre et les coûts connexes, une personne de soutien ou médiatrice pour aider les victimes et une application de la loi qui prendrait plus au sérieux les menaces en ligne.

Les discussions de l'atelier ont également mis en évidence la nécessité de financer davantage les efforts des organismes sans but lucratif et des universités visant à renforcer la résilience numérique de la population face à la désinformation. Les personnes participantes ont toutefois noté que si les fonds proviennent uniquement du gouvernement pour les initiatives d'alphabétisation numérique, le risque de perception de partialité peut être accru pour certaines communautés. Les personnes participantes ont exprimé la nécessité de diversifier les sources de financement philanthropiques, universitaires et autres pour ce travail.

Améliorer les outils qui permettent aux personnes dirigeantes et aux organismes communautaires d'accroître la résilience et de démystifier la désinformation étrangère au sein de leurs communautés.

Deuxièmement, les personnes participantes ont milité pour le besoin d'introduire de de nouveaux outils, codéveloppés en fonction des besoins des leaders et organismes communautaires pour accroître la résilience des communautés et démystifier la manipulation de l'information par les étrangers et l'ingérence étrangère. Ces outils devraient tenir compte du rôle de l'IA dans la création et la propagation de la désinformation, dans l'enseignement de la littératie numérique, qui inclut les compétences nécessaires pour distinguer le contenu généré par l'IA (p. ex. les « hypertrucages »). Les outils existants, comme les programmes d'études et les trousses d'outils sur la pensée critique, devraient également être mis à jour pour satisfaire aux besoins changeants de la population en raison de l'évolution de la technologie. Les outils créés pour cibler les communautés vulnérables, comme les diasporas, devraient idéalement être conçus en collaboration et intégrer les besoins culturels et linguistiques. Les balados du projet Xīn Shēng (anciennement le projet WeChat Project) sur la mésinformation en anglais et en chinois simplifié sont un exemple de ressources créées avec les besoins culturels et linguistiques à l'esprit.[25] La trousse d'outils du Council of Agencies

Serving South Asians (CASSA) pour lutter contre la haine en ligne est un autre exemple de ressources conçues avec et pour les communautés racialisées et les organismes impliqués dans la lutte contre la haine en ligne.[26] La collaboration avec les personnes qui travaillent déjà dans la lutte contre l'ingérence étrangère dans les communautés vulnérables et les leçons tirées de leurs pratiques exemplaires peuvent également servir de fondement à l'élaboration future de ressources.

Les personnes participantes à l'atelier ont également cité Taïwan, la Finlande et l'Estonie comme exemples de pays ayant réussi à déployer des activités de sensibilisation de la population par l'intermédiaire de la société civile, sur différentes tranches d'âge. En ce qui concerne Taïwan, les personnes participantes ont noté l'approche du pays consistant à cultiver des espaces d'information sains par l'intermédiaire d'organismes de la société civile, tout en maintenant les gouvernements à distance afin d'instaurer la confiance du public. La Finlande a mis en place une formation à l'esprit critique dès l'école maternelle ainsi qu'une émission aux heures de grande écoute destinée à renforcer les connaissances du public et des cours nationaux sur l'IA et l'alphabétisation numérique. L'Estonie dispose d'un modèle similaire pour enseigner l'éducation aux médias aux élèves en intégrant le contenu dans d'autres matières existantes.

Les personnes participantes ont aussi mentionné la nécessité de s'appuyer sur les questions et les préoccupations de l'ensemble de la population pour concevoir et promouvoir les programmes et les initiatives. Elles ont souligné l'intérêt de reconnaître le rôle de la famille proche, des amis, des employeurs et des entreprises dans la responsabilisation des gens par la diffusion d'information, la formation et la sensibilisation.

Parmi les exemples d'outils qui pourraient être adaptés au contexte canadien, citons les tableaux de bord et les sites Web qui suivent la désinformation en temps réel, à l'instar du site Web EUvsDisinformation, et d'autres qui suivent le récit officiel d'une question ou d'un événement, comme le site Web Hamilton 2.0 Dashboard aux États-Unis. Ces outils ont été proposés comme des références d'information potentiellement utiles pour les membres de la société civile et les journalistes.

Les personnes participantes ont également évoqué la nécessité d'aller plus loin que le renforcement de la résilience dans les espaces en ligne, mais aussi d'examiner les espaces « hors ligne » en étudiant la manière dont les gens s'engagent dans les espaces physiques et sociaux. Elles ont également discuté du rôle de la santé mentale ainsi que du vide que les communautés en ligne comblent en l'absence d'options hors ligne. Le rôle des bibliothèques et les interventions qu'elles pourraient organiser ont également été évoqués comme un élément essentiel de la réponse de la société civile. Les bibliothèques proposent par exemple des outils comme des cours sur les compétences numériques, des abonnements à des plateformes qui proposent des outils d'apprentissage en ligne comme LinkedIn Learning, et tirent parti de l'intérêt du public pour la lutte contre les fraudes et les escroqueries afin d'autonomiser et d'équiper les utilisatrices et utilisateurs sur le plan numérique.

Lutter contre la propagation de la désinformation étrangère sur les plateformes en ligne par le biais d'une combinaison d'approches.

Troisièmement, les personnes participantes ont recommandé d'encourager les plateformes en ligne à amplifier leurs efforts afin de protéger les gens qui les utilisent et réduire la propagation de la désinformation étrangère. Certaines plateformes de médias sociaux ont mis en place des mesures proactives, comme les restrictions relatives aux robots et aux comportements inauthentiques coordonnés, les politiques contre la désinformation au moyen de messages publicitaires payés et le déploiement actif de la vérification des faits et des coups de pouce (« nudges »). Toutefois, certaines plateformes sont plus actives que d'autres dans la lutte contre la désinformation. Par exemple, si Meta a fait preuve d'une certaine diligence dans l'identification et la suppression des comptes inauthentiques, ces mêmes comptes existent toujours sur X (anciennement Twitter).[27] De plus, Meta a récemment annoncé

un plan pour étiqueter le contenu généré par l'intelligence artificielle, à l'aide de marqueurs visibles et de filigranes invisibles pour identifier le contenu sélectionné.[28] Cependant, ces efforts sont limités, car le contenu ne sera étiqueté que s'il comporte des filigranes et des métadonnées préexistantes, indiquant qu'il a été généré par l'IA.[29] La publicité en ligne est un autre domaine que les plateformes en ligne peuvent contrôler davantage, sachant que 92 % de la publicité canadienne sur Internet est attribuée à des plateformes et sites Internet étrangers.[30]

Comme pour la Loi sur l'intelligence artificielle de l'Union européenne,[31] es modifications proposées à Loi sur l'intelligence artificielle et les données du Canada dans le projet de loi C-27 comprennent des exigences relatives aux plateformes d'IA génératives pour permettre la détection de contenus audiovisuels générés par l'IA.[32] Les spécialistes s'attendent à ce que les plateformes mettent à jour leurs politiques sur les médias synthétiques avant la prochaine période électorale.[33]

Bien que les personnes participantes à l'atelier se soient accordées sur la nécessité d'une gouvernance des plateformes, elles ont reconnu les nuances dans les perceptions des citoyennes et citoyens, en fonction de la personne qui identifie la fausse information et la désinformation (qu'il s'agisse d'une communauté, d'une plateforme ou d'un acteur étatique). Les personnes participantes ont cité Wikipédia et les Community Notes de X comme de bons exemples d'externalisation ouverte d'information vérifiée. Les personnes participantes ont aussi mentionné la campagne de Mozilla sur la responsabilité des plateformes, au début du mois d'avril 2024, comme un exemple d'effort pour pousser les plateformes comme WhatsApp à agir de manière plus responsable sans réglementation. Grâce à la lettre de Mozilla à WhatsApp, qui demande à la plateforme d'ajouter des frictions aux transferts de messages, des étiquettes d'avertissement de désinformation au contenu viral et de réduire les capacités de diffusion de la plateforme pendant la période électorale mondiale de 2024, le public peut participer à la campagne en s'inscrivant.[34]

Les personnes participantes ont souligné la nécessité d'une plus grande transparence de la part des plateformes en ce qui concerne l'intégrité de l'information ainsi que la nécessité d'accéder à des données sur les mesures de gouvernance des plateformes qui ont été efficaces dans le passé, afin d'éclairer les mesures futures. Les discussions ont également mentionné le Projet de loi sur les préjudices en ligne et le rôle de la personne médiatrice, bien qu'il couvre étroitement les préjudices sélectifs, et ont suggéré d'introduire des exigences minimales pour les ressources des plateformes en ce qui concerne leurs équipes et activités « confiance et sécurité », qu'il s'agisse de la modération du contenu ou de la révision fréquente des politiques de la plateforme.

Les discussions ont porté sur les limites des mesures de gouvernance des plateformes et on y a cité l'absence de telles mesures sur les plateformes de messagerie privée comme WeChat. Les personnes participantes ont également souligné la nécessité de rechercher une coopération internationale en matière de gouvernance des plateformes, compte tenu de la nature multinationale de leurs activités et de leur gouvernance. Les personnes participants ont aussi exprimé leur scepticisme à l'égard des plateformes, qui ne sont pas incitées à mettre en œuvre des mesures de gouvernance plus strictes, à moins que des sanctions ne les y obligent.

THÈME CLÉ 3

Niveau gouvernements et institutions

Dans cette section, nous discutons des décisions que doivent prendre les gouvernements lorsqu'ils luttent contre l'ingérence étrangère ainsi que des occasions d'améliorer le partage d'information et de renforcer la confiance du public.

L'ENJEU :

Le fait pour les gouvernements de rechercher un équilibre entre la divulgation des menaces d'ingérence étrangère et le besoin de respecter le droit à la vie privée ainsi que le maintien des sources de renseignements classifiés peut contrecarrer les efforts de lutte contre les menaces.

RÉSUMÉ DES OCCASIONS POTENTIELLES :

- **Revoir le seuil à partir duquel les gouvernements sont tenus de communiquer de l'information au public ou aux communautés touchées en cas d'attaque informatique, afin d'encourager un échange plus ouvert dans la mesure du possible.**
- **Prévoir et créer des plans d'action pour réagir de manière proactive aux effets secondaires négatifs potentiels liés à la divulgation d'ingérences étrangères.**
- **Examiner les vulnérabilités qui ont été exploitées par les campagnes de désinformation étrangères afin d'en tirer des enseignements pour le Canada.**

Les institutions démocratiques sont confrontées au défi de maintenir la transparence auprès de la population en divulguant les menaces d'ingérence étrangère, tout en protégeant le public des risques de violation de la vie privée, par exemple, en taxant l'analyse sur le matériel de source ouverte et en maintenant les sources de renseignements classifiés qui recueillent les menaces de l'étranger. Cela se fait en reconnaissant les difficultés à établir une distinction claire entre la désinformation étrangère et la désinformation nationale, étant donné la nature de l'écosystème d'information. La portée de l'influence de l'information étrangère s'étend également au-delà de la désinformation vérifiable, par exemple par la pollution de l'information et l'amplification des désaccords subjectifs qui ont un impact considérable sur les perceptions individuelles et la confiance dans l'environnement de l'information. Le gouvernement du Canada a récemment pris des mesures pour accroître la transparence, y compris une consultation sur un registre visant la transparence en matière d'influence étrangère, ainsi que des modifications à la Loi sur le Service canadien de renseignement de sécurité afin de permettre une meilleure divulgation de l'information en dehors du gouvernement du Canada.[35]

Le mécanisme de réponse rapide du Canada (MRR) a fait part de cas d'opérations d'information détectées, y compris la probable campagne de « spamouflage » (divulgation de pourriels) en 2023, dans laquelle des réseaux de robots ont ciblé sur Facebook et X des députées et députés du Canada.[36] Des chercheuses et chercheurs ont examiné le rôle de la Russie dans le convoi de la liberté, tandis que d'autres ont fait part de leurs propres expériences de la désinformation étrangère dans le cadre d'une campagne politique.[37] Quel que soit le forum dans lequel les renseignements et rapports sur la désinformation sont communiqués, la communication de l'information demeure un important acte de transparence qui permet des contre-mesures comme l'inoculation psychologique et le renforcement de la confiance entre le gouvernement et la population canadienne.

Nous avons déterminé trois occasions clés pour les institutions démocratiques de réagir aux menaces de désinformation étrangère.

Revoir le seuil à partir duquel les gouvernements sont tenus de communiquer de l'informations au public ou aux communautés touchées en cas d'attaque informatique, dans la mesure du possible.

Les gouvernements peuvent revoir le seuil à partir duquel ils sont tenus de communiquer de l'informations au public en cas d'attaque informatique, afin d'encourager un échange plus ouvert dans la mesure du possible, particulièrement pour remédier aux vides d'information. Les personnes participantes à l'atelier ont souligné la nécessité de fournir davantage de contexte lors de la communication d'information, afin de mieux informer les citoyennes et citoyens qui ne connaissent probablement pas le contexte mondial ou historique d'une question. L'importance du format dans lequel les renseignements sont communiqués a également été soulevée au cours des discussions, en raison de la nécessité de renforcer et d'exploiter la confiance des citoyennes et citoyens dans des sources fiables. VIGINUM, une agence gouvernementale dédiée à la publication de contenu officiel dans le but de détecter et de caractériser les interférences numériques étrangères en France, a été citée comme un exemple pertinent.[38] Toutefois, certaines personnes participantes ont contesté la volonté des gouvernements d'être plus transparents et ont fait remarquer qu'il serait difficile de fixer ces seuils de manière non partisane, en particulier en ce qui concerne la désinformation sur des sujets politiques sensibles.

Par l'entremise des rapports du MRR, du protocole public en cas d'incident électoral majeur et d'autres renseignements sur la mésinformation et la désinformation étrangères, les gouvernements devraient régulièrement revoir leurs méthodologies et leurs seuils en matière de surveillance et de divulgation éthiques. En reconnaissant les avantages et les conséquences de la messagerie cryptée, les personnes participantes à l'atelier ont souligné la nécessité de maintenir un cryptage fort et de rechercher d'autres moyens de collecter des renseignements, comme les métadonnées, l'information de sources ouvertes, les rapports de transparence des plateformes privées ainsi que l'engagement direct et les enquêtes.

Prévoir et créer des plans d'action pour réagir de manière proactive aux effets secondaires négatifs potentiels liés à la divulgation d'ingérences étrangères.

En plus de la surveillance et de la divulgation, les gouvernements peuvent également prévoir et créer des plans d'action proactifs pour parer aux conséquences négatives potentielles liées à la divulgation de la désinformation étrangère. Les personnes participantes ont souligné la nécessité pour les gouvernements d'intervenir avec discernement et de veiller à ce que leurs interventions ne deviennent pas des actes d'ingérence dans les processus démocratiques comme les élections. Cela a été mentionné en particulier en relation avec les défis que les agences de sécurité et de renseignement peuvent rencontrer par les méthodes de collecte de renseignements, afin de s'assurer que ces méthodes n'ont pas d'impact direct ou indirect sur les résultats des élections.

Les personnes participantes à l'atelier ont également suggéré de procéder à une évaluation annuelle de la menace que représente la désinformation étrangère et à des mises à jour régulières de l'écosystème de l'information, à l'instar de l'évaluation nationale de la cybermenace ou dans le cadre de celle-ci. Il s'agirait d'un effort proactif de la part du gouvernement pour pré-renseigner les questions émergentes, réduire les risques de sensationnalisme et tenir les gouvernements et les institutions à tous les niveaux informés des menaces qui pèsent sur le pays de manière plus détaillée que ce qui est actuellement disponible.

Examiner les vulnérabilités qui ont été exploitées par les campagnes de désinformation étrangères afin d'en tirer des enseignements pour le Canada.

Les campagnes de désinformation étrangère ont également exploité la polarisation accrue et l'approfondissement des clivages sociaux existants pour cibler et exploiter les divisions au Canada. Les gouvernements et les organismes publics devraient également prendre l'occasion de revoir les vulnérabilités existantes, au lieu de se concentrer uniquement sur les menaces connues. À l'instar de l'examen du mouvement pour la liberté de la Commission sur l'état d'urgence, d'autres clivages sociaux peuvent être analysés de la même manière afin d'éclairer de futures mesures préparatoires.[39] Un examen approfondi et interministériel des menaces possibles de l'extrémisme violent motivé par la politique, la religion et l'idéologie, telles qu'elles sont décrites dans le rapport de juin 2023 du groupe de travail SITE (Security and Intelligence Threats to Elections), pourrait constituer un bon point de départ.[40]

Parmi les exemples internationaux de divisions exploitées, on peut citer les campagnes russes qui visent à semer la discorde entre les groupes raciaux et religieux, en s'appuyant sur le mouvement « Black Lives Matter », et les tensions religieuses consécutives aux déclarations incendiaires de l'ancien président des États-Unis, M. Trump.[41] Les personnes participantes ont également mentionné le mouvement MAGA aux États-Unis, et ont souligné sa nature organique dans l'organisation, qui n'est pas uniquement motivée par des campagnes de désinformation. D'autres personnes participantes ont fait état de campagnes chinoises visant les manifestants pour la démocratie à Hong Kong et de campagnes indiennes visant les manifestations d'agriculteurs, dans le but de discréditer les gens et leurs mouvements.[42]

Une personne participante a pu réfléchir à son expérience personnelle d'interaction avec les manifestantes et manifestants pendant le Convoi de la liberté, dans l'espoir de comprendre leur point de vue et d'engager la conversation. D'autres personnes participantes ont souligné la nécessité de s'engager auprès des nouvelles arrivantes et nouveaux arrivants dès leur arrivée au Canada, en leur donnant les moyens d'exercer leur esprit critique, de fournir de l'information exacte sur les institutions et les médias canadiens et de dissiper toute méfiance potentielle à l'égard du gouvernement canadien.

En effectuant de façon proactive une analyse des tensions en ligne et hors ligne, en travaillant de façon transparente et en dialoguant véritablement avec des groupes communautaires, en satisfaisant aux besoins des communautés et en leur fournissant des ressources, les institutions ont la possibilité de renforcer la confiance du public et augmenter sa résilience face aux menaces futures.

References

[1] Centre canadien pour la cybersécurité. « Évaluation des cybermenaces nationales 2023-2024 ». https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024. L'Évaluation des cybermenaces nationales 2023-2024 se sert du terme MDM – mésinformation, désinformation et malinformation. La mésinformation désigne le fait de diffuser de la fausse information sans avoir de mauvaises intentions; par désinformation, on entend le fait de diffuser de la fausse information dans le but de manipuler ou de tromper des personnes, des organisations et des États ou bien de leur faire du tort; et pour ce qui est de la malinformation, il s'agit du fait de diffuser de l'information qui repose sur un fait, mais qui est souvent exagérée de façon à tromper ou même à causer des préjudices.

[2] Gouvernement du Canada. « Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections », juin 2023, https://www.canada.ca/fr/institutions-democratiques/services/rapports/groupe-travail-menaces-matiere-securite-renseignements-visant-elections-menaces-elections-partielles-federales-canada-juin-2023.html; Affaires mondiales Canada. « Mécanisme de réponse rapide du Canada : Affaires mondiales Canada. » https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=fra; Loi sur la modernisation des élections, Lois du Canada 2018, ch. 31. https://laws-lois.justice.gc.ca/fra/LoisAnnuelles/2018_31/page-1.html.

[3] Gouvernement du Canada. « Initiative de citoyenneté numérique – la désinformation en ligne et les autres préjudices et menaces en ligne », https://www.canada.ca/fr/patrimoine-canadien/services/desinformation-en-ligne.html.

[4] Gouvernement du Canada. Institutions démocratiques, « Modifications proposées à la Loi électorale du Canada » https://www.canada.ca/fr/institutions-democratiques/nouvelles/2024/03/modifications-proposees-a-la-loi-electorale-du-canada.html.

[5] Centre canadien pour la cybersécurité. « Évaluation des cybermenaces nationales 2023-2024 », https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024.

[6] Dawood, Yasmin. « Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats », Election Law Journal: Rules, Politics, and Policy 20, no. 1 (17 mars 2021): 10-31. http://doi.org/10.1089/elj.2020.0652.; Media Ecosystem Observatory. « Mis- and Disinformation During the 2021 Canadian Federal Election », mars 2022. https://www.mcgill.ca/maxbellschool/files/maxbellschool/meo_election_2021_report.pdf; McQuinn, Brian, Marcus Kolga, Cody Buntain et Laura Courchesne. « Enemy of My Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support to Ukraine », Conflict Report Series. Centre for Artificial Intelligence, Data, and Conflict, mars 2023, https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf?index=true.

[7] McMahon, Dave. « Maligned Influence and Interference in Canada », Institut canadien des affaires mondiales, juillet 2023, https://www.cgai.ca/maligned_influence_and_interference_in_canada.

[8] Cybersecurity & Infrastructure Security Agency. « Foreign Influence Operations and Disinformation », https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.

[9] Naomi Nix et Cat Zakrzewski, « U.S. Stops Helping Big Tech Spot Foreign Meddling Amid GOP Legal Threats », The Washington Post, 30 novembre 2023, https://www.washingtonpost.com/technology/2023/11/30/biden-foreign-disinformation-social-media-election-interference/.

[10] U.S. Department of State. « The Framework to Counter Foreign State Information Manipulation », (fiche d'information), 18 janvier 2024, https://www.state.gov/the-framework-to-counter-foreign-state-information-manipulation/.; Gouvernement du Canada. « Déclaration commune du Canada, des États-Unis et du Royaume-Uni sur la manipulation de l'information étrangère », 16 février 2024, https://www.canada.ca/fr/affaires-mondiales/nouvelles/2024/02/declaration-commune-du-canada-des-etats-unis-et-du-royaume-uni-sur-la-manipulation-de-linformation-etrangere.html.

[11] European Union External Action. « Tackling Disinformation, Foreign Information Manipulation & Interference », 27 octobre 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en; Commission européenne. « Le code de bonnes pratiques de 2022 en matière de désinformation », 4 juillet 2022, https://digital-strategy.ec.europa.eu/fr/policies/code-practice-disinformation.

[12] EUvsDisinfo. https://euvsdisinfo.eu/fr/.

[13] République française. « LOI no 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1) », https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/.

[14] Department for Digital, Culture, Media & Sport, and Caroline Dinenage MP. « Minister launches new strategy to fight online disinformation », GOV.UK, 14 juillet 2021, https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation.

[15] Wark, Wesley. « Foreign Interference Online: Where Disinformation Infringes on Freedom of Thought », Centre for International Governance Innovation, 22 janvier 2024, https://www.cigionline.org/publications/foreign-interference-online-where-disinformation-infringes-on-freedom-of-thought/; Trauthig, Inga. « Diaspora Communities and Computational Propaganda on Messaging Apps. » Centre for International Governance Innovation, janvier 2024. https://www.cigionline.org/static/documents/PB_no.183.pdf.

[16] Parlement du Canada. « L'ingérence étrangère et les menaces entourant l'intégrité des institutions démocratiques, de la propriété intellectuelle et de l'état canadien : Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique ». octobre 2023. https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/rapport-10; Gouvernement du Canada. « Des activités ciblant un député canadien sur WeChat suggère une possible ingérence étatique étrangère », https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/wechat.aspx?lang=fra.

[17] Centre canadien pour la cybersécurité. « Évaluation des cybermenaces nationales 2023-2024 », https://www.cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2023-2024; McQuinn, Brian, Marcus Kolga, Cody Buntain et Laura Courchesne. « Enemy of My Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support to Ukraine », Conflict Report Series. Centre for Artificial Intelligence, Data, and Conflict, mars 2023, https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf?index=true.

[18] Bridgman, Aengus, Alexei Abrahams, Thomas Bergeron, Thomas Galipeau, Blake Lee-Whiting, Haaya Naushan, Jennie Phillips, Zeynep Pehlivan, Saewon Park, Sara Parker, Benjamin Steel, Peter Loewen et Taylor Owen. « The Canadian Information Ecosystem », Media Ecosystem Observatory (Canadian Digital Media Research Network), 2023, https://osf.io/b29q8/download/?format=pdf.

[19] Sirlin, Nathaniel, Ziv Epstein, Antonio A. Arechar et David G. Rand. « Digital Literacy is Associated with More Discerning Accuracy Judgments but not Sharing Intentions », Harvard Kennedy School (HKS) *Misinformation Review*, décembre 2021, https://misinforeview.hks.harvard.edu/article/digital-literacy-is-associated-with-more-discerning-accuracy-judgments-but-not-sharing-intentions/.

[20] Factchequeado, https://factchequeado.com/english/; Auntie Betty, https://auntiebetty.ca/.

[21] Fenlon, Brodie. « Our Journalists are Facing More Harassment, Threats for Doing Their Jobs », CBC News. 8 février 2022. https://www.cbc.ca/news/editorsblog/editor-note-pandemic-protests-media-experience-1.6343672; Smit, Cristina. « Data on Online Hate Directed at BBC Journalists Mirrors Global Trend ». VOA News, 10 août 2023. https://www.voanews.com/a/data-on-online-hate-directed-at-bbc-journalists-mirrors-global-trend/7220041.html.

[22] Murero, Monica. « Coordinated Inauthentic Behavior: An Innovative Manipulation Tactic to Amplify COVID-19 Anti-vaccine Communication Outreach via Social Media ». Frontiers in Sociology 8 (8 mars 2023), doi:10.3389/fsoc.2023.1141416; Stricklin, Kasey. « Social Media Bots: Laws, Regulations, and Platform Policies ». Center for Naval Analyses, septembre 2020, https://apps.dtic.mil/sti/trecms/pdf/AD1112566.pdf.

[23] Parlement du Canada. « Projet de loi C-63 », https://www.parl.ca/documentviewer/fr/44-1/projet-loi/C-63/premiere-lecture.

[24] Gouvernement du Canada. « Nouvel investissement visant à rehausser la sécurité de la recherche au Canada » (communiqué), 14 novembre 2022, https://www.rsf-fsr.gc.ca/news_room-salle_de_presse/latest_news-nouvelles_recentes/2022/new_investment_research_security_capacity-nouvel_investissement_securite_recherche_canada-fra.aspx.

[25] Xīn Shēng Project. « Podcast. » https://www.xinshengproject.org/archive.

[26] Council of Agencies Serving South Asians (CASSA). « #EradicateHate: A Collaborative to Combat Online Hate », https://www.cassa.ca/eradicatehate/.

[27] Menn, Joseph, Aaron Schaffer, Naomi Nix and Clara Ence Morse. « Chinese Propaganda Accounts Found By Meta Still Flourish on X »,The Washington Post, 16 février 2024, https://www.washingtonpost.com/technology/2024/02/16/x-meta-china-disinformation/; Hénin, Nicolas et Maria Giovanna Sessa. « Disinformation on X: Research and Content Moderation Policies », EU DisinfoLab, janvier 2024, https://www.disinfo.eu/wp-content/uploads/2024/01/20240116_Twitter-X_factsheet.pdf.

[28] Clegg, Nick. « Labeling AI-Generated Images on Facebook, Instagram and Threads », Meta, 6 février 2024, https://about.fb.com/news/2024/02/labeling-ai-generated-images-on-facebook-instagram-and-threads/.

[29] Irwin, Kate. « Meta will Label AI-Generated Content, But There's a Catch », PCMag, 6 février 2024, https://www.pcmag.com/news/meta-will-label-ai-generated-content-but-theres-a-catch.

[30] Miller, Peter et David Keeble. « Close the Loophole! The Deductibility of Foreign Internet Advertising », Les amis des médias canadiens, 6 mars 2024. https://friends.ca/wp-content/uploads/2024/03/Close-the-Loophole-2024-update-March-6-FINAL-1.pdf.

[31] Commission européenne. « Loi sur l'IA. » (dernière mise á jour le 6 mai 2024), https://digital-strategy.ec.europa.eu/fr/policies/regulatory-framework-ai.

[32] Innovation, Sciences et Développement économique Canada. « Code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés », septembre 2023. https://ised-isde.canada.ca/site/isde/fr/code-conduite-volontaire-visant-developpement-gestion-responsables-systemes-dia-generative-avances; Parlement du Canada. « Projet de loi C-27 », https://www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-27.

[33] Michelle Bartleman et Elizabeth Dubois, « Les utilisations politiques de l'IA au Canada », Labo Pol Comm Tech, Université d'Ottawa, 2024, https://fr.polcommtech.com/_files/ugd/eeebb0_f0a8b44897ac42dcb6db727269bb9db1.pdf.

[34] Mozilla, « WhatsApp: Reform Features *Now* to Protect Election Integrity », Mozilla, 2 avril 2024, https://foundation.mozilla.org/fr/blog/whatsapp-reform-features-now-to-protect-election-integrity/.

[35] Service canadien du renseignement de sécurité. « Lancement d'une initiative du gouvernement du Canada visant à consulter le public au sujet des modifications législatives proposées pour contrer l'ingérence étrangère », 24 novembre 2023, https://www.canada.ca/fr/service-renseignement-securite/organisation/lancement-dune-initiative-du-gouvernement-du-canada-visant-a-consulter-le-public-au-sujet-des-modifications-legislatives-proposees-pour-contrer-l-ingerence-etrangere.html. Sécurité publique Canada. « Rapport "Ce que nous avons entendu" : Bilan des consultations des Canadiens sur le bien-fondé d'un registre pour la transparence en matière d'influence étrangère », novembre 2023. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nflnc-wwh/index-fr.aspx.

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

[37] Orr Bueno, Caroline. « Russia's Role in the Far-Right Truck Convoy: An Analysis of Russian State Media Activity Related to the 2022 Freedom Convoy », The Journal of Intelligence, Conflict, and Warfare 5, No. 3, (31 janvier 2023), https://journals.lib.sfu.ca/index.php/jicw/article/view/5101; Shahrooz, Kaveh [@kshahrooz]. « In light of insufficient time to conduct a campaign and due to unprecedented foreign interference which regrettably went unaddressed, I am hereby withdrawing from the Conservative Party of Canada nomination election in the riding of Richmond Hill. My full statement », X, 22 février 2024, https://twitter.com/kshahrooz/status/1760621192182923506?s=46&t=izoswVl4edVit4U2W3N56Q.

[38] Secrétariat général de la défense et de la sécurité nationale. « Service de vigilance et protection contre les ingérences numériques étrangères », 17 novembre 2022, https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

[39] Graves, Frank. « Document commandé : Série sur les clivages sociaux : Comprendre le mouvement pour la liberté : Causes, conséquences et réponses possibles », Commission sur l'état d'urgence, https://commissionsurletatdurgence.ca/files/documents/Policy-Papers/S%C3%A9rie-sur-les-clivages-sociaux-Comprendre-le-mouvement-pour-la-libert%C3%A9-causes-cons%C3%A9quences-et-r%C3%A9ponses-possible.pdf.

[40] Bronskill, Jim. « Anti-authority Narratives Could Tear "fabric of society", Intelligence Report Warns », CTV News, 24 mars 2024, https://www.ctvnews.ca/politics/anti-authority-narratives-could-tear-fabric-of-society-intelligence-report-warns-1.6820025.

[41] Entous, Adam, Craig Timberg et Elizabeth Dwoskin, « Russian Operatives Used Facebook Ads to Exploit America's Racial and Religious Divisions », The Washington Post, 25 septembre 2017, https://www.washingtonpost.com/business/technology/russian-operatives-used-facebook-ads-to-exploit-divisions-over-black-political-activism-and-muslims/2017/09/25/4a011242-a21b-11e7-ade1-76d061d56efa_story.html.

[42] Wong, Tessa. « Technology has Become the Double-edged Sword of Asia's Protests », BBC, 25 mars 2023, https://www.bbc.com/news/world-asia-64300442.