Comment explique-t-on l'action publique du Canada pour répondre à la désinformation ?

MÉMOIRE – API 6999

Nicolas Larivière

Maîtrise en affaires publiques et internationales
Maître ès arts (M.A.)

École supérieure d'affaires publiques et internationales
Université d'Ottawa
Ottawa, Canada

15 juin 2022

Université d'Ottawa

« **The problem with quotes found on the internet is that they are often not true** »

- **Abraham Lincoln**

REMERCIEMENTS

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Je tiens d'abord à remercier ma partenaire, Corélia, pour sa patience et son soutien indéfectible au cours des derniers mois.

J'aimerais aussi remercier Patrick Leblond, directeur de ce mémoire, pour tous ses conseils, son aide, et son encadrement chaleureux.

Finalement, un grand merci à Larry pour son humour essentiel, et pour m'avoir épaulé moralement tous les jours dans la construction de ce mémoire.

TABLE DES MATIÈRES

Table des matières

RÉSUMÉ

L'information, à l'ère du numérique, se transmet à un rythme inégalé dans l'histoire. La rapidité et la portée de la propagation de la désinformation ne fait pas exception. Les nouvelles technologies et la popularité grandissante des médias sociaux facilitent la capacité des acteurs étatiques et non étatiques de propager de l'information trompeuse pour atteindre leur fin. Alors que le gouvernement canadien prend au sérieux les risques que pose la désinformation, le Canada a mis en place diverses mesures pour répondre à ce phénomène au cours des dernières années. À l'aide d'une analyse qualitative, ce mémoire cherche à comprendre comment s'explique la réponse du gouvernement canadien. Après avoir présenté une revue de la littérature sur le thème de la désinformation, le présent mémoire dresse un éventail des mesures du Canada pour répondre à cet enjeu. Ensuite, ce mémoire cherchera à expliquer que l'incohérence entre les nombreuses mesures canadiennes peut s'expliquer par les défis de répondre à la désinformation, mais aussi par une sécuritisation de la désinformation. Enfin, le mémoire propose des recommandations pour améliorer la réponse à la désinformation au Canada.

ABSTRACT

In the digital age, information is transmitted at a rate unmatched in history, and the rapid spread of disinformation is no exception. New technologies and the popularity of social media make it easier for state and non-state actors to spread misleading information to achieve their goals. The Canadian government takes the risks associated with disinformation seriously and has put in place several measures to address this phenomenon in recent years. Using a qualitative analysis, this paper seeks to explain the Canadian government's response. After presenting a literature review on the topic of disinformation, this paper examines Canada's actions to address this issue. Then, it seeks to explain that the inconsistency between the many Canadian measures can be explained by the challenges of disinformation, but also by a securitization of the issue. Finally, the paper proposes recommendations to improve Canada's response to disinformation.

Liste des Abréviations

AMC : Affaires mondiales Canada

CST : Centre de la sécurité des télécommunications

DCMS: Department for Digital, Culture, Media & Sport

FCO: Foreign & Commonwealth Office

GRC: Gendarmerie royale du Canada

HMG: Her Majesty's Government

IRA: Internet Research Agency

MRR : Mécanisme de réponse rapide du G7

MSB: The Swedish Civil Contingencies Agency

NSCR: National Security Capability Review

ONG : Organisations non gouvernementales

OTAN : Organisation du Traité de l'Atlantique Nord

SCRS : Service canadien du renseignement de sécurité

SITE : Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections

1. Introduction

« You're *fake news* ! ». C'est ce qu'a répondu l'ex-président américain Donald Trump à un journaliste de CNN parce qu'il était insatisfait de la couverture de l'institution médiatique à son égard. Cette référence aux *fake news*, omniprésente pendant le mandat du président américain, est à l'image d'une rhétorique qui a contribué à la mise à l'ordre du jour de l'enjeu de la manipulation de l'information au sein du débat public, particulièrement dans les démocraties occidentales. Comme le suggère la Commission européenne (2018 : 10), le terme *fake news* sera évité pour décrire le phénomène étudié pour des raisons qui seront explorées dans ce mémoire. Le terme désinformation sera privilégié, qui fait plutôt référence à de l'information qui est « deliberately false or misleading»[1] (Jack, 2007 : 3). C'est donc sur ce concept que nous nous pencherons dans le cadre de cette rédaction.

L'intérêt politique et académique pour la désinformation dans l'histoire contemporaine est un phénomène relativement nouveau. Les chercheurs (p. ex. Jackson, 2022; Vilmer et coll., 2018) indiquent généralement deux évènements qui ont marqué un regain de l'intérêt pour la désinformation comme objet d'étude : l'annexion de la Crimée par la Russie en 2014 et les élections fédérales américaines de 2016. Depuis, « le sujet n'a cessé de croître. Tous les sondages confirment qu'il est une préoccupation majeure pour les populations, les journalistes, les ONG [organisations non gouvernementales] et les

[1] Traduction libre : délibérément fausse ou trompeuse.

gouvernements dans le monde entier, qui reconnaissent les dommages que ces manipulations peuvent causer à la société » (Vilmer et coll., 2018 : 22).

Comme nous allons voir dans ce mémoire, il existe un débat quant aux conséquences réelles de la désinformation. Par exemple, en lien aux campagnes de désinformation visant à interférer dans les élections, « certaines études disent observer des changements notables d'attitudes politiques chez les personnes exposées à de la désinformation venue de l'étranger [tandis que] d'autres suggèrent que cette dernière vient toucher avant tout les individus déjà prédisposés à la croire, et ne permet donc pas d'influencer significativement l'ensemble d'une population » (Rapin, 2021).

Cela étant dit, il faut reconnaitre que les « acteurs derrière celles-ci semblent pour leur part déterminés à y accorder des ressources significatives » (Rapin, 2021). Cela est possiblement dû au fait qu'il est possible d'observer certains impacts. En effet, là où il peut être difficile de mesurer les conséquences réelles de la désinformation sur les campagnes électorales ou sur l'opinion publique, il existe des instances ou un effet direct est observé. Si on retourne en novembre 1979,

> en marge de la prise d'otages de la grande mosquée de La Mecque, le KGB dissémina au Pakistan la rumeur que le gouvernement américain était secrètement derrière l'attaque. Des manifestants s'assemblèrent devant l'ambassade des États-Unis à Islamabad, des heurts éclatèrent, et un Marine en charge de la protection de l'ambassade ainsi que plusieurs membres du personnel perdirent la vie dans la foulée (Rapin, 2021).

Plus récemment, au Myanmar, des leaders antimusulmans ont utilisé Facebook pour propager de fausses informations visant à attiser la haine envers les Rohingyas (Gowen et Bearak, 2017). Ces « manipulations sur Facebook, à coups de fausses rumeurs et de photos retouchées, ont joué un rôle non négligeable dans la persécution des Rohingyas en Birmanie, que les Nations unies ont qualifiée de nettoyage ethnique » (Vilmer et coll., 2018 : 23). Par ailleurs, Vilmer et coll. (2018) utilisent aussi l'exemple de l'Inde en 2018 ou en « seulement deux mois […] une quinzaine de personnes ont été lynchées, dans tout le pays, suite à la diffusion de fausses rumeurs à leur endroit, ce qui a poussé les autorités à réagir en coupant temporairement l'accès à certaines plateformes numériques » (23). Finalement, plus largement, une étude britannique a démontré que l'information trompeuse avait un impact négatif sur l'acceptabilité des vaccins contre la COVID-19 au sein de la population (Loomba et coll., 2021). Sachant que de la fausse information sur la COVID a été propagée délibérément par certains acteurs, notamment la Russie et la Chine (Dubow et coll., 2021), on peut voir que la désinformation a même nui, à un certain degré, à la lutte contre la pandémie. Bref, il faut reconnaitre un phénomène ayant le potentiel d'être dévastateur sur certains aspects de la société, comme la cohésion sociale et la santé publique, ainsi que sur certains principes démocratiques comme la participation citoyenne et la tenue d'élections justes et équitables.

Pour en venir à notre objet d'étude, il faut souligner que le Canada n'est pas exempté des effets de la désinformation. Le tout récent exemple du « convoi de la liberté », qui a bloqué les rues d'Ottawa pendant plusieurs semaines, démontre la présence notable de ce phénomène au Canada, avec une partie des participants qui brandissait des messages

contradictoires et fallacieux sur leurs pancartes, comme « la Covid a été créée par Bill Gates » ou bien « la Covid n'existe pas » (Hum, 2022). Par ailleurs, ce convoi peut aussi servir d'exemple pour illustrer une instance de désinformation parrainée par l'État, un élément important de l'étude de la désinformation. Dans un article, le journaliste Andrew Nikiforuk démontre la similarité entre un éditorial de *Russia Today*, une agence médiatique appartement à l'État russe et les propos d'un organisateur du convoi, Tom Marazzo, tous deux proclamant de manière similaire la mise en place au Canada d'un système de crédit social comme celui de la Chine (Nikiforuk, 2022). Que cela représente une coïncidence ou non, Marcus Kolga, directeur de *Disinfowatch*, affirme avec certitude que des puissances étrangères se sont immiscées dans l'évènement. Ce dernier indique que « the pandemic provided a huge opportunity for Russia propaganda […] It is fuelling the movement we are now seeing in downtown Ottawa » (cité dans Nikiforuk, 2022). Cela est d'autant plus concernant lorsqu'on observe les discussions sur les réseaux sociaux de ces groupes qui sont déjà très enflammés, dans lesquels on peut y observer des appels à la pendaison d'experts médicaux et où l'on compare la vaccination au génocide (Stewart, 2021).

1.1 Question de recherche et méthodologie

Considérant tous ces éléments, ce travail part donc de l'hypothèse partagée par Heer et coll. (2021) que la désinformation « may threaten the health and safety of the Canadian public, as well as the legitimacy of democratic processes in Canada»[2] (5). Ce point de départ sous-entend que le problème est si important qu'il exige une action gouvernementale. De plus, nous remarquons, comme Jackson (2022), que le gouvernement

[2] Traduction libre : peut menacer la santé et la sécurité de la population canadienne, ainsi que la légitimité des processus démocratiques au Canada.

canadien, depuis 2014, n'a pas de politique cohérente face à la désinformation, ce qui mène à des actions fragmentées. Face à ce constat, nous nous posons donc la question suivante : comment explique-t-on l'action gouvernementale du Canada face à la désinformation depuis environ une décennie ? Pour répondre à cette question, ce travail consistera en une analyse qualitative de la recherche faite sur la désinformation et des mesures mises en place au Canada pour contrer celle-ci.

La première partie de cette rédaction se concentre sur une revue de la littérature du thème à l'étude. Nous y clarifions les différents concepts pertinents et verrons où en est la recherche sur ce sujet. Une attention particulière est portée sur l'évolution de la désinformation jusqu'à l'ère du numérique, sur les acteurs, ainsi que sur les impacts de la désinformation. La deuxième partie de la rédaction se concentre sur les mesures mises en place par le gouvernement fédéral canadien pour lutter contre la désinformation. Nous examinons aussi les mesures mises en place par deux acteurs aux valeurs similaires, soit le Royaume-Uni et la Suède, ce qui nous sert à mettre en perspective l'approche du Canada. La troisième partie, à la lumière des sections précédentes, analyse la réponse du gouvernement canadien afin de répondre à notre question de recherche. Nous voyons que l'action gouvernementale du Canada peut s'expliquer par les défis que pose la désinformation, mais aussi par une sécuritisation de l'enjeu par les acteurs relevant du domaine de la sécurité au Canada. Pour conclure, des recommandations reflétant les pratiques conseillées dans la littérature sont offertes.

2. Revue de la littérature

2.1 Définitions et concepts

Il existe une absence de consensus notable au niveau des définitions et des concepts entourant la désinformation. Un bon point de départ est le lexique proposé par Caroline Jack (2017). Pour commencer, il y a le terme « information problématique », utilisé par certains auteurs (Molina et coll., 2021; Jack, 2017; Giglietto et coll., 2019; Frelon et Wells, 2020). Jack définit l'information problématique comme étant l'information qui est « inaccurate, misleading, inappropriately attributed, or altogether fabricated »[3] (Jack, 2017 : 3). Ce terme est utile puisqu'il permet de regrouper les différents types d'information qui sont, comme l'indique le terme, problématiques. Les théories de conspiration, la propagande, les rumeurs, la satire, etc. sont toutes considérées comme de l'information problématique.

Puis, comme l'explique Jack (2007 : 2), l'information problématique tombe généralement dans deux catégories : la mésinformation et la désinformation. On définit généralement comme Jack (2007 : 2-3) les deux concepts ainsi : « misinformation is information whose inaccuracy is unintentional [and] disinformation is information that is deliberately false or misleading»[4] . Comme on peut l'observer, ces deux termes réfèrent à de l'information trompeuse. Cependant, la distinction se trouve dans le fait que le terme mésinformation est utilisé quand on n'observe pas d'intention de tromper, tandis que la désinformation sous-entend une tromperie délibérée.

[3] Traduction libre : inexacte, trompeuse, attribuée de façon inappropriée ou entièrement fabriquée.
[4] Traduction libre : la mésinformation est une information dont l'inexactitude est involontaire et la désinformation est une information délibérément fausse ou trompeuse.

Bref, cette définition de la désinformation reste assez large qu'elle représente, selon nous, une sorte de dénominateur commun des différentes définitions de la désinformation que l'on peut retrouver. En effet, comme le souligne Jackson (2022 :548), malgré une prolifération récente d'études, la définition académique de la désinformation demeure ambiguë et controversée. Ainsi, il est possible d'observer des définitions de la désinformation qui incluent des éléments différents ou additionnels. Par exemple, certains auteurs ajoutent que la désinformation est faite dans l'optique de causer un préjudice public ou d'obtenir un gain monétaire (Commission européenne, 2021 : 10). De plus, d'autres vont dire que l'information de la désinformation doit nécessairement être fausse (Heer et coll., 2021 : 6) ou alors qu'elle doit nuire aux personnes, institutions et aux intérêts (Nielsen, 2021). Bref, nous croyons alors que notre définition est assez précise pour cibler le phénomène que nous cherchons à étudier, mais reste assez large pour ne pas rejeter les autres définitions existantes.

Fallis (2015) précise qu'il existe trois caractéristiques importantes à la définition de la désinformation : la désinformation est un type d'information, la désinformation est un type d'information trompeuse, et la désinformation est de l'information trompeuse qui est non accidentelle. En premier lieu, la désinformation est un type d'information. Il faut alors noter qu'il existe plusieurs définitions du terme « information », et qu'il est donc utile de définir ce qu'est l'information. Par exemple, si l'on utilisait la définition de l'information de Buckland (1991, cité dans Fallis, 2015 : 405) (« any object that "one might learn from,"

including “fossils, footprints, and screams of terror,” counts as information»[5]) la définition de la désinformation deviendrait trop large et perdrait sa valeur analytique. Fallis (2015) explique:

> Any kind of deceptive activity would count as disinformation. For instance, in addition to fake radio transmissions, the Allies built fake tanks and airplanes out of rubber and canvas in their attempt to convince the Germans that the D-Day invasion would take place at Calais. These objects would count as disinformation. As a result, we would really have no need for a special term for disinformation[6] (405).

Donc, quand on parle de désinformation, il est préférable de définir l’information ainsi : « Information refers to representational content that is false, as well as to representational content that is true »[7] (Fallis, 2015 : 406).

En deuxième lieu, la désinformation est de l’information qui est trompeuse, en d’autres mots, qui est « likely to create false beliefs »[8] (Fallis, 2015 : 406). Fallis apporte une précision à ce point en notant que la désinformation n’a pas nécessairement besoin de tromper pour être considérée comme telle. En effet, Fallis (2015) explique que, à l’image du mensonge, la désinformation n’est pas un « terme de réussite ». L’auteur explique que le mensonge reste un mensonge même si la personne que vous avez l’intention d’induire

[5] Traduction libre : tout objet dont « on pourrait tirer des leçons », y compris les fossiles, les empreintes de pas et les cris de terreur, est considéré comme de l’information.
[6] Traduction libre : Toute activité trompeuse serait considérée comme de la désinformation. Par exemple, en plus de fausses transmissions radio, les Alliés ont construit de faux chars et avions en caoutchouc et en toile pour tenter de convaincre les Allemands que l’invasion du jour J aurait lieu à Calais. Ces objets seraient considérés comme de la désinformation. Par conséquent, nous n’aurions vraiment pas besoin d’un terme spécial pour la désinformation.
[7] Traduction libre : L’information renvoie au contenu représentatif qui est faux, ainsi qu’au contenu représentatif qui est vrai.
[8] Traduction libre : susceptible de créer de fausses croyances.

en erreur ne croit pas ce que vous dites. De la même manière, la désinformation reste de la désinformation même si le public ciblé n'y adhère pas (Fallis, 2015: 406).

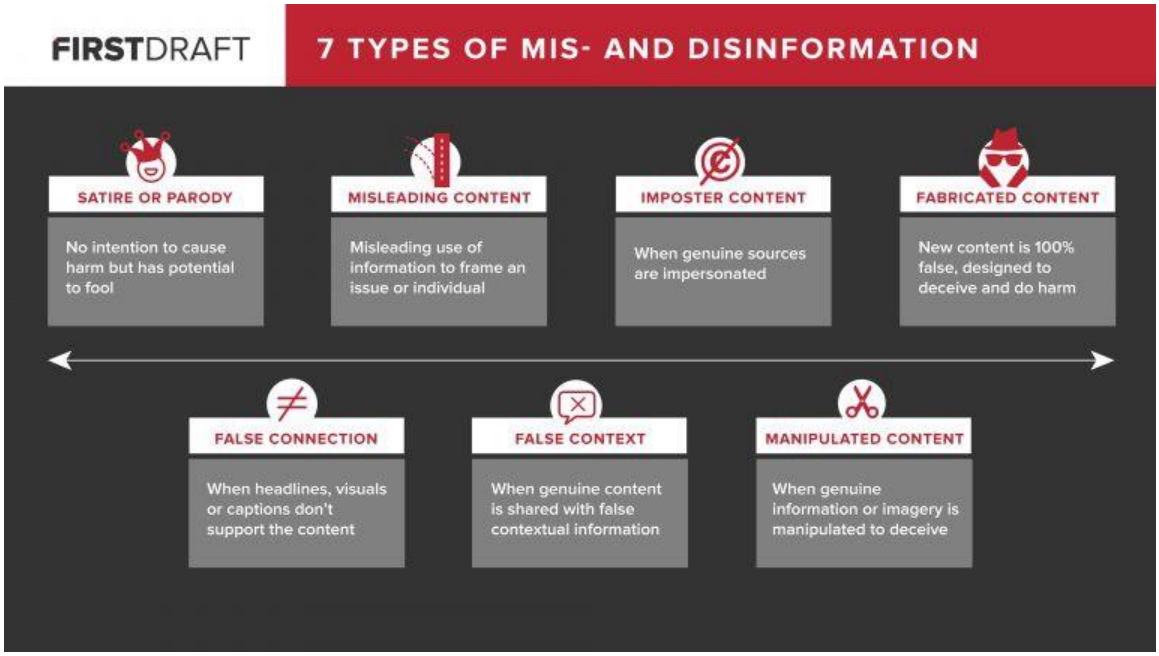
En troisième lieu, l'information trompeuse de la désinformation n'est pas accidentelle. C'est cette dernière caractéristique qui distingue la désinformation des formes plus inoffensives d'information trompeuse, comme la satire trop subtile (Fallis, 2015 : 406). D'ailleurs, la satire est un cas particulier. En effet, certains médias satiriques comme *The Onion* ou le *Beaverton* vont publier du contenu qui peut parfois être trompeur. Cependant, en général, leur but réel est plutôt d'amuser l'audience et/ou apporter une critique sociale à l'aide de l'humour. Leur contenu ne serait alors pas considéré comme de la désinformation. Il faut cependant noter que si du contenu provenant d'un journal satirique est repartagé par un parti tiers dans le but de tromper, ce même contenu devient alors de la désinformation.

Cela étant dit, plusieurs auteurs (Jack, 2017; Jackson, 2022; Giglietto et coll., 2019) soulignent qu'il est très difficile de prouver l'intention de tromper. Comme l'indique Jackson, « well-known difficulties in identifying "false information" and in determining whether it is deliberately or intentionally false (and to what purpose—e.g., to deceive, for economic or political gain, or to harm) continue »[9] (Jackson, 2022: 549). En raison de cette difficulté à distinguer le phénomène de la mésinformation de celui de la désinformation, il est parfois nécessaire de les étudier conjointement. Par exemple, nous croyons qu'il est possible de considérer les dangers de la mésinformation et ceux de la désinformation de la

[9] Traduction libre : les difficultés bien connues à identifier les « renseignements faux » et à déterminer s'ils sont délibérément ou intentionnellement faux (et à quelle fin — p. ex., pour tromper, pour un gain économique ou politique, ou pour nuire) se poursuivent.

même façon. En effet, si c'est l'intention de tromper qui distingue ces deux phénomènes, nous croyons qu'il peut être possible de tirer des conclusions sur la désinformation à l'aide des études sur la mésinformation. Par exemple, si une rumeur circule sur le fait que la prise d'un vaccin est dangereuse, que ce soit un acteur étranger ou simplement un proche mal informé qui est à l'origine de cette information problématique, le résultat est ultimement le même. Bref, ces deux phénomènes sont intimement liés, et c'est pourquoi certains auteurs vont regrouper les deux concepts au moment de les classifier. Par exemple, Wardle (2017) propose une classification de l'information problématique qui démontre sept types de mésinformation et désinformation (voir Graphique 1). On observe alors que Wardle ne sépare pas les deux phénomènes, mais les divise sous un spectre qui mesure plutôt le degré d'intention de tromper. Comme l'on peut le voir au Graphique 1, la satire et la parodie seraient le type d'information le moins trompeur tandis que le contenu fabriqué serait le type avec le plus d'intention de tromper.

Graphique 1: 7 Types de Més- et Désinformation



Source : Wardle (2017)

Finalement, il faut aussi noter qu'il existe d'autres termes utilisés pour décrire différentes formes d'information problématique et que certains auteurs utilisent ces termes (propagande, manipulation de l'information, etc.) de la même façon, ou similairement, à la façon dont nous utilisons le terme désinformation. Nous croyons qu'il est nécessaire d'apporter des précisions sur un de ces termes en particulier. En effet, plusieurs auteurs, y compris certains consultés dans notre recherche, utilisent plutôt le terme *fake news* au lieu du terme désinformation. Cela est sans doute dû au fait que cette expression a gagné en popularité dans les dernières années, notamment en raison de son utilisation par certains médias et politiciens. La popularité de ce terme, malgré le fait qu'il soit inadéquat pour capturer l'essence du phénomène, s'explique probablement par sa capacité à capter l'attention. De ce fait, nous croyons qu'il est mieux d'éviter d'utiliser *fake news* dans un contexte académique, car ce terme a évolué pour représenter toutes sortes d'information problématique, y compris la désinformation, en plus d'être utilisé de façon partisane pour nuire à la crédibilité des organisations de presse et des opinions opposées (Molina et coll., 202l :184). De plus, le terme *fake news* est inadéquat pour décrire le phénomène à l'étude, car il n'arrive pas à capter la complexité de la désinformation, qui implique du contenu qui n'est pas réellement, ou complètement faux, mais de l'information fabriquée mélangée avec des faits et des pratiques qui vont bien au-delà de tout ce qui ressemble à des nouvelles (Commission européenne. 2018, 12). Comme le soulignent Molina et coll. (2021), le terme *fake news* devrait normalement servir à désigner des « false stories that appear to be news, spread on the Internet or using other media, usually created to influence political views or

as a joke »[10] (184), et c'est donc ainsi que nous définissons le terme *fake news* dans ce mémoire.

2.2 Contexte historique

En considérant la définition de la désinformation que nous avons présentée plus tôt, on peut comprendre que la désinformation n'est pas un phénomène nouveau. En effet, plusieurs auteurs se servent de différents moments de l'histoire pour illustrer l'ancienneté du phénomène. Comme l'expliquent Le Bras et Bourdin (2018) :

> [D]éjà au VIe siècle avant notre ère, le général et stratège chinois Sun Tzu expliquait dans l'Art de la guerre toute l'importance de la tromperie et de la duperie dans la conduite d'un conflit. Il insistait notamment sur la nécessité de trouver un compromis entre vérité et mensonge, afin de rendre les fausses nouvelles les plus crédibles et efficaces possibles.

Jayakumar (2021), de son côté, utilise l'exemple du conflit entre Marc Antoine et Octavien après la mort de Jules César en 44 AC. Il explique:

> [What followed] was an unprecedented disinformation war in which the combatants deployed poetry and rhetoric to assert the righteousness of the respective campaigns. From the outset, Octavian proved the shrewder propagandist, using short, sharp slogans written upon coins in the style of archaic tweets. His theme was that Antony was a Roman soldier gone awry: a philanderer, a womaniser and a drunk not fit to lead, let alone hold office. (5)[11]

[10] Traduction libre : fausses histoires qui semblent être des nouvelles, diffusées sur Internet ou utilisant d'autres médias, généralement créées pour influencer les opinions politiques ou pour faire une blague

[11] Traduction libre : [Ce qui a suivi] était une guerre de désinformation sans précédent dans laquelle les combattants ont déployé la poésie et la rhétorique pour affirmer la droiture des campagnes respectives. Dès le début, Octave s'est montré le propagandiste le plus habile, utilisant des slogans courts et tranchants écrits sur des pièces de monnaie dans le style de tweets archaïques. Son thème était qu'Antoine était un soldat romain qui avait mal tourné : un coureur de jupons, un coureur de jupons et un ivrogne inapte à diriger, encore moins à occuper un poste.

Puis, plusieurs siècles plus tard, Posetti et Mattews (2018 : 1) expliquent que l'invention de l'imprimerie de Gutenberg en 1493 a considérablement amplifié la diffusion de la mésinformation et de la désinformation, comme l'illustre le premier canular médiatique à grande échelle – « The Great Moon Hoax »[12] de 1835.

Plusieurs décennies après, on peut retrouver une forme ou un autre de désinformation dans la plupart des évènements marquants : la Première Guerre mondiale (Neander et Martin, 2010, dans Posetti et Mattews, 2018) ainsi que la deuxième (Herztein, 1978, dans Posetti et Mattews, 2018), la guerre du Vietnam (Moise, 2017, dans Posetti et Mattews, 2018) ainsi que dans la guerre froide (Osgood. 2017, dans Posetti et Mattews, 2018), pour ne nommer que ceux-là.

Finalement, comme l'explique Ang et coll. (2021 : 5), cela nous apprend que « the lie, whether big or small, necessarily travelled at the speed that contemporary communications or technology would allow it to; its dissemination would likewise be circumscribed by these same realities. As the technology developed, so did the speed and reach of falsehoods » [13]. C'est ainsi que dans les dernières années, avec l'arrivée d'internet et de l'hyperconnectivité suscitée par les nouvelles technologies, l'enjeu de la désinformation a pris une ampleur sans précédent. Ce qui est nouveau, c'est la vitesse et la portée de la désinformation.

[12] Lors du *Great Moon Hoax of 1835* (littéralement "grand canular lunaire"), le *New York Sun* a publié six articles sur la découverte de vie extraterrestre sur la lune, prétendant raconter les découvertes de l'astronome Sir John Herschel.
[13] Traduction libre : le mensonge, grand ou petit, a nécessairement voyagé à la vitesse que la communication ou la technologie contemporaine lui permettrait; sa diffusion serait également circonscrite par ces mêmes réalités. Au fur et à mesure que la technologie évoluait, la vitesse et la portée des faussetés.

2.2.1 La désinformation à l'ère numérique

L'environnement informationnel d'aujourd'hui est beaucoup plus favorable à la désinformation qu'autrefois. D'abord, il faut noter l'immense impact des réseaux sociaux sur l'écosystème médiatique. Vilmer et coll. (2018 : 40) notent que les réseaux sociaux ont augmenté les risques de manipulation de l'information par : la surabondance d'information, qui affaiblit notre vigilance et notre capacité d'envisager des réfutations ; le nombre de vecteurs disponibles (et pouvant potentiellement diffuser de la fausseté) ; le faible coût de la diffusion et la facilité de copier l'apparence journalistique ; l'horizontalité des médias sociaux, qui permet la diffusion de contenue sans passer par des instances de contrôle éditorial ; et par le progrès technique d'éditions de contenus photo, vidéo ou audio. On remarque ainsi différents changements qui sont propices la désinformation, facilitant autant la création que le partage de l'information trompeuse.

Un autre élément important est la présence des algorithmes dans les plateformes numériques, qui sont programmées pour façonner la manière de présenter l'information aux usagers afin d'augmenter les clics et l'engagement avec le contenu (Heer et coll., 2021 : 21). D'abord, les internautes se retrouvent dans des « bulles filtrantes [qui sont] des espaces cognitifs clos où ne seraient portés à leur connaissance que des contenus qui les conforteraient dans leurs positions » (Vilmer et coll., 2018 : 41-42). Ces bulles filtrantes vont finalement présenter du contenu à l'image de l'utilisateur, créant ainsi des « espaces cognitifs confortables » (Vilmer et coll., 2018 : 42) qui vont confirmer leur propre façon de penser. Donc, on comprend que ces espaces ne privilégieront pas toujours l'information neutre, véridique et basée sur des faits.

Un deuxième élément présenté par Vilmer et coll. (2018) est un phénomène qu'ils qualifient « d'information en cascade » dans lequel « les utilisateurs relaient les informations postées par leurs proches sans nécessairement les vérifier ou même questionner leur validité. Plus l'information sera partagée, plus on tendra à lui faire confiance et moins on exercera son esprit critique » (Vilmer et coll., 2018 : 42). Messing et Westwoord (2021) ajoutent que: « users encountering news through social media appear to place as much weight on the social identity of the sharer as the reputation of the creator in determining informational credibility, further undermining the potentially moderating role of centrist journalistic media »[14] (cité dans Freelon et Wells, 2021 : 147).

Un troisième élément souligné par Vilmer et coll. (2018) est que, pour augmenter le temps sur les plateformes, l'information présentée est l'information qui est la plus susceptible de faire réagir. On favorise alors souvent les contenus les plus divertissants ou scandaleux. « Ce modèle participe ainsi à la polarisation de l'opinion en réduisant la visibilité des contenus nuancés, car jugés moins engageants. Ce modèle d'affaires est optimisé pour le profit plus que la vérité : il valorise les fausses nouvelles » (Vilmer et coll., 2018 : 42). Pour appuyer ce point, Soroush et coll. (2018) indiquent que « an MIT study published in 2018 concluded that on the social media platform Twitter, false stories get consistently much bigger reach than factually correct news » [15] (cité dans Sarts, 2021 : 25).

[14] Traduction libre : les utilisateurs qui rencontrent des nouvelles par l'entremise des médias sociaux semblent accorder autant de poids à l'identité sociale du participant qu'à la réputation du créateur dans la détermination de la crédibilité informationnelle, ce qui mine davantage le rôle potentiellement modérateur des médias journalistiques centristes.
[15] Traduction libre : une étude du MIT publiée en 2018 a conclu que sur la plateforme de médias sociaux Twitter, les fausses histoires ont toujours une portée beaucoup plus grande que les nouvelles factuelles.

Bref, ces éléments représentent de nouvelles dynamiques qui constituent l'environnement dans lequel se partage l'information aujourd'hui, à l'ère du numérique. Il faut finalement noter que ces nouvelles dynamiques ont un effet sur les médias traditionnels. Ayant vu leur situation se fragiliser dans les dernières années, plusieurs médias, pour s'adapter à ces changements, vont finalement imiter les approches des médias sociaux en optant pour un contenu sensationnaliste et émotionnel au détriment d'un contenu factuel et équilibré (Sarts, 2021 : 25). De ce fait, les médias traditionnels deviennent eux aussi vulnérables aux manipulations de l'information. De plus, cette porosité de la frontière entre les médias sociaux et les médias traditionnels crée, selon Tenove et coll. (2018), un « alternative media ecosystem that enables online misinformation to be amplified on television, on the radio, or in newspapers »[16] (17). Le rôle du journalisme traditionnel comme garde-fou de la vérité s'en retrouve affaibli.

Bien que les changements apportés par le numérique expliquent en quoi la désinformation se propage aussi rapidement, certains auteurs soulèvent des causes structurelles qui peuvent aussi expliquer la facilité de propagation de la désinformation. Comme le suggère Yaffa (2020), les divisions causées par la partisanerie, ainsi que les inégalités raciales et économiques, sont des terreaux fertiles à la désinformation. De plus, certains auteurs (Yaffa, 2020, Rapin, 2021, Vilmer et coll. 2018) soulignent que la crise de confiance envers les institutions est aussi un élément important à considérer. Comme le souligne Vilmer et coll. (2018), les fausses nouvelles traitent souvent de thèmes qui

[16] Traduction libre : écosystème médiatique alternatif qui permet d'amplifier la désinformation en ligne à la télévision, à la radio ou dans les journaux.

incarnent cette crise de confiance, avec des sujets comme « la trahison des élus, la confiscation de la parole par les médias [et] d'un certain nombre d'angoisses liées à la mondialisation » (37). Ainsi, on peut voir que la désinformation est « l'une des manifestations de cette crise de confiance, en même temps qu'elle l'entretient » (Vilmer et coll. 2018 : 37). Bref, la littérature examinant cette perspective structurelle reste assez mince, mais il peut être révélateur de prendre en considération ces éléments sociopolitiques, puisque cela se traduit par une compréhension plus complète des conditions qui permettent l'essor de la désinformation.

2.3 Les acteurs de la désinformation

2.3.1 Les acteurs non étatiques

Bien que des entités étatiques, notamment la Russie, aient beaucoup retenu l'attention sur cet enjeu, il faut noter que la désinformation n'est pas une activité limitée à l'État. Comme l'indique Vilmer et coll. (2018 : 43), « les techniques de manipulation de l'information sont aussi utilisées par des acteurs non étatiques agissant pour leur propre compte et pour promouvoir leur propre agenda ». Par exemple, ces derniers utilisent le cas de Daesh pour illustrer comment un groupe non étatique produit et utilise la désinformation. On explique que dans le cas de Daesh la désinformation est souvent utilisée dans le but de recruter des membres. Les auteurs expliquent que les cibles des campagnes de désinformation de Daesh

> font l'objet d'un ciblage méticuleux qui cherche avant tout à exploiter les vulnérabilités sociales, économiques, politiques et culturelles des sociétés visées. La multiplication des mèmes et vidéos terroristes le montre, les jeunes constituent la principale cible des thèses complotistes de l'État islamique, qui leur offre des réponses à des crises d'identité vécues localement, à l'heure

> d'entrer dans le monde du travail ou de se bâtir une identité d'adulte (Vilmer et coll., 2018 : 5).

On peut alors observer, par cette instance, qu'il existe des stratégies de désinformation relativement complexe même dans des groupes non étatiques. Finalement, bien que nous ayons utilisé l'exemple de Daesh, les groupes terroristes sont loin d'être les seuls à utiliser la désinformation. Dans la catégorie des acteurs non étatiques, on peut retrouver aussi les communautés ethniques et/ou religieuses et les mouvements nationalistes et/ou populistes qui ont joué un rôle dans le Brexit (Vilmer et coll., 2018 : 43) et l'élection de Donald Trump (Marwirk et Lewis, 2017 : 2).

2.3.2 Les acteurs étatiques

Les États sont aussi de grands producteurs de désinformation, qui peuvent viser la population intérieure ainsi que la population extérieure. Au niveau national, les tactiques de manipulation de l'information sont généralement utilisées dans le but de renforcer l'emprise du pouvoir. Vilmer et coll. (2018 : 48) démontrent en quoi plusieurs pays (Russie, Chine, Inde, Mexique, Argentine) utilisent différentes tactiques de désinformation pour manipuler l'opinion publique. Pour illustrer ce point, le cas de la Chine est sans doute le plus considérable. En effet, King et coll. (2017) démontrent comment le groupe nommé « 50c party », composé d'entre 500 000 et 2 000 000 membres, est à l'origine de la fabrication de plus de 480 millions de publications par année sur les réseaux sociaux. Les membres de ce groupe se font passer pour des citoyens ordinaires et créent une illusion d'appui généralisée en interagissant avec les différentes publications et contenus sur les réseaux sociaux.

Par ailleurs, la désinformation est aussi être dirigée vers des populations extérieures. Dans cette catégorie, la Russie et dans une moindre mesure la Chine sont les principaux producteurs de désinformation. En effet, comme l'explique un rapport du Service canadien du renseignement de sécurité (SCRS, 2018), « la Russie se distingue par sa stratégie de désinformation extrêmement élaborée visant à perturber les régimes politiques d'autres pays, à influencer les opinions politiques de ses citoyens ainsi qu'à semer et à attiser la division et la méfiance » (8). Par exemple, à travers l'Internet Research Agency (IRA), la Russie s'est livrée à de nombreuses activités de désinformation. La IRA est une organisation russe qui avait pour but, pendant la période des élections américaines de 2016, de « sow discord in the U.S. political system by posing as Americans and operating internet accounts that addressed divisive U.S. political issues »[17] (Cooley et Nexon, 2020 : 154). Cooley et Nexon indiquent que la IRA, qualifié d'« usine à trolls » opérait avec un budget mensuel de 1,25 million de dollars et générait du contenu sur les différentes plateformes de réseaux sociaux. Sur Twitter, 3 600 comptes liés à la IRA auraient envoyé plus de 9 millions de tweets en 2016 (Cooley et Nexon, 2020 : 154). Le contenu généré par l'IRA visait généralement à polariser la société américaine, en générant du contenu qui promouvait les deux côtés d'enjeux polarisant aux États-Unis, comme les vaccins, les questions raciales, l'avortement, les armes à feu, etc.

Pour sa part, la Chine utilise plutôt la désinformation à l'internationale dans une optique de « puissance douce »[18] dans le but de mettre en place un ordre du jour global

[17] Traduction libre : semer la discorde dans le système politique des États-Unis en se faisant passer pour des Américains et en exploitant des comptes Internet qui abordaient les questions politiques qui divisaient les États-Unis.
[18] Traduction libre de « soft power » : concept inventé par le politologue Joseph Nye qui est utilisée dans le cadre des relations internationales pour désigner la capacité d'un État à influencer et persuader sans utiliser la menace ou autre moyen coercitif.

enligné avec les intérêts chinois (CSIS, 2018 : 79). Cette désinformation dirigée vers l'extérieur est à l'image de celle qui est dirigée vers sa propre population. En revanche,

> la propagande chinoise, efficace pour modeler les opinions de la population chinoise au pays est beaucoup moins utile à l'étranger. Les opérations d'information de la Chine souffrent d'un manque de subtilité et d'attrait et sont minées par les relations sévères que Beijing entretient avec ses voisins et par sa répression intérieure. (SCRS, 2018 : 79).

Cela étant dit, la Chine reste toutefois un acteur important de la désinformation. Comme le mentionne Bandurski (2022), « [i]t has sown disinformation about COVID-19, about the efficacy of Western Vaccines, about the ongoing genocide in Xinjiang and much more »[19].

2.3 Pourquoi produit-on de la désinformation ?

Bien qu'il soit souvent difficile d'étudier les acteurs de la désinformation, en raison du fait que ces derniers cherchent à rester dans l'anonymat (Guess et Lyons, 2020 : 13), on relève trois grandes catégories de motif qui pousse généralement les différents acteurs, étatiques ou non étatiques, à faire de la désinformation.

La première catégorie représente les raisons économiques. Par exemple, un groupe de producteur de désinformation étant localisé en Macédoine, dans la ville de Veles, abritait plus d'une centaine de sites de nouvelles pro-Trump pendant la période menant aux élections américaines de 2016. On rapporte que les personnes responsables de la production

[19] Traduction libre : elle a semé de la désinformation au sujet de la COVID-19, de l'efficacité des vaccins occidentaux, du génocide en cours au Xinjiang et bien plus encore.

de ces articles de journaux étaient des adolescents motivés par des gains financiers plutôt que par une idéologie quelconque (Guess et Lyons, 2020 : 13). En effet, on rapporte que les adolescents qui produisaient ces histoires pouvaient générer des revenus allant jusqu'à 8 000 $ par mois, un montant 20 fois plus élevé que le salaire typique à Veles à cette époque (Guess et Lyons, 2020 : 13).

Puis, en second lieu, on peut aussi observer des acteurs qui produisent de la désinformation pour des raisons politiques. Le cas de l'IRA, mentionné précédemment, peut être utilisé en exemple pour ce point. Bien que les conséquences des tactiques de l'IRA soient incertaines, il reste que la motivation d'utiliser ces tactiques était faite dans l'objectif, selon Cooley et Nexon (2020), de « further destabilizing the willingness and the ability of the United States to promote liberal architecture and sustain its hegemonic infrastructure »[20] (157).

Finalement, des motifs idéologiques pousseraient aussi les acteurs à faire de la désinformation. Les « réseaux collaboratifs anonymes » comme 4chan et 8chan représentent bien les motifs idéologiques (Guess et Lyons, 2020 : 16). Ces groupes se servent des plateformes participatives pour produire et partager de la désinformation, souvent pour propager des idées d'extrême droite. Ces groupes ne sont pas organisés centralement, mais se retrouvent sur le web pour se coordonner et créer/partager de la désinformation. Ce sont d'ailleurs ces types de groupe qui seraient à la base de l'insurrection du capitole américain le 6 janvier 2021. Comme l'indiquent Heilweil et

[20] Traduction libre : déstabilisant encore davantage la volonté et la capacité des États-Unis de promouvoir l'architecture libérale et de soutenir son infrastructure hégémonique

Ghaffary (2021), « The groups that stormed Capitol Hill […] have long been active on platforms like Gab and 4chan, and more recently, they've adopted newer tools like the lightly moderated social media site Parler and the anonymous messaging service Telegram to organize[21] ». Enfin, il faut aussi noter que certains membres de ces groupes n'adhèrent pas tous à une idéologie d'extrême droite, et qu'une partie de ces participants sont simplement motivés par « the enjoyment they get at the expense of others »[22] (Marwick et Lewis, 2017, cités dans Guess et Lyons, 2020 : 16).

2.4 Techniques et technologies de dissémination

Comme nous l'avons mentionné précédemment, la technologie et les médias sociaux ont permis de créer un environnement favorable à la propagation de la désinformation. De ce fait, on peut constater que les techniques de propagation d'aujourd'hui sont surtout axées sur le numérique.

D'abord, les acteurs cherchant à propager la désinformation vont utiliser un vaste éventail de plateformes pour y arriver : sites internet, forums de chat et revues en ligne, réseaux sociaux, blogues, messageries instantanées, sites de partage vidéo, etc. (Vilmer et coll., 2018 : 43). En plus d'utiliser en partie ou en totalité ces plateformes pour disséminer de la désinformation, les acteurs contribuant à cet enjeu ont recours à différentes stratégies et technologies. Autre que le partage normal de l'information trompeuse entre usagers, les

[21] Traduction libre : Les groupes qui ont pris d'assaut Capitol Hill […] ont longtemps été actifs sur des plateformes comme Gab et 4chan, et plus récemment, ils ont adopté de nouveaux outils comme le site de médias sociaux légèrement modéré Parler et le service de messagerie anonyme Telegram pour s'organiser.
[22] Traduction libre : la jouissance qu'ils obtiennent aux dépens des autres.

principales techniques numériques utilisées pour propager la désinformation sont les « bots » et les « sock puppets » (Tenove et coll., 2018 : 22).

En bref, les « bots » sont des « automated online agents that mimic human behaviour »[23] (Dubois et McKelvey, 2019, cités dans Heer et coll., 2021 : 12). Guess et Lyons (2020 : 21) expliquent que les bots travaillent pour disséminer la désinformation avec une stratégie spécifique :

> First, they amplify false content in the early stages of dissemination, prior to achieving organic spread. Second, bots single out influential accounts, trying to leverage their influence by gaining their attention through replies and mentions. [As a result] people retweet bots just as much as other humans, suggesting the strategies are at least in part effective.[24]

D'ailleurs, il est possible d'observer le volume considérable de l'activité des bots. Par exemple, Wardle (2017 : 37) indique que deux comptes Twitter sur trois publiant des messages sur la présence de l'OTAN dans les pays baltes et la Pologne étaient des bots (37). D'autre part, durant le dernier mois de l'élection présidentielle de 2016, Bessi et Ferera (2016), dans leur étude, ont identifié 400 000 bots responsables d'avoir publié 3.8 millions de tweets, ce qui représentait 20 % de l'échantillon collecté dans le cadre de leur recherche (Bessi et Ferrara. 2016, cité dans Tucker et coll., 2018 : 38).

[23] Traduction libre : des agents en ligne automatisés qui imitent le comportement humain.
[24] Traduction libre : Tout d'abord, ils amplifient le faux contenu dans les premiers stades de la diffusion, avant d'atteindre la propagation organique. Deuxièmement, les bots ciblent les comptes influents, en essayant de tirer parti de leur influence en attirant leur attention au moyen de réponses et de mentions. [En conséquence] les gens retweetent des bots tout autant que d'autres humains, suggérant que les stratégies sont au moins en partie efficaces.

Puis, l'utilisation de « sockpuppets » est une autre technique utilisée pour propager la désinformation : les sockpuppets (« faux-nez » en français) sont des « human-operated fake accounts (…) which enable actors to hide or misrepresent their identities »[25] (Morgan et Shaffer, 2017, cité dans Tenove et coll., 2018 : 18). Ces comptes peuvent être utilisés pour rendre un message plus crédible notamment en se faisant passer pour une source légitime ou bien en promouvant des idées qu'un acteur faussement incarné ne partage pas réellement. Par exemple, durant la période électorale américaine de 2016, un compte nommé « *United Muslims of America* » attaquait les politiciens américains et partageait de l'information trompeuse sur la politique étrangère américaine. Or ce compte, contrairement à ce que sous-entend son nom, était contrôlé par des utilisateurs russes (Collins, Poulsen et Ackerman, 2017, cités dans Tenove et coll., 2018 : 18).

Une autre technique de désinformation utilisée est le « trolling ». Dans son sens plus large, le trolling fait référence à des « civil, threatening and disruptive behaviours online »[26] (Tenove et coll., 2018 : 22). Cependant, comme action politique, le trolling est plutôt défini ainsi :

> [A] specific kind of political activity that is marked by a refusal to participate in the kind of productive exchange of ideas that marks democratic politics. Instead of engaging in activity marked by democratic principles of reciprocity, accommodation, and inclusion, trolls actively work to dominate and control the conversations on any given site[27] (Forestal, 2017, cité dans Tenove et coll., 2018 : 23).

[25] Traduction libre : faux comptes exploités par des humains (…) qui permettent aux acteurs de cacher ou de présenter sous un faux jour leur identité.
[26] Traduction libre : comportements civils, menaçants et perturbateurs en ligne.
[27] Traduction libre : [Un] type spécifique d'activité politique qui est marqué par un refus de participer au genre d'échange productif d'idées qui marque la politique démocratique. Au lieu de s'engager dans une activité marquée par des principes démocratiques de réciprocité, d'accommodement et d'inclusion, les trolls travaillent activement à dominer et à contrôler les conversations sur un site donné.

Il faut noter qu'il existe plusieurs formes de trolling. Par exemple, certaines formes mises sur l'intimidation et les menaces, en harcelant des opposants politiques ou des journalistes (Tenove et coll., 2018 : 23). Cependant, quand nous nous concentrons sur la désinformation, le trolling prend d'autres apparences. Ainsi, pendant les élections américaines de 2016, le processus de vote lui-même a été perturbé par des trolls qui ont ciblé les électeurs potentiels du Parti démocrate avec des informations erronées sur le lieu et la façon de voter (Eordogh, 2016, dans Tenove et coll., 2018 : 22). Le trolling peut aussi prendre d'autres formes plus subtiles afin de créer l'illusion que « significant parts of society share a specific point of view and actively exploits human popularity bias, by making people believe something is true because many other people think it is true »[28] (Sarts, 2021: 28). Le cas de la Chine et du « 50c party » mentionné ci-dessus est un bon exemple pour illustrer cette technique.

La création de fausses nouvelles est probablement la technique de désinformation ayant attiré le plus l'attention. Cette technique consiste à créer des sites ou des nouvelles ayant l'allure de vraies sources journalistiques pour propager de l'information trompeuse. Cependant, certains auteurs remettent en question l'efficacité de ce type de contenue, puisqu'ils sont généralement faciles à vérifier (Rojecki et Meraz, 2016, cité dans Tenove et coll., 2018 : 26). Par contre, Guess et Lyons (2020, 21) indiquent que certains types de fausses nouvelles, notamment les sites de « dernière heure»[29], semblent plus efficaces que les autres pour propager la désinformation. Ils indiquent que les utilisateurs de Twitter

[28] Traduction libre : d'importantes parties de la société partagent un point de vue précis et exploitent activement le biais de popularité humaine, en faisant croire que quelque chose est vrai parce que beaucoup d'autres personnes pensent que c'est vrai.
[29] Traduction libre de : breaking news sites

semblent faire confiance à ces comptes qui imitent les sources d'information légitimes ce qui leur donne un air d'autorité et permet à ces sites de construire de grandes bases crédules (Guess et Lyons, 2020 : 21). Andrews et coll. (2016) confirment que ces « "breaking news" accounts are highly retweeted [and] recent research shows that these accounts might actually be more trusted than mainstream media sources »[30] (11).

Puis, l'utilisation du « big data », une expression qui réfère à l'explosion de la quantité des données numériques et, surtout pour le cas qui nous intéresse, aux données personnelles des individus, est aussi utilisée pour propager de la désinformation. De manière similaire aux campagnes de marketing qui se fient sur ces données pour vendre des produits aux consommateurs, les acteurs cherchant à faire de la désinformation commencent à s'en servir pour tenter d'affecter les attitudes politiques (Sarts, 2021 : 29). Ces données peuvent être accédées, de façon légitime ou non, et utilisées pour créer des messages microciblés. Comme outil de désinformation, ces messages, en étant adaptés à une audience précise, augmentent l'efficacité de la manipulation de l'information. En effet, en ayant accès à ces informations, il est plus facile de cibler « particular groups in the society that are disillusioned or have adversarial perspectives or specific beliefs and target them with itemized messages for predesigned outcomes »[31] (Sarts, 2021 : 29). Cette tactique, relativement nouvelle, a été observée durant les élections américaines de 2016. Des acteurs russes auraient acheté plus de 3 000 publicités microciblées sur Facebook dans

[30] Traduction libre : ces comptes « dernière heure » sont fortement retweetés [et] des recherches récentes montrent que ces comptes pourraient en fait être plus dignes de confiance que les sources de médias grand public.
[31] Traduction libre : des groupes particuliers de la société qui sont désillusionnés ou qui ont des points de vue antagonistes ou des croyances particulières et qui les ciblent avec des messages détaillés pour des résultats pré désignés.

le but d'influencer les électeurs américains (Isaac et Shane, 2017; Stamos, 2017; cités dans Tenove et coll., 2018 : 22).

Il existe aussi d'autres techniques de dissémination, mais qui sont plus rarement étudiées. Par exemple, il semble que les « memes », ces « visual trope that proliferates across internet spaces as it is replicated and altered by anonymous users »[32] (Lyons 2017, cité dans Tenove et coll., 2018 : 22), soient aussi utilisés pour propager l'information problématique. Ces images, souvent de nature humoristique, font partie du paysage culturel d'internet et des médias sociaux depuis maintenant plusieurs années. Les « memes » semblent être efficace pour propager la désinformation. D'abord parce qu'ils peuvent être consommés et partagés rapidement, mais aussi parce qu'ils sont considérés comme insignifiants et inaptes à la discussion et, par conséquent, font rarement face à des corrections (Lyons, 2017, cité dans Tenove et coll., 2018 : 22). Puis, des développements technologiques récents sur les intelligences artificielles, les « *machine learning* »[33] et les « *deepfakes* » amènent les experts à prédire que ces outils seront de plus en plus utilisés pour propager de la désinformation (Swedish Civil Contigencies Agency, 2019 : 23). Par exemple, il est maintenant possible, à l'aide des *deepfakes*, de superposer le visage d'une autre personne sur des séquences vidéo préexistantes et reconstruire numériquement la voix d'une personne (Swedish Civil Contigencies Agency, 2019 : 23), ce qui offre des possibilités infinies pour les acteurs malicieux.

[32] Traduction libre : tropes visuels qui se prolifèrent dans les espaces Internet en étant répliqué et modifié par des utilisateurs anonymes.
[33] Traduction libre : apprentissage automatique.

Pour conclure, il faut noter que ces différentes techniques de dissémination de l'information trompeuse ne sont pas nécessairement indépendantes les unes des autres et peuvent parfois (voir souvent) être utilisées conjointement. De ce fait, un acteur pourrait créer une fausse nouvelle, la nouvelle pourrait ensuite être publiée sous le compte d'un sockpuppet, pour finalement être amplifiée à l'aide de bots, trolls, etc. dans le but d'étendre le plus possible la portée de la désinformation.

2.5 Les impacts

Les impacts de la désinformation sont, par sa nature, difficiles à observer. D'une part, il est difficile de discerner le côté délibéré que sous-entend la désinformation. De l'autre, les acteurs qui la pratiquent ont généralement intérêt à rester dans l'anonymat et à cacher leurs méthodes. Certains auteurs, comme Jackson (2022), tentent de nuancer les effets et les impacts de la désinformation. Jackson (2022) souligne, en faisant référence aux élections canadiennes de 2019, qu'il n'y avait aucune preuve d'impact des campagnes de désinformation sur les élections (11). Cette vision des impacts de la désinformation est partagée par Alexander Lanoszka (2019), qui observe « almost no meaningful empirical evidence on outcomes such as beliefs, attitudes, and behaviour »[34] (cité dans Guess et Lyons, 2020 : 24). Il en va de même pour Aral et Eckles (2019), qui indiquent que « the effects of misinformation on candidate preferences themselves and, moreover, the effects on electoral outcomes or other behaviours have yet to be reliably detected »[35] (cité dans Guess et Lyons, 2020: 24). On observe alors que les impacts de la désinformation au

[34] Traduction libre : presque aucune preuve empirique valable sur les résultats comme les croyances, les attitudes et les comportements

[35] Traduction libre : les effets de la désinformation sur les préférences des candidats eux-mêmes et, en outre, les effets sur les résultats électoraux ou d'autres comportements n'ont pas encore été détectés de façon fiable.

niveau politique sont potentiellement moins importants que l'on pourrait penser. Bien que certains auteurs réduisent le risque que la désinformation pose réellement, ces derniers reconnaissent généralement que le manque de preuve sur ces impacts peut être lié à la difficulté de mesurer le phénomène.

Cependant, nous croyons que cette diminution des risques par certains auteurs s'explique par le fait que l'on réduit l'impact de la désinformation à son influence sur les processus électoraux. Or, la désinformation peut avoir des impacts autres que sur les élections. D'abord, on peut observer des impacts au niveau des délibérations publiques. Comme l'indiquent Tenove et coll. (2018), la désinformation « undermine the epistemic quality of public deliberation. This not only leads to weak understanding of public issues and disagreement on facts but can also lead to belief in dangerous conspiracy theories (e.g., #pizzagate, voter fraud) »[36] (28). Puis, en plus d'avoir un impact sur la qualité du débat, la désinformation peut aussi avoir un impact sur ce qui fait l'objet du débat. Guess et Lyons (2020 : 24) indiquent qu'il a été observé que des sites de fausses nouvelles ont contribué à la mise à l'ordre du jour de certains enjeux, ce qui est un impact non négligeable puisque le pouvoir de la mise à l'ordre du jour influence quel enjeu capte l'attention du public. Par ailleurs, il existe des situations où l'on a pu observer des impacts au niveau de la participation démocratique. Eordogh (2016) indique que des électeurs se sont fait convaincre qu'il était possible de voter par message texte par des groupes de trolls « alt-

[36] Traduction libre : sape la qualité épistémique de la délibération publique. Cela mène non seulement à une mauvaise compréhension des enjeux publics et des désaccords sur les faits, mais aussi à la croyance en de dangereuses théories du complot (p. ex., #pizzagate, fraude électorale).

right » sur internet. En raison du partage de cette information par ces groupes de droites, des électeurs ont perdu l'occasion d'exercer leur droit de vote.

De plus, bien que la plupart des travaux se concentrent sur les impacts de la désinformation sur la démocratie, d'autres types d'impact sont relevés. Des recherches indiquent que l'information trompeuse « may do most of its damage in increasing cynicism and apathy while feeding extremism and affective polarization »[37] (Garrett et coll., 2014; Lau et coll., 2017; Tsfati et Nir, 2017; Lazer et coll., 2018; Suhay et coll., 2018; cités dans Guess et Lyons, 2020 : 25). D'autre part, Heer et coll. (2021 :15) indiquent que la désinformation peut aussi entraîner de la discrimination, de la stigmatisation et de la marginalisation dans certains contextes. Pour illustrer ce point, Harb et Henne (2019 : 200-201) démontrent comment la désinformation a été utilisée pour légitimer des activités de surveillance de la Gendarmerie royale du Canada (GRC) visant des manifestants autochtones anti-pipeline.

En outre, certains éléments de la désinformation n'ont tout simplement pas fait l'objet de recherche quant à leurs impacts. Par exemple, la stratégie de désinformation russe qualifiée de « firehose of falsehood » [38] (Guess et Lyons, 2020 : 25) reste très peu étudiée. Comme l'expliquent ces auteurs, cette stratégie, qui consiste à envoyer rapidement de nombreux messages à travers de nombreux canaux, vise présumément à générer de la confusion et à accabler ses cibles. De ce fait, les effets cumulatifs de cette stratégie, sans

[37] Traduction libre : peut causer la plupart de ses dommages en augmentant le cynisme et l'apathie tout en alimentant l'extrémisme et la polarisation affective.
[38] Traduction libre : tuyau d'incendie du mensonge.

compter la fatigue mentale qu'elle peut causer, sont difficiles, mais importants à mesurer (Guess et Lyons, 2020: 25).

Au final, on remarque qu'il faut encore plus de recherche pour évaluer avec précision l'ampleur et les impacts de la désinformation. On peut toutefois observer que les impacts les plus importants de la désinformation ne correspondent pas aux préconceptions des conséquences de cet enjeu. En effet, le nouvel intérêt porté sur la désinformation s'explique surtout sur la perception de son influence sur le processus électoral. Or, il a été observer que les impacts réels peuvent être beaucoup plus subtils. Il sera d'ailleurs possible d'observer cette conception erronée des impacts dans les mesures mises en place par le Canada, avec l'emphase particulière qui est portée sur la protection du système électoral.

3. Les mesures du Canada pour répondre à la désinformation

L'action publique du Canada face à la désinformation s'est considérablement accélérée au courant des dernières années. Comme il a été mentionné précédemment, la présence de désinformation émanant de la Russie dans les élections américaines de 2016, sans oublier les instances de désinformation observées durant le référendum sur le *Brexit* au Royaume-Uni, ont incité le Canada à établir différentes mesures pour contrer la désinformation en marge des élections canadiennes (Vilmer, 2021 : 15). D'ailleurs, un bon nombre de mesures mises en place par le Canada pour répondre à la désinformation se concentrent spécifiquement sur la protection du système électoral canadien. Il est aussi possible d'observer, comme le souligne Jackson (2022 :561), que les mesures mises en place ne visent pas seulement la désinformation, mais s'attaquent aux catégories plus larges de

mésinformation, d'ingérence étrangère hybride et de cybermenaces. Cela s'explique, entre autres, par l'absence apparente d'une stratégie cohérente pour répondre à la désinformation au Canada (Jackson, 2022 : 562). Cette section du mémoire trace d'abord un portrait de ces mesures, du point de vue national et international, pour ensuite analyser les stratégies du Royaume-Uni et de la Suède afin de les comparer à la situation canadienne.

3.1 Les mesures nationales

Les mesures mises en place dans un contexte national peuvent être divisées en trois grandes catégories : les mesures législatives, les actions institutionnelles et les mesures pour accroitre la résilience.

3.1.1 Les mesures législatives

Il n'y a aucune loi qui empêche de propager de la désinformation au Canada. La seule exception étant pour les propos couverts par les lois relatives à la diffamation (Levush, 2019 : 35). Cela n'a pas toujours été le cas. En effet, la section 181 du Code criminel canadien empêchait le partage de fausses nouvelles jusqu'à ce que cette disposition soit jugée inconstitutionnelle par la Cour suprême dans *R v Zundel* (1992) pour avoir enfreint l'article 2(b) de la *Charte canadienne des droits et de la liberté* en raison de son atteinte à la liberté d'expression (Levush, 2019 : 35). Il en va de même pour l'article 91 de *la Loi électorale du Canada*, qui a été rendu ineffectif pour les mêmes raisons en 2021 par un juge de la Cour supérieure de l'Ontario (Gobeil, 2021). On peut ainsi observer la difficulté de légiférer sur la désinformation, en raison du clivage qui existe entre le contrôle de

l'information et les principes de liberté d'expression qui sont fortement protégés dans les démocraties occidentales.

Au-delà des fausses nouvelles, la *Loi concernant des questions de sécurité nationale* (adoptée en 2018) permet au Canada de se défendre des cybermenaces. En bref, cette loi donne au Centre de la sécurité de la télécommunication (CST) le pouvoir de mener des

> "active cyber operations" to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to Canada's defence, security or international affairs […] the threat of possible Canadian counterattacks (including against the digital information environment) is meant to deter attacks, but it is argued that Canada could also "proactively shut down the source of a possible attack against Canada"[39] (Jackson, 2022 : 558).

Il faut noter que la loi ne mentionne pas spécifiquement les tactiques de désinformation venant de l'étranger. Cependant, puisque le gouvernement canadien a tendance à considérer la désinformation comme un type d'ingérence étrangère (Jackson, 2022 : 547), il est vraisemblable que le gouvernement invoque cette loi pour répondre à la désinformation, possiblement en mettant en place des réponses offensives ayant pour but de dissuader les acteurs propageant la désinformation.

Une autre mesure législative mise en place par le Canada est la *Loi sur la modernisation des élections* (entrée en vigueur en juin 2019). Cette loi apporte trois

[39] Traduction libre : « cyberopérations actives » visant à « dégrader, perturber, influencer, intervenir ou entraver les capacités, les intentions ou les activités d'une personne, d'un État, d'une organisation ou d'un groupe terroriste étranger en ce qui a trait à la défense du Canada, la sécurité ou les affaires internationales […] la menace d'éventuelles contre-attaques canadiennes (y compris contre l'environnement de l'information numérique) vise à dissuader les attaques, mais on soutient que le Canada pourrait aussi « arrêter de façon proactive la source d'une éventuelle attaque contre le Canada.

éléments explicites à la lutte contre la désinformation. D'abord, la loi émet des exigences en matière de divulgation pour la publicité politique payée pendant les périodes préélectorales et électorales, ce qui comprend la création de registres numériques de messages publicitaires pour les plateformes en ligne (Dawood, 2021 : 19). Cela comprend aussi l'interdiction d'utiliser des fonds étrangers pour des publicités ou des activités partisanes. De plus, la loi

> creates an offense of distributing or publishing any material during an election period that purports to be from a candidate, political party, or the chief electoral officer where the material was published with the intent of misleading the public into believing that it was authorized [40] (Dawood, 2021: 20).

En d'autres mots, la loi interdit d'usurper l'identité d'un acteur politique pour partager du matériel trompeur. Elle fait d'ailleurs une exception dans les cas où le matériel est distribué aux fins de parodie ou de satire.

Il existe d'autres recours législatifs qui pourraient être utilisés pour répondre à la désinformation, mais qui ne le sont pas puisqu'ils ne sont pas adaptés aux nouvelles dynamiques du monde numérique. Par exemple, l'article 372 (1) du Code criminel indique : « commet une infraction quiconque, avec l'intention de nuire à quelqu'un ou de l'alarmer, transmet ou fait en sorte que soient transmis par lettre ou tout moyen de télécommunication des renseignements qu'il sait être faux ». De plus, Tenove et Tworek (2019 : 224) expliquent que différentes entités gouvernementales au niveau provincial et

[40] Traduction libre : crée une infraction en distribuant ou en publiant, au cours d'une période électorale, des documents qui sont censés provenir d'un candidat, d'un parti politique ou du directeur général des élections lorsque ces documents ont été publiés dans l'intention d'induire le public en erreur en lui faisant croire qu'ils étaient autorisés.

fédéral détiennent des moyens qui pourraient être utilisés pour répondre à différentes formes de désinformation. Les auteurs utilisent l'exemple de la *Loi canadienne antipourriel* qui peut être utilisé pour contrer la distribution de masse des courriels, des textos, et autres messages. Les auteurs soutiennent que cette loi aurait le potentiel d'être élargie pour répondre au problème des bots. En revanche, bien que ces dispositions existent et puissent en théorie servir à répondre à la désinformation, Tenove et Tworek (2019 : 225) notent qu'elles sont inadaptées pour répondre à la désinformation en ligne, notamment parce qu'elles sont couteuses et difficiles à appliquer (surtout si le responsable se trouve en dehors du Canada). De plus, Tenove et Tworek (2019 : 225) expliquent que, en général, ces instruments législatifs sont ciblés et ont des seuils d'action élevés. Ils sont donc surtout adaptés pour des sanctions légales individuelles, et ne consistent donc pas des outils appropriés pour ce phénomène répandu.

En bref, on remarque donc qu'il y a peu d'instruments législatifs mis en place pour lutter contre la désinformation ; une absence qui est d'une part liée aux exigences de la liberté d'expression, mais aussi parce que les dispositions actuelles ne sont pas adaptées au monde numérique.

3.1.2 Les mesures institutionnelles

Plusieurs ministères et agences jouent un rôle lié à la désinformation au Canada, chacun agissant sur une ou plusieurs facettes du phénomène : Affaires mondiales Canada (AMC) coordonne les réponses à la désinformation avec ses partenaires internationaux ; Patrimoine Canada met en place des programmes visant l'accroissement de la résilience à la

désinformation ; Élection Canada joue un rôle considérable sur la protection du processus électoral; Santé Canada est particulièrement actif dans ses efforts pour lutter contre la désinformation liée à la COVID ; et, finalement, les agences de renseignement (Centre de la sécurité et des télécommunications [CST] et Service canadien du renseignement de sécurité [SCRS]) qui surveillent et collectent les activités de désinformation extérieure (Vilmer, 2021 : 18). Ces acteurs institutionnels ont, individuellement ou en concert, mis en place diverses initiatives pour répondre à la désinformation. Les mesures les plus importantes au niveau institutionnel sont les suivantes.

D'abord, le Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections (SITE[41]) est un groupe regroupant le CST, le SCRS, AMC et la GRC. Le groupe vise à agir sur les « activités secrètes, clandestines ou criminelles qui entravent ou influencent les processus électoraux au Canada » (Gouvernement du Canada, 2021a). Pour y arriver, les activités du groupe de travail cherchent à « building awareness of foreign threats to Canada's electoral process [and] preparing the Government to assess and respond to those threats »[42] (Levush, 2019: 40). Peu d'information est accessible sur les activités du SITE spécifique à la désinformation, ce qui peut être expliqué par la confidentialité parfois requise par les agences de sécurité afin de ne pas miner leurs activités. Cependant, une des activités mentionnées consiste à « effectuer des recherches sur les campagnes de désinformation ciblant le Canada et menées par des acteurs étrangers » (Gouvernement du Canada, 2021a). Enfin, le Groupe

[41] Mieux connu sous l'appellation anglophone « SITE » Task Force (Security and Intelligence Threats to Elections).
[42] Traduction libre : accroître la sensibilisation aux menaces étrangères qui pèsent sur le processus électoral du Canada [et] préparer le gouvernement à évaluer ces menaces et à y réagir

de travail est en coordination et échange d'information avec le Mécanisme de réponse rapide du G7[43] (Jackson. 2022, 14), une collaboration qui est explorée plus en détail dans les mesures à l'internationale.

Le gouvernement canadien a aussi mis en place le *Protocole public en cas d'incident électoral majeur* qui a pour but de déterminer si la capacité du Canada à mener des élections démocratiquement a été compromise. En effet, dans le cadre du *Protocole*, cinq hauts fonctionnaires devaient être informés de toute interférence potentielle durant les élections fédérales de 2019, et de déterminer si ces incidents étaient assez sérieux pour informer les Canadiens (Jackson, 2022: 557). Jackson (2022 : 558) souligne qu'aucun incident n'a été considéré comme étant assez sérieux pour être reporté.

Par ailleurs, le Canada a mis en place la *Charte numérique du Canada*. En bref, la *Charte* constitue un point d'ancrage qui doit orienter la modernisation de la règlementation numérique au pays. Un des dix principes de la charte déclare que « le gouvernement du Canada défendra la liberté d'expression et assurera une protection contre les menaces en ligne et la désinformation visant à miner l'intégrité des élections et des institutions démocratiques » (Gouvernement du Canada, 2021b). Le but de la *Charte numérique* est de moderniser le cadre de règlementation du numérique, tout en regagnant la confiance des citoyens en l'environnement numérique (Dawood, 2021: 23). Bien que la *Charte* soit non contraignante, elle illustre un désir d'action de la part du gouvernement.

[43] Annoncé lors du Sommet du G7 à Charlevoix en juin 2018, le Mécanisme de réponse rapide (MRR) est une initiative visant à renforcer la coordination à l'échelle du G7 pour déceler, prévenir et contrer les menaces qui pèsent sur les démocraties des pays membres.

La *Déclaration du Canada sur l'intégrité électorale en ligne* est une autre initiative non contraignante mise en place par le gouvernement. La déclaration s'adresse aux réseaux sociaux et aux plateformes en ligne qui peuvent être utilisés pour « répandre de la désinformation dans le but de faire obstacle aux élections libres et justes, d'affaiblir les grandes institutions démocratiques et d'exacerber les tensions sociétales existantes » (Gouvernement du Canada, 2021c). La *Déclaration* représente un engagement à « travailler ensemble pour assurer le respect des principes d'intégrité, de transparence et d'authenticité nécessaires à des débats et à une expression démocratique en ligne » (Gouvernement du Canada, 2021c). On peut lire dans le document que les plateformes s'engagent à « intensifier leurs efforts de lutte contre la désinformation, qui constitue une menace pour les processus et les institutions démocratiques du Canada » (Gouvernement du Canada, 2021c). Facebook, Google, LinkedIn, Microsoft, TikTok, Twitter et YouTube font partie des entreprises appuyant la déclaration. On observe à l'aide de cette déclaration que le gouvernement fédéral canadien opte pour l'autorégulation des plateformes numériques plutôt que d'agir sur ces dernières par voie règlementaire.

3.1.3 Les mesures pour accroitre la résilience

Une partie des mesures mises en place par le gouvernement canadien vise à l'accroissement de la résilience. Selon Humprecht (2020), la résilience dans un contexte de désinformation réfère à un :

> structural context in which disinformation does not reach a large number of citizens. At the same time, [people who are exposed to disinformation] will be less inclined to support or further distribute

> such low-quality information, and in some cases, they will be more able to counter that information[44] (408).

Donc, dans le cadre de cette analyse, les mesures pour accroitre la résilience sont les mesures de sensibilisation, d'éducation et de formation à la désinformation. Cela s'applique aussi aux mesures structurelles qui limitent la propagation de l'information trompeuse. Par exemple, selon Boulianne et coll. (2021 : 6), le Canada est un pays ayant déjà une grande résilience qui s'explique par sa règlementation des médias et son système de diffusion financé par des fonds publics.

Pour accroitre davantage sa résilience face à la désinformation, le Canada a lancé en 2019 *l'Initiative de citoyenneté numérique*.

> [Elle s]outient la démocratie et la cohésion sociale au Canada en faisant la promotion d'un écosystème d'information fiable, diversifié, sûr et exempt de désinformation et de contenu illégal, y compris les discours haineux. L'initiative vise à renforcer la résilience des citoyens face à la désinformation grâce à des activités et des programmes d'éducation à la citoyenneté, aux nouvelles et aux médias numériques qui sont offerts par des tiers. (Gouvernement du Canada, 2022a)

Dans le cadre de cette initiative, Patrimoine Canadien a financé plus de 50 projets visant à répondre à la mésinformation et à la désinformation, en sensibilisant le public à cet enjeu. Une somme de 7,2 millions de dollars a été allouée à ces projets depuis janvier 2020 (Heer et coll., 2021 : 18). À travers cette initiative, le gouvernement a financé des projets visant à comprendre plusieurs facettes de la désinformation comme le rôle des algorithmes sur les

[44] Traduction libre : contexte structurel dans lequel la désinformation n'atteint pas un grand nombre de citoyens. En même temps, [les personnes qui sont exposées à la désinformation] seront moins enclines à appuyer ou à diffuser davantage cette information de piètre qualité et, dans certains cas, elles seront plus en mesure de contrer cette information.

réseaux sociaux, la propagation transnationale de la désinformation à travers les communautés diasporiques, l'impact sur les communautés autochtones et la désinformation liée à la COVID-19 (G7, 2021 : 12).

Puis, dans le cadre d'une entente de 2,5 millions de dollars sur une période de 4 ans, *l'Initiative de citoyenneté numérique* soutient également le *Projet de démocratie numérique du Forum des politiques publiques du Canada* qui « réunit des universitaires, de simples citoyens et des professionnels de la politique pour poursuivre la recherche et l'élaboration de politiques sur la désinformation et les préjudices en ligne » (Gouvernement du Canada, 2022a). Enfin, le gouvernement a aussi accordé un financement de 50 millions de dollars pour le journalisme local, dans le but de réduire l'influence de sources trompeuse au niveau communautaire (Karen, 2018).

Finalement, les mesures de résilience à la désinformation ne sont pas limitées à l'éducation citoyenne. Le gouvernement du Canada indique s'engager à renforcer la préparation organisationnelle, en sensibilisant « les décideurs à la nature de l'ingérence étrangère » (Gouvernement du Canada, 2019). De ce fait, en vue des dernières élections « des exercices pangouvernementaux ont […] été organisés, notamment dans les domaines de la cybersécurité et des campagnes de désinformation » (Gouvernement du Canada, 2019), ce qui a permis de préparer les décideurs et haut fonctionnaire à être exposé et répondre à la désinformation.

3.2 Les mesures à l'internationale

À l'international, la stratégie du Canada pour lutter contre la désinformation se définit surtout par la création de partenariats pour échanger et coordonner de l'information avec ses alliés. Pour y arriver, le gouvernement canadien met en valeur sa présence déjà bien établie dans les organisations multilatérales. En effet, le gouvernement cherche à « position Canada at the centre of collective cyber defence by coordinating roles and sharing best practices »[45] (Jackson, 2022 : 17). À cet effet, AMC joue un rôle de premier plan pour coordonner les efforts du Canada avec les pays du G7, l'Union européenne, les « fives eyes » et ses autres alliés. Cela s'illustre par la place du Canada au centre du Mécanisme de réponse rapide (MRR) du G7, conçu pour coordonner les services de renseignement et les corps policiers des États afin de mieux identifier et contrer la désinformation ainsi que l'ingérence électorale (Tenove, 2020 : 7). Les efforts de coopération les plus importants du Canada se retrouvent au sein de ce mécanisme, dans lequel les pays membres partagent les meilleures pratiques et décider d'approches communes pour la lutte contre les manipulations informationnelles (G7, 2021 : 10). AMC détient une place importante au sein du MMR, en occupant le rôle de l'unité de coordination. Le Canada assure ainsi la coordination et le leadership de l'organisation, plaçant le pays au centre des efforts des pays du G7.

Par ailleurs, le Canada s'attaque aussi à la désinformation à travers l'OTAN, qui traite maintenant la désinformation comme une menace à la sécurité. En effet, l'OTAN a

[45] Traduction libre : positionner le Canada au cœur de la cyberdéfense collective en coordonnant les rôles et en partageant les pratiques exemplaires.

identifié la désinformation comme un « key aspect of "hybrid warfare" and increasingly coordinate their military and intelligence capabilities to address it »[46] (NATO StratCom 2016 cité dans Tenove, 2020: 7). À travers l'OTAN, un des outils que le Canada utilise est la communication stratégique, une méthode qui mène à de bons résultats selon Jackson (2022). En effet, l'auteure indique que la réponse la plus unifiée et la plus efficace du Canada pour lutter contre la désinformation se trouve dans la Force opérationnelle du Canada en Lettonie, qui s'est concentrée sur la sensibilisation du public pour répondre aux propos malveillants qui visaient le personnel militaire du Canada en Lettonie et les mérites de la participation de l'OTAN dans la région (17). Plus largement, le Canada, à travers l'OTAN, s'engage dans une « diplomatie publique active et collabore avec des partenaires mondiaux. Elle renforce ainsi les efforts déployés pour relever le défi de la désinformation, notamment au moyen de produits numériques sur des plateformes de médias sociaux destinés à des publics internationaux » (Gouvernement du Canada, 2022b). Par exemple, l'OTAN a créé « Mise au point », un site web visant à réfuter les mythes concernant les relations de l'OTAN avec la Russie (OTAN, 2022).

Le Canada tente aussi de développer des normes à l'international. À cet effet, Jackson (2022) indique que l'effort le plus important pour y arriver fut lors de négociations[47] aux Nations Unies durant lesquelles le gouvernement canadien avait l'objectif de « create a new global cybersecurity architecture to protect digital information

[46] Traduction libre : aspect clé de la « guerre hybride », et de coordonner de plus en plus leurs capacités militaires et de renseignement pour y faire face.

[47] Les discussions entourant ces négociations ont pris place lors du « United Nations Groups of Governmental Experts (UN GGE) » et plus récemment au sein des procédés du « Open-ended Working Group (OEWG) » (Jackson, 2022 : 561).

and the infrastructure on which it resides »[48] (Jackson, 2022 : 560). Pour arriver à cet objectif, le Canada a fourni des conseils sur la façon dont certaines normes pourraient être opérationnalisées. À cet effet, le Canada a soumis une proposition qui visait à créer un forum permanent aux Nations Unies pour examiner les questions de cyber sécurité, ce qui aurait permis d'examiner régulièrement le comportement en ligne des États et de négocier des mesures de coopération (Jackson, 2022: 561). Au final, aucune avancée n'a été faite en raison de préoccupations légales, politiques et autres (Jackson, 2022 : 561).

Enfin, le Canada multiplie son appui à des initiatives ou à des déclarations (des actions plutôt symboliques) qui appellent à réduire l'information problématique en général. Par exemple, le Canada a soutenu l'*Appel à l'action de Christchurch* à la suite d'un attentat terroriste en Nouvelle-Zélande. Il s'agit d'« engagements volontaires et collectifs en vue d'empêcher les gens d'utiliser l'Internet pour promouvoir ou glorifier le terrorisme » (Canada, 2019). Plus récemment, le Canada a appuyé la *Coalition pour la liberté en ligne*, une coalition de 34 gouvernements qui appellent à la « cessation de la mise en œuvre et du parrainage de campagnes de désinformation » par la Fédération de Russie (Gouvernement du Canada, 2022c). Similairement, la *Coalition pour la liberté des médias* condamne fermement le recours de longue date de la Russie à des campagnes de désinformation (Gouvernement du Canada, 2022d).

Finalement, on remarque que le Canada a établi des mesures variées pour répondre au problème de la désinformation, mais qui ne sont pas organisées autour d'une stratégie

[48] Traduction libre : créer une nouvelle architecture mondiale de cybersécurité pour protéger l'information numérique et l'infrastructure sur laquelle elle repose.

claire. Au contraire, la désinformation est parfois amalgamée à d'autres enjeux (p.ex. l'ingérence étrangère, les activités cyber, le terrorisme, etc.). En revanche, il existe une certaine cohérence dans les actions du gouvernement dans la protection du processus électoral. En effet, plusieurs mesures législatives, institutionnelles et de résilience (dans une moindre mesure) visent la protection de l'intégrité des élections.

3.3 Les mesures mises en place par d'autres pays

Les modèles du Royaume-Uni et de la Suède sont présentés ici afin d'observer comment la stratégie du Canada se compare à celle d'autres pays. Ces deux modèles ont été choisis puisqu'ils partagent des valeurs et des modèles politiques relativement similaires à ceux du Canada, mais aussi parce qu'ils illustrent des particularités distinctes dans leurs efforts pour contrer la désinformation.

3.3.1 Les mesures du Royaume-Uni

Le cas du Royaume-Uni est particulier puisqu'il a dû faire face à un volume important de désinformation dans les dernières années. En effet, durant la période entourant le référendum sur le Brexit, beaucoup de désinformation a circulé, notamment en provenance de la Russie grâce à l'Internet Research Agency (Booth, 2017). Or, la possibilité que des puissances extérieures se soient immiscées dans cet évènement important a fortement contribué à la mise à l'ordre du jour de cet enjeu.

Tout comme au Canada, le Royaume-Uni n'a actuellement pas de loi qui empêche la désinformation. Cependant, divers rapports gouvernementaux britanniques (Cairncross Review et Online Harm White Paper) proposent l'introduction de lois pour réguler la

fidélité des nouvelles sur les plateformes en lignes (Levush, 2019 : 162). En réponse à ces recommandations, le gouvernement a tout récemment introduit le « *Online Safety Bill* » qui vise à sévir contre les informations fausses et nuisibles sur Internet en exigeant des plateformes de médias sociaux, des moteurs de recherche et des sites Web qu'ils renforcent la protection des utilisateurs (Carlin, 2022). Cependant, comme au Canada, le projet de loi a rencontré des difficultés à répondre aux exigences de la liberté d'expression. Par exemple, Carlin (2022) explique que les défenseurs de la liberté d'expression affirment que la menace de lourdes amendes poussera les entreprises technologiques comme Google et Facebook à censurer le contenu légitime, à étouffer le débat public et à nuire à la liberté de la presse.

Au Royaume-Uni, la « Fusion Doctrine » oriente l'action gouvernementale. La doctrine fut introduite dans le National Security Capability Review (NSCR) et elle établit qu'une approche pangouvernementale est nécessaire pour répondre aux nouvelles menaces à la sécurité nationale (Ellehuss, 2020 : 19). De ce fait, la doctrine stipule que le:

> government must use the full suite of security, economic, diplomatic and influence capabilities to deliver our national security goals. This means strategic communications are to be considered with the same seriousness as financial or military options[49] (Levush, 2019 : 168).

En ligne avec cette doctrine, on assiste à une réorganisation de l'appareil étatique pour répondre aux nouvelles menaces.

[49] Traduction libre : le gouvernement doit utiliser toute la gamme des capacités en matière de sécurité, d'économie, de diplomatie et d'influence pour atteindre nos objectifs de sécurité nationale. Cela signifie que les communications stratégiques doivent être considérées avec le même sérieux que les options financières ou militaires.

> Under the program, the Cabinet Office is charged with heading up all counter-disinformation and counterinfluence efforts for HMG[50]. It is supported in this effort by the Home Office, Foreign and Commonwealth Office (FCO), and DCMS[51]. The Home Office leads on the UK domestic response to disinformation and other influence activities, drawing on its experience in counterterrorism and radicalization. The FCO is responsible for the United Kingdom's international response to disinformation, including capability and resilience building in nine countries abroad. […] DCMS plays a coordinating role and has the lead for UK counterdisinformation strategy and other new legislation[52] (Ellehuss, 2020 : 19)

Pour combattre la désinformation, le Royaume-Uni a mis en place différentes mesures pour surveiller, identifier et éliminer la désinformation. Pour y arriver, la stratégie du Royaume-Uni s'oriente autour de la création d'un réseau composé de différentes équipes et unités à travers le gouvernement. Ces différentes équipes deviennent des centres d'expertise dans leur champ d'action et répondent à différentes facettes de la désinformation.

D'abord, le gouvernement britannique a mis en place le National Security Communication Team (NSCT) dont l'objectif est de s'attaquer aux éléments des communications qui menacent la sécurité nationale, y compris (mais sans s'y limiter) à la désinformation (Vilmer, 2021 : 19). Une initiative particulièrement notable de l'organisation est la mise en place d'une liste de vérification nommée « SHARE », qui cherche à aider les citoyens à identifier le contenu faux ou trompeur afin d'empêcher la propagation de la désinformation (Vilmer, 2021 : 19). De plus, Alex Aiken, un haut

[50] Her Majesty's Government (HMG).
[51] Department for Digital, Culture, Media, and Sport.
[52] Traduction libre : Dans le cadre du programme, le Bureau du Cabinet est chargé de diriger tous les efforts de contre-désinformation et de contre-influence pour HMG. Il est soutenu dans cet effort par le Home Office, le Foreign and Commonwealth Office (FCO), et le DCMS. Le Home Office dirige la réponse nationale du Royaume-Uni à la désinformation et à d'autres activités d'influence, en s'appuyant sur son expérience dans la lutte contre le terrorisme et la radicalisation. Le FCO est responsable de la réponse internationale du Royaume-Uni à la désinformation, y compris le renforcement des capacités et de la résilience dans neuf pays à l'étranger. […] Le DCMS joue un rôle de coordination et est responsable de la stratégie de lutte contre la désinformation au Royaume-Uni et d'autres nouvelles lois.

fonctionnaire britannique, explique que « the NSCT works closely and collaboratively across government with policy and operational colleagues to ensure that we have coherent plans for the range of threats we face and the right strategic communication to deter our enemies »[53] (Aiken, 2018). Cela s'illustre avec l'établissement du modèle « RESIST » (voir Annexe A), qui établit des lignes directrices pour les ministères afin de répondre à la désinformation.

La NSCT collabore avec la *Rapid Response Unit* (RRU) qui est une unité composée de divers experts des médias et du numérique. Son rôle consiste à

> Monitor news and information being shared and engaged with online to identify emerging issues with speed, accuracy and with integrity. The results of this monitoring helps government understand the current media environment and assess the effectiveness of their public communications[54] (Levush, 2019: 170).

Par exemple, la RRU a contribué à contrer la désinformation sur le type et les origines de l'agent neurotoxique utilisé pour l'empoisonnement de Sergei Skripal en 2018, ainsi que de fausses informations sur les frappes aériennes en Syrie cette même année (Ellehuss, 2020 : 20). De plus, le mandat de surveillance de la RRU lui permet d'agir de façon préventive pour contrer les tactiques des adversaires qui voudraient propager de la

[53] Traduction libre : le NSCT travaille en étroite collaboration avec ses collègues des politiques et des opérations à l'échelle du gouvernement pour s'assurer que nous avons des plans cohérents pour l'éventail des menaces auxquelles nous faisons face et la bonne communication stratégique pour dissuader nos ennemis.
[54] Traduction libre : Surveiller les nouvelles et l'information échangées en ligne afin de cerner les nouveaux enjeux avec rapidité, exactitude et intégrité. Les résultats de cette surveillance aident le gouvernement à comprendre l'environnement médiatique actuel et à évaluer l'efficacité de ses communications publiques.

désinformation avant un vote, une décision ou un évènement important (Ellehuss, 2020 : 20).

Il existe ainsi plusieurs autres entités de la sorte au sein du gouvernement britannique comme : le Media Monitoring Unit, qui fait des rapports de surveillance sur les médias traditionnels et les réseaux sociaux; le Open-Source Unit, qui s'occupe de la surveillance des données provenant de sources ouvertes; et la Russia Unit, en charge d'implémenter le Counter Disinformation and Media Development (CDMD), un programme compréhensif se concentrant sur les opérations de désinformation provenant de la Russie (Vilmer, 2021 : 20). Plus récemment, en réponse à l'accentuation de la désinformation avec le coronavirus, le Royaume-Uni a mis en place, au sein du Department for Digital, Culture, Media and Sports *(DCMS)*, la Counterdisinformation Unit, qui « monitors harmful misinformation and disinformation and works with social media platforms to ensure action to address it »[55] (Carlin, 2022).

Bref, la majeure partie de la stratégie britannique pour combattre la désinformation tourne autour de ce réseau intergouvernemental d'unités spécialisées. Vilmer (2021 : 20) souligne que, bien que cela puisse constituer un défi, la coordination entre ces entités ne semble pas être un problème en raison d'une bonne communication entre ces groupes ainsi qu'une bonne définition des rôles.

Une partie des efforts du Royaume-Uni est aussi dirigée vers l'accroissement de la résilience par l'éducation citoyenne. Par exemple, la campagne « *Don't Feed the Beast* »

[55] surveille la désinformation et la désinformation préjudiciables et collabore avec les plateformes de médias sociaux pour prendre des mesures pour y remédier

encourage les consommateurs à déterminer la fiabilité de l'information en ligne avant de la partager. De plus, la Online Media Literacy Strategy prévoit 340 000 euros pour accroitre la résilience citoyenne dans les communautés et les organisations (GOV.UK, 2021). Cette initiative prévoit aussi de créer un groupe de travail composé d'experts venant des plateformes technologiques, de la société civile, du milieu académique et d'autres parties prenantes dans l'objectif d'organiser une action collective pour supprimer les barrières à l'éducation aux médias des citoyens. (GOV.UK, 2021).

Finalement comme le Canada, le Royaume-Uni collabore avec ses alliés traditionnels, comme le G7 et l'OTAN, pour répondre à la désinformation. Par exemple, pour contrer l'information trompeuse entourant la COVID, le Royaume-Uni a déployé des experts sur la désinformation pour conseiller et appuyer les efforts de l'OTAN (Vilmer, 2021 : 21).

3.3.2 Les mesures de la Suède

Il est possible d'observer des différences entre le modèle suédois et celui du Canada et du Royaume-Uni. Par exemple, la Suède utilise le concept de « l'influence informationnelle » (informationspåverkan) :

> [Information influence is] meant to refer to activities that involve potentially harmful forms of communication orchestrated by foreign state actors or their representatives. They constitute deliberate interference in a country's internal affairs to create a climate of distrust between a state and its citizens. Information influence activities are used to further the interests of a foreign power through the exploitation of perceived vulnerabilities in society. Foreign state actors study the controversies and challenges

> of a society and exploit these vulnerabilities to disrupt and polarize[56] (Vilmer. 2021, 10).

On remarque alors que la conception de la Suède de la désinformation est explicitement centrée sur l'État et semble aussi référer aux pratiques de désinformation qui sont propre à celles émanant de la Russie.

Au niveau des lois, la Suède dispose de quelques recours législatifs qui criminalisent la désinformation. Par exemple, il constitue un crime de « intentionally affect public opinion or limit the freedom of a political organization or a union or trade association to act and thereby jeopardize the freedom of speech and association through the use of force, coercion, or criminal threats »[57] (Levush, 2019: 144). De plus, Levush (2019 : 144) explique qu'accepter une rémunération de sources étrangères pour partager de la propagande en Suède constitue également un crime, tout comme diffuser des informations qui pourraient être dangereuses pour la sécurité nationale de la Suède. Bref, bien qu'il existe des dispositions criminalisant la désinformation, aucune de ces lois ne permet au gouvernement de bloquer du contenu en ligne pour des motifs de sécurité nationale (Levush, 2019 : 144).

[56] Traduction libre : [L'influence de l'information] désigne les activités qui impliquent des formes de communication potentiellement nuisibles orchestrées par des acteurs d'États étrangers ou leurs représentants. Elles constituent une ingérence délibérée dans les affaires intérieures d'un pays pour créer un climat de méfiance entre un État et ses citoyens. Les activités d'influence de l'information servent à promouvoir les intérêts d'une puissance étrangère en exploitant les vulnérabilités perçues dans la société. Les acteurs des États étrangers étudient les controverses et les défis d'une société et exploitent ces vulnérabilités pour perturber et polariser.

[57]Traduction libre : nuire intentionnellement à l'opinion publique ou limiter la liberté d'action d'une organisation politique ou d'un syndicat ou d'une association professionnelle, et ainsi compromettre la liberté d'expression et d'association par le recours à la force, à la coercition ou à des menaces criminelles

Au niveau institutionnel, la Swedish Civil Contingencies Agency (MSB) joue « un rôle de hub pour l'ensemble des services concernés » (Vilmer, 2018 : 119). Vilmer explique que l'agence « has been tasked with identifying and countering information influence campaigns. Their notable work includes raising awareness and preventing election interference »[58] (2021, 10).

Avant d'explorer plus en détail les mesures mises en place par la Suède, il faut noter que le modèle de gouvernance suédois est particulier. En effet, Vilmer (2021 : 10) explique que la structure du gouvernement suédois repose sur des agences fortes et de petits ministères. Ainsi, cette structure politique mène la Suède à opter pour une approche qualifiée de « par le bas »[59] par Vilmer (2021: 11), ce qui signifie que la Suède mise surtout sur la résilience de ces agences pour contrer la désinformation. Selon Vilmer (2021), cette approche par le bas « gives agencies the ability to counter foreign influence and disinformation without government support. This approach contrasts favourably with other countries […] and represents a clear strength of the Swedish approach »[60] (Vilmer, 2021: 11). Au sein de ce modèle, la MSB a une approche à trois niveaux pour combattre la désinformation :

> At the first level, it visits agencies and authorities and tells them about the threats; at the second level, it organizes preventative training; and at the third level, it arranges specific training on

[58] Traduction libre : a été chargé d'identifier et de contrer les campagnes d'influence de l'information. Leur travail remarquable comprend la sensibilisation et la prévention de l'ingérence électorale.
[59] Traduction libre de : « bottom-up approach ».
[60] Traduction libre de : donne aux organismes la capacité de contrer l'influence étrangère et la désinformation sans l'appui du gouvernement. Cette approche contraste favorablement avec celle d'autres pays […] et représente une force évidente de l'approche suédoise

> countermeasures where everyone prepares to fight together[61] (Vilmer, 2021: 13).

Cette approche mène donc les agences à mettre en place différentes mesures et initiatives qui sont alignées avec la stratégie du MSB. Les initiatives mises en place par la MSB et ses partenaires sont surtout axées sur l'accroissement de la résilience citoyenne. D'ailleurs, la Suède surplombe les autres pays dans la liste offerte par Vilmer et coll. (2018 : 123), qui illustre les initiatives visant la sensibilisation et l'éducation à la désinformation dans le monde. Voici des exemples de ces mesures :

- Soutien à la recherche par la collaboration avec les universités (le MSB suédois a préparé un Handbook sur les opérations d'influence avec l'université de Lund) et le financement de projets de recherche (le MSB finance 2 à 5 projets de recherche pour un budget total de 2 millions d'euros);
- Campagnes massives de sensibilisation, y compris en diffusant par voie postale (le MSB a tiré 4,7 millions d'exemplaires d'une brochure expliquant quoi faire en cas de crise, incluant les cas d'attaques terroristes ou campagnes de manipulation de l'information […];
- Formation des fonctionnaires, journalistes, entreprises (le MSB a déjà formé 11 000 fonctionnaires) ;
- Élaboration d'outils simples d'identification et de diagnostic à la disposition du public […].

Finalement, pour améliorer la coordination dans le modèle suédois, le gouvernement a récemment mis en place une nouvelle agence, la Agency for Psychological Defence, pour prendre le relais de la MSB comme nouveau hub pour diriger les efforts suédois. La nouvelle agence aura comme mandat d'identifier, analyser, prévenir et contrer les activités de désinformation dirigée vers les intérêts suédois (Sweden, 2022). Là où la

[61] Traduction libre : Au premier niveau, il visite les agences et les autorités et leur parle des menaces; au deuxième niveau, il organise une formation préventive; et au troisième niveau, il organise une formation spécifique sur les contre-mesures où tout le monde se prépare à combattre ensemble

MSB avait d'autres responsabilités qui n'étaient pas liées à la désinformation, la Agency for Psychological Defence sera entièrement concentrée sur cet enjeu.

À l'international, la Suède se concentre surtout sur la surveillance de la Russie, et aussi de la Chine. Par contre, contrairement au Canada et au Royaume-Uni, la Suède met aussi une emphase particulière sur la surveillance de l'Iran en raison de la forte diaspora iranienne au pays. De ce fait, les activités de la MSB ont beaucoup mis l'emphase sur l'extrémisme islamique (Vilmer, 2021 : 14). En termes de collaboration internationale, la MSB travaille avec la Swedish Institute, une agence du Ministère des affaires étrangères (MFA), qui a la responsabilité de surveiller la désinformation et les discours contre la Suède ou nuisant à l'image de la Suède à l'étranger (Vilmer 2021, 14). Au niveau de la coopération internationale, la Suède coopère surtout avec l'Union européenne et l'OTAN[62], et agit à travers les institutions multilatérales. Ainsi, « the MSB has two experts at the European External Action Service (EEAS), one in the East StratCom Task Force, and the other in the Western Balkan StratCom Task Force. They also have an expert at the NATO Centre of Excellence in Riga »[63] (Vilmer, 2021: 14).

Pour conclure, on peut voir au niveau canadien que l'emphase des mesures gouvernementales (fédérales) est dirigée vers la protection du processus électoral. En effet, la plupart des mesures sont, de près ou de loin, liées aux élections. De plus, hormis le registre de publicité politique pour les plateformes numériques en période électorale, la

[62] La Suède ne fait pas parti de l'OTAN. Cependant, les discussions pour que le pays scandinave se joigne à l'alliance militaires s'accentue depuis la toute récente invasion de l'Ukraine par la Russie.
[63] Traduction libre : la MSB compte deux experts au Service européen pour l'action extérieure (SEAE), l'un au sein de la East StratCom Task Force et l'autre au sein de la Western Balkan StratCom Task Force. Ils ont également un expert au Centre d'excellence de l'OTAN à Riga.

collaboration avec le secteur privé est de nature volontaire. On observe alors que, pour le moment présent, le gouvernement mise sur l'autorégulation des plateformes. On remarque aussi la décentralisation des mesures mises en place, qui émanent de différents ministères et organismes, une situation que Jackson (2022) qualifie de « fragmented and overlapping actions that cause concern about federal effectiveness »[64] (562). On peut alors observer une absence de stratégie claire sur la désinformation. De plus, il est possible d'observer, comme le souligne Jackson (2022), que l'enjeu de la désinformation semble avoir été « sécuritisé ». Le concept de « sécuritisation » est utilisé « pour comprendre comment des enjeux de sécurité non-traditionnels sont transformés en sujets référents de la sécurité (Lupovici, 2014: 401 cité dans Vigneau, 2020 : 904). La sécuritisation de la désinformation par le gouvernement canadien est explorée plus en détail dans la partie suivant. Il faut cependant noter que le Canada n'est pas le seul pays à avoir pris cette posture sécuritaire. Tenove (2020 : 523) explique que les acteurs à travers le monde se sont tournés vers le secteur de la sécurité nationale pour répondre à la désinformation en ligne. Il a d'ailleurs été possible d'observer l'adoption d'une conception similaire au sein des modèles suédois et britannique.

Au final, les trois modèles présentés, ceux du Canada, du Royaume-Uni et de la Suède, présentent des similitudes et des différences. Les trois pays mettent un accent sur la désinformation en provenance d'autres États et voient la désinformation comme une menace sécuritaire à la démocratie. Cependant, ils manifestent des accents différents. Le Canada concentre largement ses actions sur la protection des processus électoraux, le

[64] Mesures fragmentées et qui se chevauchent et qui suscitent des préoccupations au sujet de l'efficacité fédérale.

Royaume-Uni sur la mise en place d'unités spécialisées en charge de lutter à différentes facettes de la désinformation et la Suède sur des mesures pour accroitre la résilience des citoyens et des institutions contre l'influence informationnelle. De plus, un sentiment d'urgence plus prononcé se fait sentir en Suède et au Royaume-Uni. Cela s'explique par les expériences propres à ces pays. La Suède, étant en périphérie de la Russie, devient une cible probable pour cet acteur réputé pour livrer ce type d'activité. Il en va de même pour le Royaume-Uni et son expérience singulière lors du référendum sur le Brexit. L'impulsion générée par ce sentiment d'urgence peut donc expliquer en quoi ces deux pays ont semblé avoir une meilleure coordination et des mesures plus concertées en ce qui a trait à la désinformation.

Bien que cette comparaison puisse nous illuminer sur certains aspects, il faut noter qu'il est difficile de juger l'efficacité de ces réponses. Puisqu'il est déjà difficile de mesurer les impacts de la désinformation, il est encore plus difficile d'évaluer l'efficacité de contrer la désinformation (Vilmer, 2021 : 8). De plus, à l'exception du Royaume-Uni dans le cadre du Brexit, ces pays n'ont toujours pas été la cible principale d'une campagne de désinformation, ce qui pourrait bientôt ne plus être le cas. Au Canada, Woolf (2022) explique que la Russie a eu une influence sur le Convoi de la liberté et le mouvement anti-vaccin. De plus, une étude analysant plus six millions de tweet sur la guerre en Ukraine a démontré qu'environ 25% des comptes circulait des points de discussion pro-russes (Woolf, 2022). Par ailleurs, Kragh et Asberg (2017) démontrent que la Suède, dans les dernières années, a notamment été la cible d'activité d'influence en provenance de la Russie, avec le but ultime de préserver le statu quo géopolitique en Europe (2017: 808).

De ce fait, les discussions récentes entourant la possibilité que la Suède rejoigne l'OTAN pourraient être un élément qui pourrait amener la Russie à cibler davantage le pays scandinave. De futures études pourraient être révélatrices pour étudier l'efficacité de miser sur la résilience comme stratégie principale pour lutter contre la désinformation.

4. Comment explique-t-on l'action publique du Canada ?

Cette partie de la rédaction tentera une réponse à la question de recherche : comment explique-t-on l'action publique du Canada pour répondre à la désinformation ? D'abord, les défis liés aux réponses politiques aident à expliquer les mesures mises en place. En effet, ces défis démontrent les difficultés de mettre en place des mesures pour répondre à la désinformation, ce qui limite le champ d'action du gouvernement. Ces défis peuvent donc expliquer en quoi le gouvernement agit ou non sur certaines facettes de la désinformation. Dans le cadre de cette rédaction, les défis ont été catégorisés ainsi : les défis technologiques, les défis d'économie politique, les défis de coopération internationale et finalement les défis liés à la liberté d'expression. Ensuite, la sécuritisation de l'enjeu par les acteurs du domaine de la sécurité peut expliquer la réponse du Canada à la désinformation. En effet, en se faisant sécuritiser, le phénomène de la désinformation a été traité d'une façon différente que s'il n'avait pas été considéré comme un enjeu relevant de la sécurité nationale. Cette partie du travail est suivie d'une discussion sur les différents facteurs qui peuvent expliquer la fragmentation des mesures mises en place au Canada.

4.1.1 Les défis technologiques

Comme il a été démontré, l'évolution des technologies de télécommunication est intimement liée au rythme et à la portée de la propagation de la désinformation. Les défis technologiques liés à la désinformation sont abondants ; chaque technologie ou technique utilisée pour créer et propager de l'information trompeuse a ses propres défis et enjeux. Cependant, dans le cadre de cette rédaction, il faut retenir que ces technologies sont en constante évolution. Comme l'expliquent Nemr et Gangware (2021), « the challenge of confronting disinformation will continue to change as old technologies evolve and new ones develop. These changes may widen existing gaps between the threat of disinformation and the ability to counter it »[65] (39). Par exemple, pour illustrer ce dernier point, les auteurs expliquent que les technologies d'intelligence artificielle qui sont utilisées pour créer du contenu trompeur s'améliorent plus rapidement que les technologies qui sont chargées de repérer et bloquer ce type de contenu (Nemr et Gangware, 2021 : 41). Cela démontre qu'il serait insensé de s'appuyer uniquement sur ces technologies pour répondre à la désinformation.

Cette impossibilité de répondre à la désinformation d'une façon strictement technique peut donc expliquer le pari de certains pays, dont le Canada, de miser sur la résilience comme stratégie de réponse. Par exemple, Jackson (2022) explique que « DND has worked […] to consider how to address emerging technologies such as "deep fakes"

[65] Traduction libre : le défi de faire face à la désinformation continuera de changer à mesure que les anciennes technologies évoluent et que de nouvelles se développent. Ces changements pourraient élargir l'écart existant entre la menace de désinformation et la capacité de la contrer

and increase research and awareness about these issues »[66] (529). On voit alors que le gouvernement est toujours en train d'essayer de cerner ces nouvelles technologies, et que pour le moment, l'accroissement de la résilience est l'une des mesures privilégiées.

4.1.2 Les défis d'économie politique

Les défis technologiques sont intimement liés aux défis d'économie politique. En effet, une autre difficulté à proposer des réponses aux défis liés à la technologie est le manque de transparence et de contrôle sur ces technologies. Ce manque de transparence et de contrôle est de nature économique, puisque les détails sur le fonctionnement des algorithmes sont souvent gardés secrets pour des raisons commerciales par les plateformes numériques (Heer et coll., 2021 : 21). Par exemple, si une plateforme détient un algorithme extrêmement efficace pour générer de l'engagement (et ainsi des profits publicitaires), il est dans l'intérêt de la plateforme de garder la formule de cet algorithme secrète.

Heer et coll. (2021) expliquent que plus de transparence sur ces algorithmes « would provide the public, regulators, and researchers with an understanding of how algorithms make choices on what to amplify and to whom it is amplified it to »[67] (21). On comprend alors que ce manque de transparence rend la tâche difficile pour les décideurs politiques qui doivent mettre en place des mesures pour répondre aux problèmes causés par ces algorithmes sans l'accès à cette information.

[66] Traduction libre: Le MDN a travaillé […] à examiner la façon de traiter les technologies émergentes comme les « contrefaçons profondes » et à accroître la recherche et la sensibilisation à ces questions.
[67] Traduction libre : permettrait au public, aux organismes de réglementation et aux chercheurs de comprendre comment les algorithmes font des choix sur ce qu'il faut amplifier et à qui il est amplifié »

On remarque donc que les plateformes des réseaux sociaux ont une place extrêmement importante dans l'écosystème de la désinformation, et d'une part, les réseaux sociaux démontrent de l'intérêt à collaborer sur cet enjeu. Au Canada, cela s'observe avec l'exemple de la *Déclaration du Canada sur l'intégrité électorale en ligne* mentionné précédemment. Bien que les plateformes comme Google, Facebook, Twitter, etc. ont bel et bien mis des efforts importants pour lutter contre la désinformation, il reste que ces efforts ont majoritairement été réactifs à des pressions politiques (Reuters, 2019).

En réalité, les intérêts des plateformes ne sont pas toujours alignés avec ceux des gouvernements. Comme l'expliquent Nemr et Gangware (2021) sur le sujet :

> [S]ocial media platforms' incentives are not always prioritized to limit disinformation. In some respects, their incentives are aligned with spreading more of it. Tech giants' revenues are generated almost entirely through advertising, which depends on maximizing user engagement with the platform. As outlined earlier, users are more likely to click on or share sensational and inaccurate content; increasing clicks and shares translates into greater advertising revenue[68] (26).

Il existe ainsi un défi à désaligner les intérêts des plateformes et ceux des propagateurs de désinformation (Dipayna et Ghosh, 2018 : 29). Pour y arriver, la littérature propose généralement deux avenues : partenariat privé-public et/ou réglementation. On peut observer que le gouvernement canadien considère les deux modèles avec la *Déclaration*

[68] Traduction libre : Les incitations des plateformes médiatiques sociales ne sont pas toujours priorisées pour limiter la désinformation. À certains égards, leurs incitatifs sont axés sur une plus grande diffusion. Les revenus des géants de la technologie sont générés presque entièrement par la publicité, qui dépend de la maximisation de l'engagement des utilisateurs avec la plateforme. Comme indiqué précédemment, les utilisateurs sont plus susceptibles de cliquer sur ou de partager du contenu sensationnel et inexact; l'augmentation des clics et des partages se traduit par une augmentation des revenus publicitaires.

du Canada sur l'intégrité électorale en ligne versus le registre de publicités mandataires en période électorale inclue dans la *Loi sur la modernisation des élections.*

Il faut cependant noter que le modèle d'affaires des réseaux sociaux, qui encourage la désinformation pour vendre plus de publicité, n'est pas le seul responsable de la désinformation sur les réseaux sociaux. En effet, Dipayna et Ghosh (2018) soulignent l'exemple de Whatsapp, l'application de messagerie, où un grand volume de désinformation circule sur la plateforme, et ce, même si elle n'a pas de composante publicitaire (36).

4.1.3 Les défis liés à la liberté d'expression

Comme nous l'avons vu au Canada avec l'article 91 de *la Loi électorale du Canada*, mais aussi à l'internationale, il peut être difficile de formuler une réponse à la désinformation sans empiéter sur les principes de liberté d'expression. Il est surtout difficile pour le gouvernement de ne pas donner l'impression d'empiéter sur ces principes. La baisse de confiance envers les institutions facilitant déjà la désinformation (Vilmer, 2018 : 36), il y a donc un défi à limiter les dégâts les plus dommageables de la désinformation sans compromettre encore plus la confiance de la population.

Un des défis liés à la liberté d'expression est connexe à la section précédente. En effet, la relation entre le gouvernement et les entreprises de médias sociaux peut nuire à la liberté d'expression, si les pressions du gouvernement sont trop importantes ou mal ciblées, puisque pour répondre à ces pressions les plateformes tendent à surcensurer du contenu par précaution (Rasmus, 2021). Par exemple, Kelley et York (2017) démontrent sept instances

durant lesquelles différentes plateformes ont censuré du contenu à la suite de pressions diverses. Ainsi, les politiques de modération mises en place par les plateformes peuvent se traduire en restriction sur les discours légitimes, en plus d'être appliqués de façon inconsistante, et avec peu de transparence et de supervision (Rasmus, 2021).

De plus, la modération du contenu est souvent effectuée par des technologies d'intelligences artificielles plutôt que des employés (Heer et coll., 2021 : 21), ce qui peut causer des problèmes. Comme l'explique Rasmus (2021),

> the very real limitations of necessarily imperfect technologies combined with the inherently political nature of decisions over what constitutes disinformation means there are serious practical and principled limitations to how useful artificial intelligence will be in dealing with disinformation.[69]

Il est alors possible que ces technologies enlèvent du contenu légitime, au lieu de supprimer du contenu trompeur. De plus, il y a un manque de transparence sur les décisions et un manque de recours dans les cas où les publications sont enlevées (Heer et coll., 2021 : 21).

Un dernier élément important à présenter pour cette section est la présence de cas d'abus dans les réponses à la désinformation ailleurs dans le monde. En effet, comme le souligne De Lancer et Ouatik (2019), « des lois anti-fausses nouvelles plus sévères ont été adoptées, mais elles sont dénoncées par des groupes de défense de la liberté d'expression comme étant des moyens de censurer les critiques envers le gouvernement ». Par exemple,

[69] Traduction libre : les limites très réelles des technologies nécessairement imparfaites combinées à la nature intrinsèquement politique des décisions sur ce qui constitue de la désinformation signifient qu'il y a de sérieuses limites pratiques et fondées sur des principes à la façon dont l'intelligence artificielle sera utile pour traiter désinformation.

> En Thaïlande, pays dirigé par une junte militaire, le gouvernement a utilisé ce genre de loi pour poursuivre des journalistes, des artistes ou des politiciens qui avaient critiqué la monarchie ou l'armée. Des citoyens ont été arrêtés pour avoir partagé ou pour avoir apposé une mention « J'aime » à des publications Facebook jugées fausses par les autorités (De Lancer et Ouatik, 2019).

Ainsi certains groupes, au nom de la liberté d'expression, vont s'opposer aux lois pour contrer la désinformation en évoquant ces instances d'abus par des régimes autoritaires. Bref, le gouvernement doit prendre ces différents éléments sur la liberté d'expression en compte lors de la mise en place de mesure pour répondre à la désinformation. Ces contraintes peuvent expliquer l'absence de mesures draconiennes pour contrer la désinformation, puisqu'elles pourraient être perçues de façon négative par la population. De plus, comme il a été démontré, la protection judiciaire sur le droit à la liberté d'expression a déjà empêché la mise en place de certaines mesures au Canada, ce qui limite aussi la capacité d'action du gouvernement canadien.

4.1.4 Les défis de la coopération internationale

Étant un phénomène mondial et transfrontalier, les solutions à la désinformation requièrent nécessairement une variété d'acteurs à travers le monde. Cependant, la coopération internationale sur cet enjeu fait face à quelques obstacles.

Premièrement, il n'y a pas de lois à l'international sur lesquelles peuvent s'appuyer les États pour répondre à la désinformation, et ce, même en période électorale (Hollis, 2018 ; Ohlin, 2017 dans Tenove, 2021 : 523). En effet, là où les cyberattaques sur des infrastructures vitales à l'État pourraient être vues comme des violations à la souveraineté

de l'État, et pouvant ainsi justifier des mesures de représailles selon l'article 51 de la charte des Nations Unies, il est « much more difficult to make that argument regarding disinformation, as it affects people's beliefs, emotions, and cognitive processes »[70] (Tenove, 2021 : 523). En conséquence, les démocraties occidentales, y compris le Canada, se sont surtout tournées vers leurs alliés traditionnels pour coopérer à l'international. Comment explique-t-on cette difficulté d'établir des lois et des normes à l'international pour lutter contre la désinformation ? D'abord, comme nous l'avons suggéré précédemment dans ce mémoire, il est possible que la perception de la menace que représente la désinformation ait une influence sur capacité des États et leur désir d'agir sur cet enjeu. Par exemple, Vilmer (2017) illustre comment, il y a de cela quelques années, la différence entre les perceptions de la Russie de la part des pays de l'Union européenne entravait la capacité de ces pays à agir sur la désinformation. L'auteur explique :

> Les institutions européennes ne semblent pas très investies (…) Les 28 ayant des relations différentes avec la Russie, ils n'accordent pas tous la même importance au problème de la désinformation russe. Les pays baltes sont ultra-conscients de leur vulnérabilité, due à la proximité géographique, aux liens historiques et à la présence d'importantes communautés russophones (37 % des Lettons par exemple). Ils sont donc à la pointe de la lutte contre l'influence russe, suivis par la Scandinavie, l'Europe centrale et, pour des raisons différentes, le Royaume-Uni. À l'autre bout du spectre, des États lointains et plus préoccupés par le flanc sud (Italie, Grèce, Chypre) sous-estiment le problème et défendent même un rapprochement avec Moscou (levée des sanctions au nom des intérêts économiques). Comme sur d'autres sujets, l'Europe est donc divisée en matière de lutte contre la désinformation russe, ce qui affaiblit les initiatives communes (Vilmer, 2017 : 13).

[70] Traduction libre: Il est beaucoup plus difficile de présenter cet argument concernant la désinformation, car elle influe sur les croyances, les émotions et les processus cognitifs des gens

Heureusement, la coordination s'est améliorée en termes de coopération européenne comme le démontre le « *Plan d'action contre la désinformation* »[71] et la « *Législation sur les services numériques*[72] ». Cependant, il est quand même possible d'observer, avec cet exemple de l'Union européenne, que la différence entre les perceptions de l'enjeu entre les différents pays peut être une entrave à la coopération sur la désinformation.

De ce fait, cette différence de perception peut avoir un impact sur l'attention et les efforts d'un pays. Dans une étude de l'OCDE, en 2020, seulement 54 % des pays avaient adopté une définition du terme « désinformation » ou de « mésinformation » (OCDE, 2021). Cela constitue donc un défi puisque, comme l'indique Matasick et coll. (2020), « accurately defining mis- and disinformation is essential to fully understanding the challenges it poses and the potential responses »[73] (cité dans OCDE, 2021). Donc, en considérant que certains pays n'ont tout simplement pas de définition de la désinformation, tandis que d'autres ont des définitions différentes, il devient alors difficile de mettre en place des normes ou des lois dans un contexte international en raison de ces différentes postures.

[71] En préparant les élections européennes, la Commission européenne a appelé au développement d'une réponse coordonnée à la désinformation en juin et octobre 2018. Le Plan d'action contre la désinformation a été adopté en décembre 2018 dans le but de renforcer les capacités et la coopération entre les États membres et les institutions de l'UE. Le Plan d'action définit une approche sociétale pour contrer la désinformation qui est fondée sur les valeurs européennes, y compris la liberté d'expression (OCDE, 2021).

[72] La *Législation sur les services numériques* est une règlementation qui sera directement applicable dans toute l'UE. Voici quelques-unes des obligations : (…) Obligations pour les très grandes plateformes en ligne et les moteurs de recherche de prévenir l'utilisation abusive de leurs systèmes en prenant des mesures fondées sur le risque, y compris la surveillance au moyen de vérifications indépendantes de leurs mesures de gestion du risque. Les plateformes doivent atténuer les risques tels que la désinformation ou la manipulation électorale, la cyberviolence contre les femmes ou les préjudices causés aux mineurs en ligne. Ces mesures doivent être soigneusement équilibrées par rapport aux restrictions de la liberté d'expression et sont soumises à des audits indépendants (European Commission, 2022).

[73] Traduction libre : Il est essentiel de bien définir la mésinformation et la désinformation pour bien comprendre les défis qu'elles posent et les réponses possibles.

Un dernier élément illustrant le défi de la coopération internationale peut se trouver dans la différence des valeurs entre les pays. Ignatidou (2019) utilise l'exemple des États-Unis et de l'Union européenne pour illustrer ce point :

> The EU and US diverge in terms of constitutional and human rights priorities – e.g. freedom of expression vis-à-vis privacy or surveillance and security – and the trade-offs they have settled with feed into their non-aligned approach to disinformation. Aggravating the complexity of coordinating regulatory efforts is the fact that the debate in the US revolves around freedom of expression and the framing of efforts to constrain the power of Big Tech as being anti-free market, when in the EU freedom of expression is a qualified right that has to be balanced with other rights such as privacy[74] (Ignatidou, 2019 : 34).

On voit alors que la différence des valeurs entre ces deux acteurs influence leur conception de la réponse politique nécessaire pour combattre la désinformation. À ce niveau, aucun choc de valeur entre le Canada et un autre pays comme l'exemple susmentionné n'a été relevé dans notre recherche. Cependant, cela illustre quand même les difficultés d'avancement dans un contexte multilatéral.

Au final, ces éléments peuvent nous éclairer sur les mesures mises en place par le Canada au niveau international. On comprend, à l'aide de ces défis, pourquoi les tentatives du Canada d'établir des normes dans un contexte international ont échoué, et aussi

[74] Traduction libre : L'UE et les États-Unis divergent en ce qui concerne les priorités constitutionnelles et en matière de droits de l'homme (p. ex., la liberté d'expression en matière de vie privée, de surveillance et de sécurité) et les compromis avec lesquels ils se sont entendus pour alimenter leur approche non alignée de la désinformation. La complexité de la coordination des efforts de réglementation est aggravée par le fait que le débat aux États-Unis tourne autour de la liberté d'expression et de l'encadrement des efforts visant à limiter le pouvoir des Big Tech comme étant anti-libre marché, lorsque dans l'UE la liberté d'expression est un droit qualifié qui doit être équilibré avec d'autres droits tels que la vie privée.

pourquoi le Canada s'est tourné vers ses alliés traditionnels (G7, OTAN, É-U, etc.) pour répondre et coopérer sur la désinformation.

Pour conclure sur le thème des défis de la réponse à la désinformation, on comprend que les différents éléments exposés limitent les mesures qui peuvent être mises en place par le gouvernement contre la désinformation : la technologie utilisée est en constante évolution, et donc difficile à encadrer ; le modèle d'affaires des plateformes est problématique et difficilement changeable ; les craintes liées à la liberté d'expression sont particulièrement sensibles aux actions gouvernementales ; et, finalement, la coopération internationale est loin d'être évidente en raison des réactions différentes à la désinformation. Tout cela démontre les limites à la capacité d'action du gouvernement fédéral canadien. De plus, on peut aussi observer que, dans certains cas, ces défis peuvent être reliés entre eux. Par exemple, il a été démontré que des actions pour répondre à des défis d'économie politique pourraient avoir un impact sur le principe de la liberté d'expression. Sinon, il a été aussi démontré que la difficulté d'étudier certaines technologies était liée à des raisons commerciales. L'interrelation entre ces défis démontre aussi qu'une approche pour répondre à la désinformation devrait être holistique afin d'être efficace.

4.2 La réponse sécuritaire

Les défis de la réponse à la désinformation nous éclairent surtout sur la marge de manœuvre que détient le gouvernement canadien pour établir des mesures s'attaquant à la désinformation. Cependant, l'élément le plus révélateur sur la réponse du Canada à la

désinformation est la prise en charge de l'enjeu par les acteurs relevant de la sécurité. Nous argumentons que la caractérisation de la désinformation comme étant un enjeu relevant de la sécurité nationale a fortement influencé la façon dont le gouvernement canadien a répondu à la désinformation.

D'abord, comme l'explique Jackson (2022), les rapports gouvernementaux conçus pour informer et sensibiliser à la désinformation ont dépeint celle-ci comme un enjeu urgent, persistant, une menace légitime qui exige une réponse sérieuse (561). Par exemple dans « *Qui dit quoi ? »,* un rapport du SCRS, on peut observer cette rhétorique. On peut y lire que : « les médias et la société en général doivent comprendre que les opérations d'influence sont dangereuses, qu'elles doivent être prises au sérieux et qu'il faut s'y attaquer sans tarder » (SCRS, 2018 : 50). C'est ce type de rhétorique qui fait en sorte que le Canada se concentre sur la désinformation venant de l'étranger, ainsi que sur la protection du système électoral. Par exemple, l'*Évaluation des cybermenaces nationales* de 2018 prédisait que 2019 allait être une année particulièrement périlleuse pour les institutions canadiennes (Jackson, 2022 : 552). Similairement, le rapport de 2019 du CST établissait qu'il était très probable que des adversaires étrangers interfèrent dans les élections de la même année (Jackson, 2022 : 552).

De plus, Jackson (2022) explique que cette sécuritisation de l'enjeu permet aux acteurs qui sont impliqués dans la réponse à la désinformation d'avoir des « more prominent roles and new funds in the name of 'securing' Canada and Canadians »[75] (Jackson, 2022 : 561). Il

[75] Traduction libre : des rôles plus importants et de nouveaux fonds au nom de la « sécurité » du Canada et des Canadiens.

faut noter que la sécuritisation de la désinformation ne signifie pas que ce ne sont que les acteurs relevant du domaine de la sécurité qui ont un rôle à jouer dans la lutte contre la désinformation. C'est plutôt que les autres acteurs ont aussi rejoint cette conception sécuritaire de la désinformation. Jackson (2022) explique que « even non security and military government actors (e.g., Elections Canada) used the language of threat and urgency, and sometimes worked with security actors in new whole-of government efforts »[76] (562). Bref, les nouveaux fonds associés à la sécuritisation de la désinformation ajoutent une motivation d'inclure la désinformation dans le portfolio des activités de certains acteurs gouvernementaux, même si ces derniers ne priorisent pas forcément la désinformation. De ce fait, cette motivation d'avoir un accès accru à de nouveaux fonds augmente le nombre d'acteurs agissant sur la désinformation, ce qui mène à une augmentation des mesures mises en place, mais aussi à des mesures qui ne sont pas coordonnées entre elles.

Puis, la sécuritisation de la désinformation a fait en sorte que l'enjeu est souvent regroupé avec les autres sortes de cybermenaces, ce qui empêche de développer une réponse adaptée à la désinformation. En effet, plusieurs rapports gouvernementaux illustrent les dangers de la désinformation et établissent la désinformation comme une menace se situant aux côtés d'autres menaces comme l'ingérence étrangère, la guerre hybride et les cyberactivités (Jackson, 2022 : 561). Bien que les agences de sécurité déclarent la désinformation comme un problème important dans les rapports et

[76] Traduction libre : même les acteurs non liés à la sécurité et les gouvernements militaires (p. ex., Élections Canada) ont utilisé le langage de la menace et de l'urgence, et ont parfois collaboré avec les acteurs de la sécurité dans le cadre de nouveaux efforts pangouvernementaux.

déclarations, la désinformation n'a pas causé de réorientation stratégique. Par exemple, dans *Protection, Sécurité, Engagement*, la dernière politique de défense du Canada, la désinformation n'a été mentionnée qu'une seule fois, et ce, aux côtés des autres menaces cyber (Ministère de la défense nationale du Canada, 2017 : 72). Cette approche de la désinformation, qu'on considère comme une menace cyber parmi d'autres, explique pourquoi peu de mesures mises en place visent seulement la désinformation, ce qui mène au développement de mesures comme la *Loi concernant des questions de sécurité nationale*, qui vise les cybermenaces dans leur ensemble. Il en va de même pour le *Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections* dont la désinformation n'est qu'une composante de leur activité (Gouvernement du Canada, 2021a).

Il faut cependant noter, comme Tenove (2020) le fait, qu'il peut être justifié de traiter la désinformation comme un enjeu relevant de la sécurité. En effet, « only state security agencies have the combination of signals intelligence and human intelligence needed to discover coordinated and covert disinformation campaigns »[77] (Tenove, 2020 : 524). Il faut aussi préciser que l'approche sécuritaire ne se traduit pas nécessairement par des réponses offensives ou militaires. Au contraire, la SCRS explique que :

> Il n'existe pas de solution unique au problème complexe et multidimensionnel de la désinformation. La réglementation, la vérification des faits, la dénonciation et l'éducation ont toutes un rôle à jouer. Toute solution qui met l'accent sur un de ces éléments au détriment des autres n'a pas beaucoup de chances de réussir. Il est nécessaire de bâtir la résilience sur autant de fronts que possible. (SCRS, 2018 : 50)

[77] Traduction libre : seuls les organismes de sécurité de l'État ont la combinaison de renseignements électromagnétiques et de renseignements humains nécessaires pour découvrir des campagnes de désinformation coordonnées et secrètes.

En revanche, une logique de sécurité nationale peut aussi poser des risques. Par exemple, cela peut se faire au péril de la qualité du débat public, puisqu'une logique de sécurité nationale peut indûment interpréter des communications fausses ou partiellement fausses comme des risques pour la sécurité, plutôt que comme des possibilités de correction et de débat (Tenove, 2020: 524). De plus, ce type d'approche donne un grand rôle à ces agences qui tendent à avoir un faible contrôle démocratique (Tenove, 2020 : 524). En outre, la vision sécuritaire peut parfois limiter le champ d'analyse et les réponses politiques qui vont être considérés. Comme l'explique Rapin (2021),

> de plus en plus d'observateurs appellent maintenant à adopter un changement d'approche radical face à l'enjeu de la désinformation. Les démocraties occidentales accorderaient trop d'importance aux campagnes de désinformation étrangères (particulièrement celles venues de Russie, qui réveillent évidemment de vieux fantômes), négligeant au passage des problèmes internes plus profonds.

La posture sécuritaire fait donc en sorte de limiter le champ d'analyse lors de l'étude de ce phénomène et limite ainsi l'analyse des éléments « domestiques, sociaux et identitaires derrière l'essor de la désinformation » (Rapin, 2021). Cela peut être observé dans le contexte canadien, où les documents et rapports gouvernementaux, et le discours politique en général, n'adressent pas cette perspective plus holistique sur la désinformation. Par exemple, il a été possible d'observer qu'une emphase particulière de la réponse canadienne se concentre sur l'influence des puissances hostiles, plutôt que de chercher à revigorer les institutions démocratiques. Cela nous indique que la perspective sécuritaire limite les solutions considérées pour cet enjeu multidimensionnel. Finalement, comme le conclut Rapin (2021),

> en conséquence, les sceptiques appellent désormais les démocraties occidentales à se regarder sérieusement dans le miroir plutôt qu'à « sécuritiser » désespérément le problème de la désinformation : répondre de bonne foi à la méfiance des opinions publiques plutôt que « tout mettre sur le dos » de puissances hostiles, revigorer les institutions démocratiques plutôt que chercher à resserrer le contrôle des flux d'information. Faute de quoi, ces réflexes sécuritaires ne feront que jouer en faveur des puissances adverses, qui auront beau jeu de dénoncer une censure du prétendu « monde libre ». Semblables à une maladie auto-immune, la désinformation et les réponses qu'elle vient mécaniquement générer contribueraient ainsi à affaiblir encore davantage les organismes démocratiques attaqués.

Cette perspective nous démontre qu'il est ainsi possible de questionner si finalement la question de la désinformation est approchée de la bonne façon par les démocraties occidentales. Comme on peut l'observer, cette réponse sécuritaire de l'État tend à mettre une emphase très élevée sur la désinformation parrainée par l'État qui, rappelons-le, n'est qu'une composante parmi d'autres de la désinformation. Par le fait même, la réponse sécuritaire ignore les causes structurelles et les problèmes sociétaux qui permettent à la désinformation de croitre en premier lieu.

En bref, la sécuritisation de la désinformation par le gouvernement oriente l'action publique de différentes façons. D'abord, la désinformation est traitée comme une menace sérieuse et urgente, ce qui pousse le Canada à mettre l'emphase sur la protection des élections et sur la désinformation extérieure, parrainée par l'État. De plus, cette urgence débloque de nouveaux fonds et responsabilités qui sont convoités par différents acteurs, ce qui les motive à prendre en charge la désinformation, menant ainsi à la mise en place d'actions disparates. Puis, la désinformation a été regroupée avec les autres types de cybermenaces, ce qui nuit à la mise en place de mesures spécifiques à la désinformation.

Finalement, la sécuritisation de la désinformation limite les politiques publiques considérées en mettant l'emphase sur les puissances hostiles, ignorant d'autres aspects de la désinformation qui pourraient faire l'objet d'une intervention publique.

4.3 Discussion

Les éléments susmentionnés, soit les défis et la sécuritisation, peuvent nous aider à comprendre l'absence d'une stratégie ou d'une ligne directrice pour agir sur la désinformation, ce qui se traduit par des mesures fragmentées. En effet, les défis mentionnés illustrent la difficulté à émettre une réponse cohérente à la désinformation, en plus de démontrer les enjeux auxquels doivent faire face le gouvernement, la société civile et le secteur privé (c.-à-d. les plateformes numériques). De plus, comme il a été démontré, la sécuritisation de la désinformation a, entre autres, mis le phénomène sur un pied d'égalité avec d'autres menaces, ce qui nuit à la mise en place de mesures spécifiques à cet enjeu.

Au-delà de ces éléments, on remarque qu'il n'y a pas d'acteur gouvernemental qui a pris le leadership pour lutter contre la désinformation. Évidemment, comme il a été mentionné, les agences de sécurité ont joué un rôle important dans la réponse du Canada. Cependant, le contraste est important entre les agences de sécurité canadienne et l'exemple de la « *Swedish Civil Contingencies Agency »,* qui comme nous l'avons vu, a mis en place des efforts importants de coordination à l'échelle du pays qui se sont traduits par une réponse plus cohérente.

Plusieurs raisons pourraient potentiellement expliquer cette absence de leadership pour mener les efforts du pays, comme la structure gouvernementale canadienne ou bien

l'absence de volonté politique[78]. Cependant, il est clair que l'absence d'un organe chargé de répondre explicitement à ce phénomène contribue à la fragmentation des initiatives. En plus de la sécuritisation de la désinformation et l'implication de plusieurs acteurs gouvernementaux dans la réponse à cet enjeu, qui sont les principaux éléments explicatifs, il est aussi possible de souligner la nouveauté et la complexité du phénomène, qui rendent difficile la mise en place d'une stratégie pour répondre à la désinformation. En effet, comme il a été souligné au début de ce mémoire, l'étude du phénomène de la désinformation est si récente qu'il n'existe toujours pas de consensus au niveau de la littérature académique sur la définition de la désinformation et les impacts réels de ce phénomène. En considérant tous ces éléments, il est difficile de s'attendre à une réponse cohérente de la part des gouvernements, incluant le gouvernement canadien.

5. Recommandations

Quand vient le temps de considérer des moyens pour améliorer la réponse à la désinformation, Nemr et Gangware (2019) soulignent que

> Stakeholders face the distinct challenge of developing policy solutions to protect the information environment in a way that does not undermine public trust, while curbing a disinformation problem that will only continue evolving. What stakeholders should aim for, then, are strategies to mitigate disinformation and its potentially

[78] Dans « Defining Political Will » Lori et coll. (2010) définissent la volonté politique comme « the extent of committed support among key decision makers for a particular policy solution to a particular problem » (8). Les auteurs indiquent quatre composantes à la volonté politique : Un nombre suffisant de décideurs; une compréhension commune d'un problème particulier à l'ordre du jour officiel; un engagement des décideurs d'appuyer; et une solution politique communément perçue et potentiellement efficace. Or, dans le cas de la désinformation, on peut comprendre que ces différents critères sont difficilement atteints en prenant en considération les observations de ce mémoire. Par exemple, la difficulté de comprendre le phénomène et l'absence d'une solution communément partagé explique la difficulté de générer de la « volonté politique ».

> disastrous consequences while maintaining a robust commitment to civil liberties, freedom of expression, and privacy[79](44).

De ce fait, l'empreinte du gouvernement dans une stratégie pour combattre la désinformation devrait éviter d'être intrusive. Comme l'indique Vilmer et coll. (2018), « le premier rempart contre les manipulations de l'information, dans une société démocratique et libérale, doit rester la société civile (les journalistes, les médias, les plateformes numériques, les ONG, etc.) » (174). D'ailleurs, les auteurs soulignent que cela correspond aux attentes des populations qui croient en majorité, selon un sondage, que la lutte contre la désinformation est avant tout une responsabilité des médias et des plateformes numériques (Vilmer et coll, 2018 : 174). Bref, conformément à ce que suggèrent ces derniers, la logique d'une stratégie canadienne serait gagnante à « favoriser les approches horizontales, collaboratives, sollicitant la participation de la société civile » (174). En effet, comme il a été possible d'observer, la désinformation est un enjeu aux multiples facettes qui nécessite la collaboration de nombreux acteurs. Afin de coordonner cette approche autour d'une stratégie cohérente, le gouvernement devrait considérer la mise en place d'une entité gouvernementale se concentrant sur la désinformation. Il faut noter que cette entité, qui pourrait s'inspirer de l'agence mise en place en Suède, devrait miser sur la transparence afin qu'elle n'apparaisse pas comme un « ministère de la vérité orwellien » (Vilmer et coll. 2018 : 122). Avec un acteur jouant le rôle de *hub*, il serait plus facile d'harmoniser les recommandations sous mentionnées autour d'une stratégie efficace. De plus, la création d'une entité strictement centrée sur la désinformation permettrait de déconstruire

[79] Traduction libre : Les parties prenantes font face au défi distinct d'élaborer des solutions stratégiques pour protéger l'environnement de l'information d'une manière qui ne mine pas la confiance du public, tout en freinant un problème de désinformation qui ne fera que continuer d'évoluer. Les parties prenantes devraient donc viser des stratégies visant à atténuer la désinformation et ses conséquences potentiellement désastreuses tout en maintenant un engagement solide à l'égard des libertés civiles, de la liberté d'expression et de la protection de la vie privée.

l'amalgame de la désinformation avec les autres enjeux cyber, ce qui permettrait de développer des réponses spécifiques à la désinformation.

Puis, ce mémoire recommande que la réponse canadienne à la désinformation place l'accroissement de la résilience au centre de sa stratégie face à la désinformation. L'accroissement de la résilience comme stratégie pour répondre à la désinformation apparait par défaut, puisqu'elle réussit à répondre aux défis mentionnés dans la section précédente. Par exemple, la liberté d'expression ne se trouve pas affectée par des initiatives visant l'éducation à la désinformation. Par ailleurs, l'accroissement de la résilience par l'éducation citoyenne, l'éducation aux médias, la sensibilisation, etc. sont des mesures promues comme de bonnes solutions par un grand nombre de textes consultés pour ce mémoire, tant au niveau des acteurs relevant de la sécurité qu'au niveau académique. Ainsi le gouvernement canadien devrait continuer de créer et financer des programmes associés à la résilience, qui permettent entre autres aux citoyens de penser de façon plus critique à ce qu'ils voient et partagent en ligne. De plus, ces mesures s'avèrent efficaces. Par exemple, Guess et coll. (2020 : 3) ont démontré que des interventions en éducation des médias pouvaient augmenter la capacité de discernement de fausses nouvelles à plus de 26 %. Comme le résume Vilmer (2017) « la désinformation ne fonctionne que grâce à la crédulité du public » (33). Il existe déjà des exemples prometteurs de ce type d'initiative (voir Gouvernement du Canada. 2022a; Gouvernement du Canada. 2022e), et le Canada devrait donc concentrer ses efforts sur cette composante de ses activités sur la désinformation. Pour améliorer la réponse du Canada dans cette sphère d'activité, le gouvernement devrait augmenter le financement alloué à ses initiatives. Les dernières données financières

accessibles indiquent que 7.2 millions de dollars ont été alloués pour 50 projets, ce qui est insuffisant considérant que c'est un enjeu dynamique (nécessitant alors des efforts continus), et dont l'intervention est nécessaire à travers l'ensemble du pays.

Finalement, il faut souligner qu'il est encore très tôt pour évaluer avec certitude l'efficacité des stratégies pour contrer la désinformation. Les études ne sont pas à un stade assez avancé pour en tirer des conclusions définitives. Ainsi, il serait recommandé pour le Canada de financer la recherche sur ce phénomène qui n'est pas encore entièrement compris. De surcroit, les recherches sur la désinformation dans le contexte canadien sont minimes. L'accroissement de la connaissance spécifique au contexte canadien permettrait donc d'ajuster l'action publique du Canada dans le futur. De plus, comme il a été observé, l'enjeu de la désinformation a été sécuritisé, et cette sécuritisation peut aussi être observée au sein de la recherche sur le sujet, qui traite la plupart du temps la désinformation comme un enjeu relevant de la sécurité nationale. Cependant, certains auteurs (Yaffa, 2020; Rapin, 2021; Vilmer et coll. 2018; Humprecht, 2020) s'éloigne de la perspective sécuritaire. Par exemple, l'étude de Humprecht (2020, 507) démontre que les pays les plus résilients à la désinformation partagent des caractéristiques structurelles communes. Ces pays ont peu de polarisation, font beaucoup confiance aux médias, et ont des services publics de radiodiffusion solide. On peut alors comprendre que ces nouvelles perspectives pourraient inspirer les gouvernements à développer de nouvelles politiques publiques qui agiront sur ces facteurs structurels, plutôt qu'à se concentrer sur les puissances étrangères par exemple. D'ailleurs, Humprecht (2020) implore les chercheurs et les preneurs de décision à considérer ces facteurs structurels pour répondre à la désinformation. Ainsi, une meilleure

compréhension de la désinformation pourrait permettre de s'éloigner de la perspective sécuritaire pour répondre à la désinformation.

Pour conclure, ce mémoire contribue à la littérature sur la désinformation en peignant un tableau des politiques actuelles du Canada pour répondre à cet enjeu. Bien que l'on ait pu assister à un essor de la littérature dans les dernières années sur la désinformation, les études spécifiques au Canada sont encore rares. De ce fait, ce mémoire complémente les recherches qui se concentrent sur le cas canadien, en facilitant l'observation et l'analyse des mesures qui sont actuellement en place au Canada. Ce mémoire a démontré que la désinformation à l'ère du numérique est un phénomène complexe, toujours en définition, avec des conséquences incertaines, mais trop alarmantes pour être ignorées. Il a aussi été démontré que dans l'environnement informationnel d'aujourd'hui, la désinformation se propage à un rythme sans précédent en raison de l'apparition et la démocratisation des nouvelles technologies et des plateformes numériques. Dans cet environnement numérique, une variété d'acteurs, étatiques et non étatiques, se livrent à des activités de désinformation. Puis, à l'image de la plupart des démocraties occidentales, il a été démontré que le Canada a sécuritisé la désinformation, influençant ainsi fortement sa conception du phénomène, et du même coup, les mesures proposées. Il a aussi été possible d'observer que la réponse du Canada, quoique fragmentée, se concentre entre autres sur la protection des élections et sur la désinformation parrainée par les États. En raison des différents défis que pose la désinformation, la résilience comme stratégie de réponse apparait par défaut. Quoiqu'il soit trop tôt pour évaluer l'efficacité des stratégies pour contrer la désinformation, une conception plus large qui prend en compte

les facteurs sociaux, domestiques et identitaires de la désinformation devrait être considérée au Canada, mais aussi au sein des démocraties occidentales.

6. Bibliographie

Aiken, Alex. 2018. *Disinformation is a continuing threat to our values and our democracy*. Government Communication Service (U.K.). https://perma.cc/CJ8H-JKXB

Andrews, C., Fichet, E., Ding, Y., Spiro, E. S., & Starbird, K. 2016. *Keeping up with the tweetdashians: The impact of "official" accounts on online rumoring*. In Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (pp. 452–465).

Ang, Benjamin, Nur Diyanah Anwar, et Shashi Jayakumar. 2021. *Disinformation & Fake News: Meanings, Present, Future* ISBN: 9789811558764.

Bandurski, David. 2022. *China and Russia are joining forces to spread disinformation*. Brookings.

Booth, Robert, Matthew Weaver, Alex Hern, Stacee Smith et Shaun Walker. 2017. *Russia used hundreds of fake accounts to tweet about Brexit, data shows*. The Guardian. https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets

Canada. 2019. *Le Canada se joint à l'Appel à l'action de Christchurch pour lutter contre le contenu en ligne à caractère terroriste et lié à l'extrémisme violent*. https://pm.gc.ca/fr/nouvelles/communiques/2019/05/15/canada-se-joint-lappel-laction-de-christchurch-lutter-contre

Canadian Security Intelligence Service. 2018. *Who said what? The Security Challenges of Modern Disinformation*. Ottawa. https://www. canada.ca/content/dam/csis-scrs/documents/ publications/disinformation_post-report_eng.pdf.

Code Criminel. 2022. *Code criminel (L.R.C. (1985), ch. C-46*). https://laws-lois.justice.gc.ca/fra/lois/c-46/

Commission européenne, Direction générale des réseaux de communication, du contenu et des technologies. 2018. *A multi-dimensional approach to disinformation : report of the independent High level Group on fake news and online disinformation*. Publications Office. https://data.europa.eu/doi/10.2759/0156

Cooley, Alexander et Daniel Nexon. 2020. *Exit from Hegemony: The Unraveling of the American Global Order*. ISBN-13: 9780190916473. DOI: 10.1093/oso/9780190916473.001.0001

Dawood, Y. 2021. *Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats*. Election Law J. Rules Polit. Policy 20, 10–31. https://doi.org/10.1089/ elj.2020.0652

De Lancer, Alexis et Bouchra Ouatik. 2019. *Pourquoi n'est-il pas illégal de propager des fausses nouvelles au pays ?* https://ici.radio-canada.ca/nouvelle/1360304/lois-anti-fausses-nouvelles-canada-censure-liberte-expression

Dipayan Ghosh and Ben Scott. 2018. *#DigitalDeceit - The Technologies Behind Precision Propaganda on the Internet*. New America, https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit

Dubow, Ben, Edward Lucas, Jake Morris. 2021. *Jabbed in the Back: Mapping Russian and Chinese Information Operations During COVID-1*. CEPA. https://cepa.org/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-covid-19/

Ellehuss, Rachel. 2020. *Mind the Gaps*. Center for Strategic and International Studies. https://www.jstor.org/stable/pdf/resrep25326.6.pdf

Eordogh, Fruzsina. 2016. *Pro-Trump Trolls Want You To Vote For Hillary Via Text (You Can't)*. Forbes. https://www.forbes.com/sites/fruzsinaeordogh/2016/11/03/pro-trump-trollswant-you-to-vote-for-hillary-via-text-you-cant/.

European Commission. 2022. *Questions and Answers: Digital Services Act* https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

Fallis, Dom. 2015. *What Is Disinformation?* Libr. Trends 63, 401–426. https://doi.org/10.1353/lib.2015.0014

Freelon, Deen, et Chris Wells. 2020. *Disinformation as Political Communication*. Political Communication 37 (2): 145–56. doi:10.1080/10584609.2020.1723755.

G7 Rapid Response Mechanism. 2022. *Protecting Democracy*. http://www.g8.utoronto.ca/summit/2022elmau/2022-05-06-rrm-data.pdf

Global Internet Forum to Counter Terrorism. 2019. *GIFCT Independent Advisory Committee: Interim Terms of Reference*.https://gifct.org/wp-content/uploads/2021/09/GIFCT-IAC-Terms-of-Reference.pdf

Global Internaet Forum to Counter Terrorism. 2022. Governance. https://gifct.org/governance/

Gobeil, Mathieu. 2021. *Punir ceux qui relaient des faussetés, est-ce le moyen de lutter contre la désinformation ?* Radio-Canada. https://ici.radio-canada.ca/nouvelle/1778463/desinformation-loi-electorale-federale-fausses-declarations-reseaux-sociaux-trudel.

Gouvernement du Canada. 2018. *Le gouvernement du Canada adopte la Loi sur la modernisation des élections* *https://www.canada.ca/fr/institutions democratiques/nouvelles/2018/12/le-gouvernement-du-canada-adopte-la-loi-sur-la-modernisation-des-elections.html*

Gouvernement du Canada. 2019. *Renforcer la préparation organisationnelle*. *https://www.canada.ca/fr/institutions-democratiques/nouvelles/2019/01/renforcer-la-disponibilite-operationnelle-des-organismes.html*

Gouvernement du Canada. 2021a. *Groupe de travail sur les menaces en matière de sécurité et de renseignements visant les élections*. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/groupe-travail-securite.html

Gouvernement du Canada. 2021b. *Charte canadienne du numérique : La confiance dans un monde numérique*. https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00108.html

Gouvernement du Canada. 2021c. Déclaration du Canada sur l'intégrité électorale en ligne. https://www.canada.ca/fr/institutions-democratiques/services/protection-democratie/declaration-integrite-ectorale.html

Gouvernement du Canada. 2022a. *La désinformation en ligne*. https://www.canada.ca/fr/patrimoine-canadien/services/desinformation-en-ligne.html

Gouvernement du Canada. 2022b. *Les efforts du Canada pour contrer la désinformation - Invasion russe de l'Ukraine.* *https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=fra*

Gouvernement du Canada. 2022c. *Le gouvernement du Canada rehausse son appui aux organismes pour aider à contrer la désinformation nuisible* https://www.canada.ca/fr/patrimoine-canadien/nouvelles/2022/03/le-gouvernement-du-canada-rehausse-son-appui-aux-organismes-pour-aider-a-contrer-la-desinformation-nuisible.html

Gouvernement du Canada. 2022d. *Déclaration au nom du président de la Coalition pour la liberté en ligne : Un appel à l'action sur la désinformation parrainée par l'État en Ukraine.* *https://www.canada.ca/fr/affaires-mondiales/nouvelles/2022/03/declaration-au-nom-du-president-de-la-coalition-pour-la-liberte-en-ligne--un-appel-a-laction-sur-la-desinformation-parrainee-par-letat-en-ukraine.html*

Gouvernement du Canada. 2022e. *Document d'information – Aider les citoyens à renforcer leur pensée critique et leur résilience face aux dangers de la désinformation en ligne*. Https://www.canada.ca/fr/patrimoine-canadien/nouvelles/2019/07/fiche-dinformation--aider-les-citoyens-a-renforcer-leur-pensee-critique-et-leur-resilience-face-aux-dangers-de-la-desinformation-en-ligne.html

GOV. UK. 2021. *Minister launches new strategy to fight online disinformation*. https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation

Government Communication Service (U.K.). 2019. RESIST Counter-disinformation toolkit. https://3x7ip91ron4ju9ehf2unqrm1-wpengine.netdna-ssl.com/wp-content/uploads/2020/03/RESIST-Counter-Disinformation-Toolkit.pdf

Gowen, Annie et Max Bearak. 2017. *Fake news on Facebook fans the flames of hate against the Rohingya in Burma*. Washington Post.

Guess, Andrew et Benjamin Lyons. 2020. *Misinformation, Disinformation, and Online Propaganda*. In N. Persily & J. Tucker (Eds.), Social Media and Democracy: The State of the Field, Prospects for Reform (SSRC Anxieties of Democracy, pp. 10-33). Cambridge: Cambridge University Press.

Guess, Andrew, Michael Lerner, Benjamin Lyons, Jacob M. Montgomery, Brendan Nyhan, Jason Reifler et Neelanjan Sircar. 2020. *A Digital Media Literacy Intervention Increases Discernment between Mainstream and False News in the United States and India Proceedings of the National Academy of Sciences* 117 (27): 15536–45. https://doi.org/10.1073/pnas.1920498117.

Havelin, Miriam. 2021. *Misinformation & Disinformation in Canadian Society A system analysis & futures study.* http://openresearch.ocadu.ca/id/eprint/3505/1/Havelin_Miriam_2021_MDes_SFI_MRP.pdf

Heer, Tej, Charlee Heath, Kimberly Girling, Emma Bugg. 2021. *Misinformation in Canada: Research and Policy Options*, Evidence for Democracy. https://evidencefordemocracy.ca/sites/default/files/reports/misinformation-in-canada-evidence-for-democracy-report_.pdf

Heilwil, Rebecca et Shirin Ghaffary. 2021. *How Trump's internet built and broadcast the Capitol insurrectio*n. https://www.vox.com/recode/22221285/trump-online-capitol-riot-far-right-parler-twitter-facebook

Hum, Peter. 2022. *New uOttawa project probes disinformation driving 'Freedom Convoy' and other socio-political crises*. Ottawa Citizen

Humprecht, Edda et Frank Esser. 2020. *Resilience to Online Disinformation: A Framework for Cross-National Comparative Research.* https://doi.org/10.1177/1940161219900126

Ignatidou, Sophia. 2019. *EU–US Cooperation on Tackling Disinformation*. Chatham House. https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf

Jack, Caroline. 2017. *Lexicon of lies: Terms for problematic information*. Data & Society, 3.https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf

Jackson NJ. 2022. *The Canadian government's response to foreign disinformation: Rhetoric, stated policy intentions, and practices*. International Journal. doi:10.1177/00207020221076402

Jankowicz, Nina. 2020. *How to Lose the Information War : Russia, Fake News, and the Future of Conflict.* (chapitre 7). Bloomsbury.

Karen K. Ho and Mathew Ingram. 2018. *Canada pledges $50 million to local journalism. Will it help?* Columbia Journalism Review, https://www.cjr.org/business_of_news/canada-journalism-fund-torstar-postmedia.php.

Kelley, Jason et Jillian C. York. 2017. Seven Times Journalists Were Censored: 2017 in Review. https://www.eff.org/deeplinks/2017/12/seven-times-2017-journalists-were-censored

King, Gary, Jennifer Pan, Margaret E. Roberts. 2017. *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, American Political Science Review, 111:3, 2017, p. 484-501

Lanoszka. Alexander 2019. *Disinformation in international politics*. European Journal of International Security 4, no. 2 : 227–248

Le Bras. Stéphane et Philippe Bourdin. 2018. *Fausses nouvelles. Un millénaire de bruits et de rumeurs dans l'espace public français*. Presses universitaires Blaise Pascal, Clermont-Ferrand.

Loomba, S., de Figueiredo, A., Piatek, S.J. 2021. *Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. Nat Hum Behav* **5,** 337–348. https://doi.org/10.1038/s41562-021-01056-1

Lori Ann Post, Amber n. w. Raile, Eric d. Raile. 2010. Defining Political Will. https://doi.org/10.1111/j.1747-1346.2010.00253.x

Marwick, Alice and Rebecca Lewis. 2017. *Media Manipulation and Disinformation Online.* New York: Data & Society Research Institute https://datasociety.net/ output/media-manipulation-and-disinfo-online/.

Molina, M. D., Sundar, S. S., Le, T., & Lee, D. 2019. *"Fake news" is not simply false information: A concept explication and taxonomy of online content*. American Behavioral Scientist. doi:10.1177/0002764219878224

Neander, J., & Marlin, R. 2010. *Media and Propaganda: The Northcliffe Press and the Corpse Factory Story of World War I*. Global Media Journal, 3(2).

Nikiforuk, Andrew. 2022. *A Convoy Revved by Foreign Actors Spreading Lies*. The Tyee. https://globalnews.ca/news/8450263/infodemic-covid-19-disinformation-canada-pandemic/

OECD. 2021. *Public communication responses to the challenges of mis- and disinformation.* OECD Report on Public Communication : The Global Context and the Way Forward **https://www.oecd-ilibrary.org/sites/ce2619da-en/index.html?itemId=/content/component/ce2619da-en#back-endnotea6z4**

Organisation du traité de l'Atlantique Nord. 2022. *Mise au point.* https://www.nato.int/cps/en/natohq/115204.htm?selectedLocale=fr

Posetti, Julie et Alice Matthews. 2018. *A short guide to the history of 'fake news' and disinformation.* International Center for Journalists.

Radio-Canada. 2022. *L'Union européenne achève une réforme historique contre la jungle numérique.* https://ici.radio-canada.ca/nouvelle/1878418/ue-reforme-historique-numerique-gafam

Rapin, Alexis. 2021. *Campagnes de désinformation : menace exagérée ou réel péril stratégique ?* Les Grands Dossiers de Diplomatie n.60 - L'État des conflits dans le monde

Rasmus, Nielsen. 2021. *How to respond to disinformation while protecting free speech*. Reuters Institute. https://reutersinstitute.politics.ox.ac.uk/about-reuters-institute

Reuters. 2019. *Trudeau announces 'digital charter,' tells social media companies to fight fake news or be fined*. https://globalnews.ca/news/5283178/trudeau-digital-charter/

Sarts, Janis. 2021. *Disinformation as a Threat to National Security*. 10.1007/978-981-15-5876-4_2.

Starbird, Kate, Ahmer Arif, et Tom Wilson. 2019. *Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations*. http://faculty.washington.edu/kstarbi/

Stewart, Ashley. 2021. *The great COVID-19 infodemic: How disinformation networks are radicalizing Canadians*. Global News

Tenove, Chris, et H.J.S. Tworek. 2019. *Online Disinformation and Harmful Speech: Dangers for Democratic Participation and Possible Policy Responses*. *Journal of Parliamentary and Political Law 13: 215–32.*

Tenove, Chris, Jordan Buffie, Spencer McKay, David Moscrop, Mark Warren, Maxwell A. Cameron. 2018. *Digital Threats To Democratic Elections: How Foreign Actors Use Digital Techniques*. Vancouver, BC: Centre for the Study of Democratic Institutions. https:// democracy.arts.ubc.ca/2018/01/18/digital-threats/.

Tenove, Chris. 2020. *Protecting Democracy from Disinformation: Normative Threats and Policy Responses*. The International Journal of Press/Politics. 2020;25(3):517-537. doi:10.1177/1940161220918740

Vigneau, Elsa. 2020. *Immigration, médias et sécuritisation au Canada: une étude de La Presse et du National Post, 1998–2015*. Canadian Journal of Political Science; Cambridge Vol. 53, N° 4, 902-919. DOI:10.1017/S0008423920001092

Vilmer, Jeangène, A. Escorcia, M. Guillaume, J. Herrera. 2018. *Les Manipulations de l'information : un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, août 2018.

Vilmer, Jeangène. 2021. *Effective state practices against disinformation: Four country case studies*. The European Centre of Excellence for Countering Hybrid Threats.

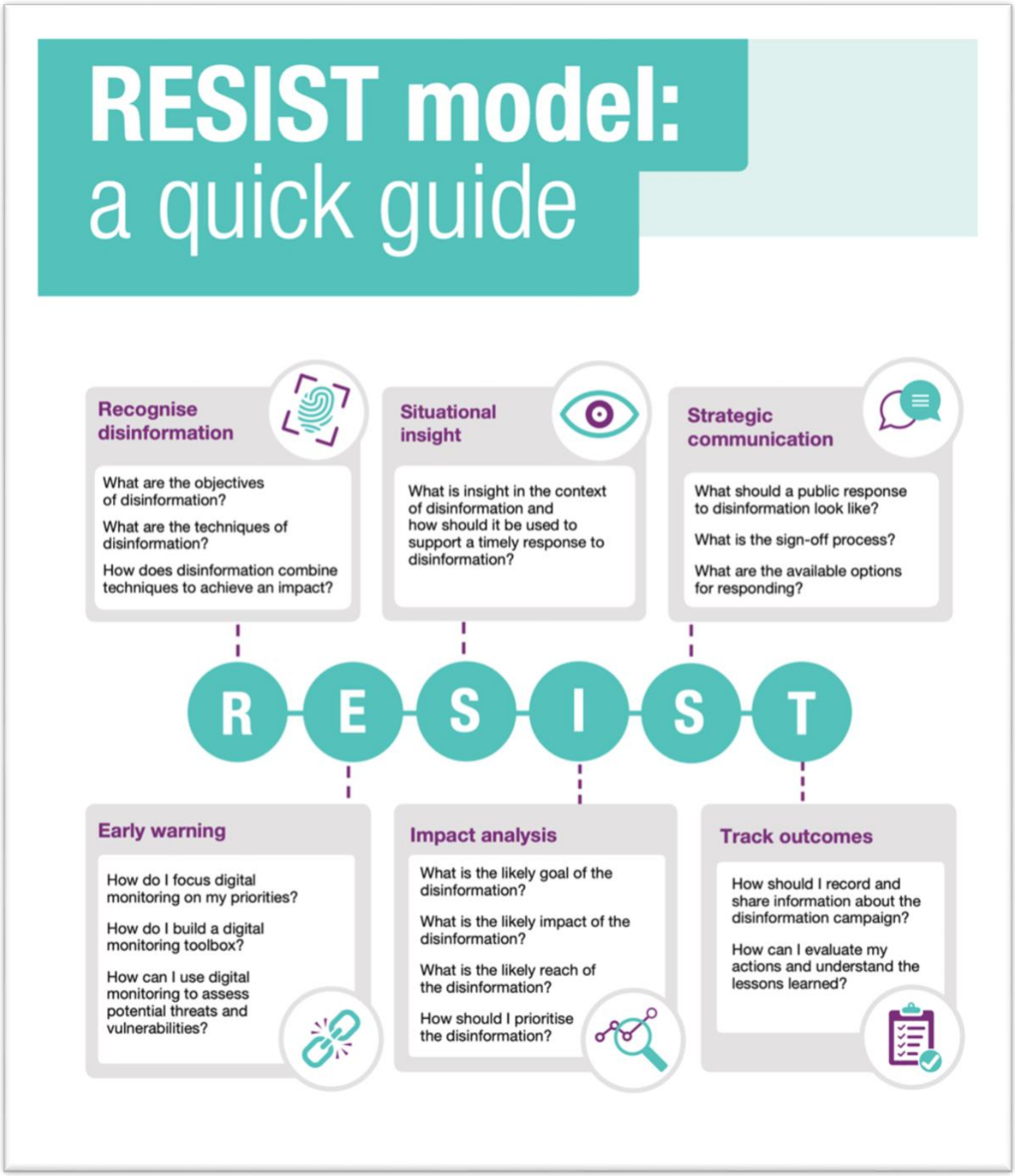
Vilmer, Jeangène. 2017. *La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande?* Revue Défense Nationale, 801, 93-105. https://doi.org/10.3917/rdna.801.0093

Wardle, Claire et Hossein Derakhshan. 2017. *Information Disorder: Towards an Interdisciplinary Framework for Research and Policymaking*. Council of Europe. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framew ork-for-researc/168076277c 4

Woolf, Marie. 2022. *Canada target of Russian disinformation, with tweets linked to foreign powers. https://www.theglobeandmail.com/canada/article-canada-is-target-of-russian-disinformation-with-millions-of-tweets/*

Yaffa, Joshua. 2020. Is Russian Meddling as Dangerous as we Think ? The New Yorker.

Annexe A : Le modèle « RESIST » : Un guide rapide



Source: U.K. Government Communication Service (2017)