Traiter l'influence comme un virus pour mettre l'accent sur la population dans la lutte contre les manœuvres d'influence hostile

Évaluation fondée sur des sources ouvertes
commandée dans le cadre du Programme de liaison-recherche
du Service canadien du renseignement de sécurité (SCRS)
Ottawa, le 29 avril 2019

[redacted]

Éléments à retenir

- Jusqu'à présent, la lutte contre les manœuvres d'influence a été en grande partie axée sur les questions en jeu, c'est-à-dire sur les allégations ou la version des faits des acteurs hostiles.
- Dans le présent document, un modèle complémentaire, axé sur la population, est proposé. Il s'agit en premier lieu d'analyser le public cible de ce type de manœuvre.
- Dans le modèle en question, inspiré de l'épidémiologie, l'influence hostile est considérée comme posant les mêmes problèmes qu'un virus.
- En conséquence, la lutte passe par la prévention de nouvelles infections et l'aide aux personnes qui ont déjà été exposées (le traitement).
- La prévention peut consister à répertorier les principales sources d'influence hostile, isoler les vecteurs de la maladie et vacciner la population par l'éducation, en vue de garantir la sécurité en ligne.
- L'expérience de celles et ceux qui travaillent à extraire les personnes des griffes des sectes ou des recruteurs extrémistes pourrait servir à trouver des moyens d'action.
- En tout état de cause, les gouvernements devraient sonder en permanence la population sur les questions clés d'information et de sécurité, afin de mieux comprendre les informations qu'elle reçoit et la pénétration des informations attribuables aux forces hostiles.

[redacted]

Les manœuvres d'influence hostile contre les démocraties occidentales sont un sujet de préoccupation de premier plan. Des acteurs russes et iraniens en ont déjà conduites, et d'autres pays affûtent leurs armes pour modeler l'opinion de leur propre population, armes qui pourraient ensuite être tournées vers des États étrangers[1]. Réel, le danger est aussi d'actualité, et les acteurs mal intentionnés, à l'intérieur ou à l'extérieur, tenteront de

mettre des techniques similaires au service de leur cause.

Depuis l'annexion de la Crimée par la Russie, les puissances occidentales ont commencé à mettre en place des structures de lutte contre les manœuvres d'influence hostile. L'Union européenne a créé l'East Strategic Communications task force (équipe spéciale chargée des communications stratégiques avec l'Est) et le Royaume-Uni s'est doté d'équipes de lutte contre la désinformation et d'analyse des sources ouvertes. Aux États-Unis, le Global Engagement Center a ajouté la Russie à la liste de ses priorités. En 2018, sous la houlette du Canada, le G7 a convenu de créer le Mécanisme de réponse rapide, qui vise à déceler et à contrer les manœuvres d'influence hostile.

En parallèle, la société civile et le secteur privé ont commencé à révéler au grand jour les manœuvres de désinformation et d'influence. Les initiatives comme Bellingcat[2], Graphika[3], FireEye[4], EU Disinfolab[5], Integrity Initiative de l'Institute for Statecraft[6], Kremlin Watch du groupe de réflexion d'European Values[7] et DFRLab d'Atlantic Council[8] ont toutes permis de découvrir certains aspects des manœuvres d'influence.

Toutes ces initiatives, qu'elles soient publiques ou privées, abordent le problème *sous l'angle des questions* : elles se fondent sur les agissements des acteurs hostiles et s'efforcent de dévoiler ou de réfuter chacune de leurs allégations et campagnes. Dans le présent article, nous proposons une *approche axée sur la population*, vouée à servir de complément à l'approche basée sur les questions, et non à la remplacer. Il s'agit de s'intéresser aux cibles des manœuvres hostiles et à les protéger de deux façons : par la prévention et par le traitement. Cette façon de faire permet aux gouvernements de jouer un rôle plus proactif et de fournir plus de soutien et d'informations que dans l'approche classique *fondée sur les questions*.

L'influence, comme le virus de la grippe

La désinformation et l'influence hostile peuvent être considérées comme des virus[9]. Elles se propagent par contact direct avec une source infectée (organes de propagande comme Russia Today et Sputnik) ou par contact avec une personne infectée (publications sur les médias sociaux, que ce soit à partir de véritables ou de faux comptes).

La désinformation et l'influence hostile peuvent être portées par différents vecteurs, comme les organes de presse, les radiodiffuseurs et les télédiffuseurs, les sites Web, les médias sociaux et le bouche-à-oreille. Certaines allégations peuvent sembler disparaître longtemps, comme un virus qui ne trouverait pas d'hôte, avant de redevenir actives (comme la théorie voulant que le virus du sida ait été conçu par les États-Unis, lancée par l'Union soviétique, qui refait surface régulièrement sur le Web). La durée d'incubation peut être assez longue avant que le comportement de la personne infectée ne se modifie, ce qui rend toute contamination difficile à détecter rapidement[10].

Il importe de souligner que tous les individus et toutes les populations ne sont pas égaux devant les manœuvres de désinformation et d'influence. Comme l'a montré l'opération russe contre les États-Unis, les réactions n'ont pas été les mêmes dans tous les groupes démographiques : certains (comme les Autochtones et les Latinos) ont été en apparence peu touchés, d'autres (notamment les membres de la « droite

alternative » et du mouvement Black Lives Matter) l'ont été bien davantage[11].

Par conséquent, comme une épidémie de grippe, toute attaque d'influence présente deux difficultés : la prévention et le traitement. La prévention répond à la nécessité urgente de faire obstacle à la propagation du virus dans la population. Il importe aussi de trouver un traitement pour guérir les personnes touchées, mais cela nécessite plus de temps et d'investissements.

Prévention et vaccination

Il existe plusieurs moyens d'aborder la prévention dans le contexte de l'influence : la découverte de la source, l'isolation des vecteurs de transmission et la vaccination.

Sondages permanents

Les gouvernements peuvent jouer un rôle essentiel en commandant des sondages d'opinion détaillés et réguliers, à grande échelle, sur des questions clés. Actuellement, les mesures de lutte contre la désinformation achoppent sur un manque de données d'observation au sujet de la façon dont le public réagit à la désinformation. Un corpus de données recevables sur le plan statistique et issues de sondages permanents pourrait permettre de bien mieux comprendre l'épidémiologie de l'influence.

Ces sondages pourraient servir à répertorier les sources d'information les plus populaires et celles qui sont considérées comme les plus fiables selon le lieu et les caractéristiques démographiques. Ils pourraient aussi permettre de connaître la perception qu'ont les participants des principaux acteurs locaux ou internationaux (autorités régionales et nationales, Union européenne, Organisation des Nations Unies, etc.) ainsi que leur point de vue sur les questions du moment (migrations, extrémisme, sécurité, transparence sur les médias sociaux). Ils pourraient être réalisés en ligne, sur papier, par téléphone, sous forme de groupes de discussion ou suivant d'autres modalités viables.

Autant que possible, il faudra éviter de mentionner les principales sources de désinformation et les principaux thèmes qui en font l'objet dans ces sondages, pour ne pas en faire la publicité. Par exemple, il vaut mieux demander : « Quelles sont les sources d'information en lesquelles vous avez le plus confiance » que : « En laquelle des sources d'information suivantes avez-vous le plus confiance? », puis énumérer à la fois de véritables organes de presse et des sources de désinformation.

Découverte de la source

Les groupes qui s'attaquent aux questions faisant l'objet de désinformation parviennent souvent à en déterminer les sources. Dans ce domaine, le gouvernement et les acteurs indépendants pourraient tirer des enseignements d'une collaboration. Dans certains cas, la source peut être directement associée à un organe comme l'Agence de recherche sur Internet russe ou l'International Union of Virtual Media (IUVM) iranienne[12]. Elle peut parfois être directement liée à un organe de presse d'un État hostile, comme Russia Today, Sputnik ou PressTV.

Une fois la source déterminée, diverses mesures sont envisageables. Selon la législation nationale, il pourra s'agir de l'interdire, purement et simplement, d'imposer des sanctions financières et politiques, de la classer dans la catégorie des agents étrangers ou de collaborer avec les entreprises de médias sociaux pour

qu'elles éliminent les comptes des fauteurs de trouble de leurs plateformes. Quoi qu'il en soit, l'objectif consiste à réduire la capacité de la source à toucher et à contaminer la population.

Isoler les vecteurs

Il est plus complexe d'isoler les vecteurs (qui favorisent la contagion), qui sont obscurs parce qu'ils sont hors ligne ou utilisent des canaux chiffrés. Pour y parvenir, il faudra aussi collaborer étroitement et de façon constructive avec les plateformes de médias sociaux, qui sont les mieux placées pour intervenir.

L'objectif consiste à déterminer comment les campagnes d'influence hostile sont relayées jusqu'au public cible. Les vecteurs peuvent être des sites Web (par exemple, l'IUVM de l'Iran), des comptes sur les médias sociaux ou des « agents de validation » dans le monde réel, qui sont payés ou qui s'associent volontairement aux campagnes qu'ils promeuvent.

Une fois repérés, les vecteurs peuvent être mis en quarantaine afin que le grand public n'y accède pas. Cela ne sera pas toujours facile, ni même toujours possible, surtout quand le vecteur en question est un « agent de validation » en chair et en os, qui n'a en apparence aucun lien douteux avec la campagne.

Cependant, il existe différentes mesures de mise en quarantaine : les sites Web suspects peuvent être descendus dans le classement des moteurs de recherche ou, dans les pires des cas, saisis par les forces de l'ordre[13]; les comptes suspects sur les médias sociaux peuvent être temporairement fermés. Quant aux « agents de validation », ils pourront être amenés à modifier ou à modérer leur opinion en dialoguant avec le public, ou perdre en crédibilité quand leur rôle dans la campagne d'influence est dévoilé.

Vaccination

Comme dans le cas d'une épidémie, la vaccination est le meilleur moyen de protéger les communautés qui n'ont pas encore été touchées par la campagne d'influence. C'est avant tout le rôle de l'éducation, qui est principalement du ressort des gouvernements.

La culture médiatique est souvent mentionnée comme nécessaire à la lutte contre la désinformation. Cependant, comme les campagnes d'influence ne passent qu'en partie par les médias, la connaissance de ces derniers n'est qu'une composante de la solution.

Il y aurait plutôt lieu de mettre l'accent sur la sécurité en ligne, afin d'élargir le débat sans pour autant exclure la culture médiatique. En outre, ce concept tient compte des similitudes entre les manœuvres d'influence politique et d'autres formes de comportement répréhensible en ligne : tactiques d'approche visant à amadouer une personne ou un enfant, pistage obsessionnel et vol d'identité.

L'éducation du grand public (et pas simplement des jeunes) à la sécurité en ligne est un projet clair et facile à expliquer, qu'un gouvernement pourra vraisemblablement présenter à la population sans susciter de polémique. Il s'agira de doter la population de compétences arrêtées à l'avance tout en s'efforçant de lui inculquer une certaine prudence générale, puisque les changements technologiques précéderont toujours l'évolution des politiques et des programmes d'enseignement.

Ces compétences doivent comprendre des techniques faciles à maîtriser et accessibles à tous, comme la recherche inversée d'images et de vidéos. Elles doivent permettre à chacun de repérer les comptes dont la photo de profil a, en fait, été volée, et de détecter le recyclage d'images (par exemple, quand des clichés ou des vidéos soi-disant de fraude électorale dans un pays proviennent en réalité d'ailleurs).

En acquérant ces compétences, les utilisateurs apprendront à exercer un jugement critique quant aux images publiées en ligne. Ils seront ainsi plus prudents à l'égard de l'ensemble des menaces.

De la même façon, le programme pourrait viser à renforcer la connaissance des précautions élémentaires à prendre en ligne (ne pas cliquer sur les liens provenant de sources inconnues et respecter les principes de base en matière de sécurité des mots de passe, notamment). Les manœuvres d'influence hostile se fondent en bonne partie sur le piratage et les fuites, donc l'enseignement des rudiments de la cyberautodéfense peut être l'occasion d'aborder la question des fuites et d'expliquer à quoi elles servent.

Sur ces fondations, la culture médiatique pourrait être abordée en même temps que les précautions générales de rigueur en ligne. Elle comprendrait la culture des médias sociaux, c'est-à-dire qu'il ne s'agirait pas seulement d'enseigner les techniques classiques permettant de reconnaître des informations incomplètes, partiales ou inexactes, mais d'aborder aussi le rôle des trolls, le harcèlement en ligne, le pistage obsessionnel, les faux comptes, et autres joyeusetés du monde virtuel.

Encore une fois, cela aurait un double objectif : renforcer la compréhension des dangers des manœuvres d'influence et inculquer les rudiments de la survie en ligne. Ce serait particulièrement important pour les parents qui (d'après ce qu'il a été possible de constater) commencent à penser qu'il est *plus risqué* pour leurs enfants de naviguer sur le Web à la maison que de marcher la nuit dans une rue mal famée.

Ainsi, bien que la culture médiatique puisse constituer un vaccin partiellement efficace contre les manœuvres d'ingérence hostile, l'enseignement de la sécurité en ligne permettrait de couvrir plus largement les différentes activités hostiles en ligne et de dispenser des conseils pratiques nettement plus utiles.

Un traitement

Il faudra adopter une autre stratégie à l'égard des collectivités ou des individus qui ont déjà accepté la version des faits, les thèmes et les allégations des fauteurs de désinformation. Pour poursuivre la comparaison avec le virus, ces populations ont déjà été contaminées. Il ne faut pas se contenter de les considérer comme un vecteur devant être isolé, il faut aussi tenter de les soigner. Cela s'annonce particulièrement difficile, et pas toujours possible. Cependant, les démocraties occidentales peuvent tirer parti de différentes expériences dans le domaine de la déradicalisation et de la réinsertion des anciens membres de sectes ou de gangs.

Il y a beaucoup d'enseignements à tirer des similitudes entre différentes manœuvres d'influence et certaines opérations de recrutement (par les djihadistes, l'extrême droite, les sectes ou les gangs). Selon l'expert en sectes Steven Hassan, celles-ci

utilisent le modèle CIPE (*BITE model*) pour garder la mainmise sur leurs recrues : elles contrôlent leur comportement, l'information à laquelle elles ont accès, leurs pensées et leurs émotions[14].

Le contrôle de l'information consiste à retenir délibérément certains éléments et à en dénaturer d'autres, ainsi qu'à décourager l'accès aux sources d'information extérieures. (On appelle parfois cela la « dépluralisation », un terme aussi utilisé dans le contexte du recrutement djihadiste[15].) Le contrôle de la pensée consiste à instiller une vision des choses sans nuances et à rejeter toute analyse rationnelle ou pensée critique.

Ces procédés sont comparables aux manœuvres d'influence du Kremlin, qui garde certaines informations et en déforme d'autres[16] et sape la crédibilité des médias grand public (campagne « Osez questionner » de Russia Today), afin de présenter une vision très tranchée des conflits dans lesquels la Russie est impliquée et de remettre en question l'idée de « reportage objectif » et de « chronologie des événements » réelle et démontrée[17].

En outre, les recruteurs de terroristes reconnaissent les personnes qui ont des ressentiments, les confortent dans cette attitude et alimentent leur dépit afin de gagner la confiance de leurs proies[18]. Ou encore, certains acteurs lancent des opérations d'information ciblant un groupe protestataire donné (comme la « droite alternative » et le mouvement Black Lives Matter aux États-Unis et les Gilets jaunes en France) et couvrent ses activités et le soutiennent sans jamais le critiquer pour mieux se donner des moyens de l'influencer.

Si ces modes de fonctionnement ne sont pas rigoureusement identiques, les procédés visant à contrôler l'information et à attiser le mécontentement sont les mêmes. Il existe des similitudes entre les méthodes de contrôle de l'information employées par les sectes, les recruteurs terroristes et les auteurs de manœuvres d'influence hostile. Les mesures visant à réinsérer les victimes des sectes pourraient donc servir d'inspiration pour ce qui est du traitement des victimes de la désinformation.

Ainsi, les gouvernements devraient envisager de faciliter les échanges entre les chercheurs qui se penchent sur les manœuvres d'influence et ceux qui se spécialisent dans la réinsertion sociale des victimes des sectes et du recrutement terroriste. Il est impossible de prédire l'issue de ces discussions ni d'affirmer que des conclusions utiles en ressortiraient, mais cette possibilité doit être étudiée.

Par ailleurs, il convient de noter que les manœuvres d'influence hostile semblent avoir eu un écho particulier dans les groupes désillusionnés : l'opération russe contre les États-Unis a remporté ses plus grands succès auprès des membres du mouvement Black Lives Matter et de la « droite alternative », et les attentats terroristes de Bruxelles et de Paris ont été perpétrés par des personnes issues de communautés immigrantes désenchantées de Bruxelles.

Par conséquent, un bon moyen de réduire l'influence des manœuvres hostiles consiste à répertorier les groupes déçus ou marginalisés, à déterminer les causes profondes de leur mécontentement et à y trouver des solutions politiques. Il est toujours honorable et utile de s'efforcer d'améliorer l'intégration sociale et d'apaiser les tensions, mais cela devient un

impératif de sécurité nationale dans un contexte où des acteurs étrangers hostiles cherchent un angle d'attaque.

De ce qui précède découle un dernier point en lien avec les sondages permanents dont il est question plus haut : les manœuvres d'influence hostile ont plus de chances d'être couronnées de succès quand leurs auteurs comprennent bien les ressorts du ressentiment des communautés qu'ils visent envers le gouvernement national.

L'une des priorités des gouvernements consistera donc à être à l'écoute de la population pour détecter rapidement les premiers signes de grogne sociale et y apporter des réponses d'ordre politique. Les sondages peuvent être effectués par des moyens traditionnels ou sur les médias sociaux, qui sont conçus spécifiquement pour recueillir des commentaires rapides sur différents moyens d'action. Il est révolu, le temps où les gouvernements pouvaient se dire qu'aucun acteur extérieur n'avait les capacités d'intervenir dans les problèmes intérieurs. Les médias sociaux ont créé un milieu sur lequel de nombreux éléments extérieurs peuvent peser aisément. La difficulté suprême pour les autorités consiste à nouer avec leurs propres citoyens un dialogue plus efficace que celui que les acteurs hostiles ont déjà amorcé.

Conclusion

Les manœuvres d'influence hostile constituent manifestement une menace pour les sociétés démocratiques. Elles peuvent être comparées à un virus, qui contamine d'abord les groupes les plus vulnérables puis met en danger la santé politique d'un pays.

Comme pour combattre un virus, il faut se doter de plusieurs moyens de riposte. Les pouvoirs publics peuvent tenter de découvrir les sources de l'infection, d'isoler les vecteurs et de vacciner la population grâce à l'éducation. Ils peuvent aussi envisager des moyens d'aider celles et ceux qui ont déjà été contaminés, notamment en exploitant les similitudes avec la lutte contre la radicalisation et contre la mainmise des sectes.

Tous ces efforts nécessitent de mieux connaître, en détail, le fonctionnement de l'écosystème national de l'information. Les manœuvres d'influence hostile sont efficaces quand leurs auteurs comprennent le public cible. Les gouvernements qui ne cherchent pas à comprendre leur propre population mieux que les acteurs hostiles manquent à leurs devoirs.

Notes

[1] Il convient de rappeler que l'Agence de recherche sur Internet russe a commencé par cibler l'opposition nationale en 2013 et qu'elle ne s'est attaquée aux États-Unis qu'en 2014.

[2] Bellingcat.com

[3] Graphika.com

[4] FireEye.com

[5] Disinfo.eu

[6] Integrityinitiative.org

[7] Kremlinwatch.eu

[8] Medium.com/dfrlab

[9] L'utilisation de l'adjectif « viral » au sujet d'une publication qui se propage partout sur Internet relève de la même comparaison.

[10] Cela atteint des sommets dans les cas de radicalisation menant à l'extrémisme islamisme ou à l'extrême droite, les personnes influencées demeurant indétectables jusqu'à ce qu'elles commettent un attentat.

[11] Il est possible de se faire une idée de la réaction des différentes communautés en consultant les publications russes archivées et présentées sur medium.com/@ushadrons.

[12] Jack Stubbs et Christopher Bing, « Exclusive: Iran-based political influence operation: bigger, persistent, global », Reuters, 29 août 2018.

[13] C'est le sort qui a été réservé au site Fancy Bears, qui était utilisé par les services de renseignement militaire russes pour publier des documents piratés. Voir fancybear.org.

[14] Steven Hassan, *BITE model*, Freedom of Mind Resource Center, non daté. Consulté à https://freedomofmind.com/bite-model/.

[15] *What is radicalisation?*, European Institute of Peace. Consulté à http://www.eip.org/en/news-events/eip-explainer-understanding-radicalisation.

[16] Voir par exemple les nombreuses décisions rendues par OfCom, l'organe britannique de réglementation des communications, contre Russia Today pour violation des normes d'impartialité, les dernières en date remontant à décembre 2018. Consultées à https://www.ofcom.org.uk/__data/assets/pdf_file/0020/131159/Issue-369-Broadcast-and-On-Demand-Bulletin.pdf.

[17] Peter Pomerantsev et Michael Weiss, « The Menace of Unreality », *The Interpreter*, novembre 2014. Consulté à : http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf.

[18] J.M. Berger, *Tailored Online Interventions: The Islamic State's Recruitment Strategy*, Combating Terrorism Center, octobre 2015.