Service canadien du renseignement de sécurité

Canadian Security Intelligence Service

QUI DIT QUOI?

Défis sécuritaires découlant de la désinformation aujourd'hui

POINTS SAILLANTS DE L'ATELIER

Canada

Pensez à recycler

Ce document est imprimé avec de l'encre sans danger pour l'environement

Publication nº 2018-02-01 de la série *Regards sur le monde : avis d'experts*

Le présent rapport est fondé sur les opinions exprimées par les participants et les exposants, de même que sur de courts articles offerts par les exposants à l'occasion d'un atelier organisé par le Service canadien du renseignement de sécurité dans le cadre de son programme de liaison-recherche. Le présent rapport est diffusé pour nourrir les discussions. Il ne s'agit pas d'un document analytique et il ne représente la position officielle d'aucun des organismes participants. L'atelier s'est déroulé conformément à la règle de Chatham House; les intervenants ne sont donc pas cités et les noms des conférenciers et des participants ne sont pas révélés.

www.scrs-csis.gc.ca

Publié en février 2018
Imprimé au Canada

Crédit photo : gettyimages.com

QUI DIT QUOI?

DÉFIS SÉCURITAIRES DÉCOULANT DE LA DÉSINFORMATION AUJOURD'HUI

POINTS SAILLANTS DE L'ATELIER

TABLE DES MATIÈRES

L'ATELIER ET SES OBJECTIFS

Le 20 novembre 2017, le programme de liaison-recherche du Service canadien du renseignement de sécurité (SCRS) a tenu un atelier au cours duquel un groupe multidisciplinaire d'experts du Canada, des États-Unis et d'Europe se sont penchés sur les conséquences stratégiques de la désinformation pour la sécurité nationale et l'intégrité des institutions démocratiques.

Tenu selon la règle de Chatham House, l'atelier a donné l'occasion aux conférenciers et aux participants d'explorer la manipulation de l'information à des fins politiques et autres, de se pencher sur des cas récents ainsi que de discuter des façon de contrer les menaces pour la sécurité aujourd'hui et demain. Les conférences données à l'atelier composent l'essentiel du présent rapport. Les opinions qui y sont exprimées appartiennent à ces experts indépendants et ne sont pas celles du SCRS.

Lancé en 2008, le programme de liaison-recherche du SCRS a pour objectif de favoriser un dialogue entre des professionnels du renseignement et d'éminents experts aux origines culturelles variées qui œuvrent dans différentes disciplines au sein d'universités, de groupes de réflexion, d'entreprises privées ou d'autres établissements de recherche, au Canada et à l'étranger. Il se peut que certains spécialistes invités défendent des idées ou tirent des conclusions qui ne concordent pas avec les points de vue et les analyses du SCRS, mais c'est précisément ce qui rend utile la tenue d'un tel dialogue.

SOMMAIRE

La portée et la rapidité d'Internet et des médias sociaux ont amplifié les répercussions possibles de la désinformation. L'augmentation de la capacité de transmission de données, jumelée au virage vers la publicité programmatique[1], a provoqué une diminution abrupte de la capacité du journalisme traditionnel d'être le garant de la qualité de l'information publique. Ce dernier a été remplacé en partie par un torrent de données provenant d'un nombre infini d'expéditeurs. Or, ce torrent charrie son lot de mensonges et de distorsions qui menacent l'intégrité du discours public, des débats et de la démocratie.

Agents de désinformation : les acteurs

La désinformation est devenue un outil extrêmement efficace pour les acteurs étatiques, les profiteurs, les personnes en quête d'un statut, les entreprises du spectacle et les vrais croyants. Le plus habile pourvoyeur étatique de mensonges est la Russie. Sa maîtrise historique de ce qu'on appelle les mesures spéciales, magnifiée par la technologie moderne, respecte le principe opérationnel de base, c'est-à-dire *diffamer et amplifier*.

- L'adhocratie russe, l'élite changeante qui entoure le président Vladimir Poutine, dirige un vaste réseau de trolls et des réseaux de zombies qui génèrent et propagent du matériel partout sur le Web. Le soutien de diplomates, d'organes médiatiques d'État comme RT (Russia Today) et Sputnik ainsi que des alliances de fait avec des organisations comme WikiLeaks intensifient ses activités.

- En collaborant, ces agents de l'État russe parviennent à créer une fausse histoire et, au moyen de Facebook, de Twitter et d'autres canaux, font en sorte qu'elle atteigne le segment de la population qu'elle est le plus susceptible d'influencer. Ils donnent aussi l'impression de corroborer l'histoire grâce à des entrevues réalisées par des agences de presse auprès de faux experts, à des documents contrefaits ainsi qu'à des photos et à des vidéos retouchées. Quiconque dénonce les mensonges devient la cible d'une campagne massive de diffamation en ligne.

- La Russie, la Chine et les Philippines emploient des techniques de désinformation pour contrôler leur population interne. 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.

Moscou et Beijing ont élaboré des doctrines d'information complexes dans le cadre de leur stratégie visant à consolider leur emprise sur la scène intérieure et à servir leurs objectifs en matière de politique étrangère. Ils coordonnent des messages sur de multiples plateformes et avancent des arguments cohérents par l'entremise des médias traditionnels et des médias sociaux dans de nombreuses langues. La désinformation sert des objectifs stratégiques immédiats et à long terme. Il existe toutefois des différences importantes entre les méthodes russes et chinoises.

- La Russie essaie de modifier la perception de la réalité et cerne les divisions exploitables au sein de ses publics cibles. Elle fait la promotion d'un programme plus nationaliste qu'idéologique et cible la population russe pour éviter la dissidence. Elle attaque les anciens membres de l'URSS qui la côtoient au moyen de messages qui pourraient, en fin de compte, soutenir une guerre hybride. Les opérations menées contre les populations occidentales visent à affaiblir la résistance aux objectifs de l'État russe. Dans la campagne qu'elle a menée à l'appui de la Syrie, elle a employé la désinformation pour dissimuler la brutalité de ses attaques contre les populations civiles.

- La Chine a créé une cyberforteresse intérieure et l'a renforcée au moyen des technologies et des entreprises de haute technologie chinoises. Les messages lancés à l'échelle nationale et internationale sont à la fois nationalistes et idéologiques. Beijing déploie sa version de la puissance douce pour influencer les politiques de la communauté internationale, c'est-à-dire qu'elle utilise efficacement sa puissance économique et la présence de communautés et d'entreprises chinoises dans des pays suscitant un intérêt.

- La Russie a militarisé explicitement sa machine de désinformation pour qu'elle serve de ressource dans les guerres de demain : elle atténue le sentiment de danger d'un pays ciblé et affaiblit la volonté de résister. La Chine se bat pour la reconnaissance de sa légitimité à titre de grande puissance tout en rejetant les normes internationales avec lesquelles elle n'est pas d'accord.

D'autres acteurs participent aussi au flot de désinformation.

- Aux Philippines, la désinformation a servi de tactique pour influencer les électeurs lors des élections présidentielles, justifier la campagne antidrogue menée dans les rues, discréditer les détracteurs du régime et délégitimer les médias grand public.

- Pendant la campagne référendaire sur le Brexit, un très grand nombre de comptes Twitter étaient actifs, particulièrement dans le camp favorable à la sortie de l'Union européenne. La plupart ont disparu immédiatement après le vote, ce qui donne fortement à penser qu'ils étaient pilotés par des robots. Leur contenu correspondait au style simpliste et hyperpartisan des tabloïdes britanniques.

Nouveaux activistes indépendants

Les agences de désinformation des États font partie d'un système complexe qui comprend des activistes indépendants dont les motivations diffèrent, mais se chevauchent. Beaucoup voient des complots dans les événements qui font les manchettes, comme les fusillades, ou même nient qu'ils ont jamais eu lieu. Ils croient que les gouvernements ne sont pas dignes de confiance, qu'ils manipulent les événements qui surviennent dans le monde et qu'ils peuvent compter sur l'aide des médias traditionnels pour dissimuler la vérité. La plupart sont antimondialistes et tiennent un discours nationaliste et anti-immigration qui plaît aux éléments de la gauche et de la droite.

Des acteurs indépendants utilisent les médias sociaux et des sites Web spécialisés pour propager et renforcer stratégiquement des messages compatibles avec les leurs. Des organismes de désinformation

des médias d'État infiltrent et utilisent leurs réseaux pour amplifier l'effet des stratégies de désinformation de l'État contre les populations ciblées. Dans ce système complexe, il est difficile de savoir dans quelle mesure et par qui les activités sont orchestrées.

Agents de désinformation : les complices

L'écosystème informationnel permet la tenue de campagnes de désinformation d'envergure. Les fausses nouvelles sont propagées de multiples façons, mais Facebook et Twitter sont des outils particulièrement importants. Ils servent tous les deux à cibler des segments précis de la population. Les personnes qui considèrent les fausses nouvelles comme dignes de foi ou utiles les propagent à leur tour. Les organismes d'État ont abondamment recours aux robots et aux faux comptes pour populariser de faux reportages et les propager en cascade, atteignant des volumes qu'il est humainement impossible de produire ou de maîtriser individuellement.

Les entreprises de médias sociaux prennent conscience de leur rôle dans le problème, mais les dirigeants de la Silicon Valley ne sont pas tous convaincus qu'il leur incombe d'éliminer les fausses informations. La lutte contre les pourriels est une nécessité commerciale, mais la fermeture de comptes ou la vérification de contenus limitent la rentabilité. Les entreprises de médias sociaux ont un engagement philosophique à l'égard de l'échange ouvert des informations, et beaucoup ont une compréhension limitée du monde des opérations de renseignement. Elles sont réticentes à s'allier aux services de renseignement et aux organes de presse grand public pour assumer la tâche de surveiller le contenu en détail.

Désinformation à la russe : les messages

La désinformation d'origine russe est adaptée aux circonstances et aux objectifs de l'État, mais elle comporte d'importants thèmes récurrents selon lesquels, par exemple, les gouvernements occidentaux sont fascistes ou les leaders mondiaux font partie d'une élite puissante qui méprise les gens ordinaires et agit contre eux.

À ces thèmes généraux s'ajoutent ceux qui appuient des campagnes précises, comme les activités de la Russie pour soutenir le Parti républicain dans la campagne présidentielle de 2016 aux États-Unis.

La réaction

De nombreux acteurs et organismes travaillent pour contrer cette menace et se protéger contre elle.

- Les gouvernements insistent de plus en plus pour que les entreprises de médias sociaux assument la responsabilité du contenu dont elles facilitent la propagation. Sur ce plan, les législateurs européens ont une longueur d'avance sur leurs homologues américains, en partie parce que les médias sociaux sont très utilisés par les terroristes.
- Certains gouvernements ont pris des mesures pour bloquer les flux connus des médias de désinformation dans leur pays, protégeant leurs citoyens contre les tentatives d'ingérence étrangère.
- De nombreuses universités et de multiples groupes de recherche privés ont analysé des campagnes de désinformation, au moyen de modèles de diffusion et d'indicateurs de contenu pour repérer les réseaux de zombies et les usines de trolls.
- Des organisations spécialisées sont devenues habiles pour ce qui est de dévoiler les faux reportages et, souvent en temps réel, de sensibiliser le public pour qu'il apprenne à détecter et à démasquer la désinformation.

Perspectives

Les répercussions négatives des fausses nouvelles sur la démocratie pourraient s'accroître si la Russie et d'autres acteurs deviennent des modèles pour d'autres, ce qui augmenterait la diffusion de messages malveillants par toutes les voies offertes par l'ère de l'électronique.

La désinformation empoisonne le débat public et menace la démocratie. Il est nécessaire de sensibiliser davantage la population

au problème pour qu'elle apprenne à distinguer le vrai du faux. Les gouvernements et les organisations disposent de nombreuses façons de contrer la menace, mais rien ne garantit que des contre-campagnes, même efficaces, peuvent neutraliser le flux à grand débit des communications malveillantes.

CHAPITRE 1

ÉVÉNEMENTS ORCHESTRÉS OU NOUVELLE TENDANCE? COMPRENDRE LA COMPLEXITÉ DE LA DÉSINFORMATION EN LIGNE

La désinformation est propagée par un réseau complexe d'acteurs souvent indépendants. Bon nombre véhiculent des théories du complot ou des canulars, unis par leur méfiance à l'égard des gouvernements occidentaux et des médias grand public. Leur discours, qui séduit des gauchistes hostiles à la mondialisation et à l'intervention militaire ainsi que des nationalistes opposés à l'immigration, est fréquemment infiltré et façonné par des trolls étatiques et par des reportages retouchés d'agences comme RT et Sputnik. On observe diverses motivations pour participer à la propagation de la désinformation.

Tous les jours ou presque, de nouvelles informations révèlent l'ampleur de l'utilisation, par le gouvernement de la Russie, des médias sociaux et d'autres outils en ligne pour s'ingérer dans le processus démocratique aux États Unis, au Royaume-Uni et ailleurs. Ces révélations mettent en lumière une stratégie multidimensionnelle qui allie techniques évoluées et méthodes rudimentaires pour produire et diffuser de la désinformation. Elles laissent aussi croire à l'existence d'un système complexe au sein duquel ces techniques trouvent un écho auprès de divers acteurs distincts et indépendants, dont elles dictent les activités.

L'examen de la prolifération des théories du complot entourant les attentats terroristes et les fusillades aux États Unis permet de mieux comprendre la dynamique complexe qui sous tend cette forme de désinformation. Par exemple, une rumeur selon laquelle l'attentat à la bombe contre le marathon de Boston était une opération clandestine (black ops) perpétrée par le gouvernement des États Unis a circulé en ligne. Les utilisateurs de Reddit et de Twitter ont émis l'hypothèse que la fusillade commise en 2015 sur le campus de l'Umpqua Community College (tout comme la tuerie à Sandy Hook trois ans plus tôt) était un canular élaboré par le gouvernement pour justifier

l'adoption de lois sur le contrôle des armes à feu. De même, la fusillade d'octobre 2017 à Las Vegas a été perçue comme une opération menée sous faux pavillon par des membres du « nouvel ordre mondial », une coterie de conspirateurs qu'on dit contrôler la marche du monde.

Bien qu'elles soient toutes distinctes dans une certaine mesure, les théories du complot s'inscrivent dans une logique d'allégations de crises anthropiques et se rejoignent dans quelques thèmes ou discours sous jacents :

- le gouvernement des États Unis et d'autres gouvernements occidentaux ou affiliés à l'OTAN ne sont pas dignes de confiance. Ce sont des agresseurs dont l'intervention dans les conflits mondiaux est injustifiée;
- ces gouvernements et d'autres personnes puissantes manipulent les événements mondiaux pour conserver le pouvoir; et
- les médias grand public et les médias privés ne sont pas fiables. Ils aident les gouvernements et d'autres acteurs puissants à cacher la vérité à la population en diffusant de « fausses nouvelles ».

Bon nombre de ces discours sont explicitement liés à une vision antimondialiste ou nationaliste du monde. Le terme « mondialisme » est apparenté au terme « mondialisation », qui sert à caractériser des perspectives transnationales[2] et des politiques favorables au libre échange et à l'ouverture des frontières[3]. Dans les faits, le terme « antimondialiste » mobilise autour d'une cause commune des personnes qui semblent être aux antipodes sur l'échiquier politique. Le discours antimondialiste relie entre eux, par exemple, des partisans de la gauche, qui dénoncent la mondialisation et l'intervention militaire à l'étranger des États Unis et d'autres pays membres de l'OTAN, et des tenants de la droite, qui s'opposent à l'immigration et favorisent les politiques nationalistes.

En examinant de la prolifération de ces théories du complot et des discours connexes, on voit comment les États qui parrainent des opérations d'information exploitent les communautés organiques d'utilisateurs en ligne pour propager la désinformation.

À titre d'exemple, considérons la tuerie perpétrée le 5 novembre 2017 dans une église d'un petit village du Texas, qui a coûté la vie à plus de vingt personnes. Dans les heures qui ont suivi, les autorités et les médias grand public ont communiqué l'identité du suspect, un homme de 26 ans qui avait des antécédents de violence conjugale et qui avait été réformé de l'Armée de l'air des États Unis. Toutefois, avant que cette nouvelle n'ait été étoffée, et même après qu'elle eut été corroborée, on prétendait, dans une autre version des faits, que le suspect était en réalité un terroriste du groupe Antifa[4]. Souhaitant promouvoir cette version, des activistes en ligne de la droite politique ont trafiqué des captures d'écran du profil Facebook du tireur afin d'y insérer un drapeau d'Antifa et, par le fait même, d'ajouter foi à cette théorie, puis se sont servi des médias sociaux pour diffuser ce contenu. La théorie s'est vite répandue dans la twittosphère entre les partisans de la droite alternative, dont Mike Cernovich, blogueur populaire, qui a indiqué dans son gazouillis que les détails concernant le tueur cadraient avec le profil d'un membre d'Antifa. Alex Jones, personnalité des médias de droite connue pour sa propension à propager des théories du complot, a fait remarquer que le tueur était tout de noir vêtu (signe qu'il s'agissait d'un activiste de gauche). Cette théorie a également été diffusée dans la presse parallèle, sur des sites Web comme TheGatewayPundit, YourNewsWire et BeforeItsNews. La chaîne d'information télévisée RT (anciennement Russia Today), financée par le gouvernement de la Russie, a aidé à propager cette allégation en partageant sur Facebook un message faisant état des liens du tueur avec Antifa, accompagné du contenu du profil Facebook trafiqué.

> *(…) les États qui parrainent des opérations d'information exploitent les communautés organiques d'utilisateurs en ligne pour propager la désinformation.*

Cela s'inscrit dans une tendance maintenant bien établie, celle des activités en ligne menées à la suite de tueries. Selon de récentes études, certaines des conversations initiales entourant ces théories se dérouleraient sur des plateformes Web comme Reddit, 4chan, Discord et autres[5], dont la visibilité est moindre, et dont les intervenants jouissent par conséquent d'un anonymat accru. Ces théories sont ensuite diffusées et amplifiées, parfois de manière stratégique, sur Twitter et Facebook. En outre, un écosystème de sites Web connexes se crée autour de ces conversations conspirationnistes et les soutient en y ajoutant hypothèses, analyses et preuves sous diverses formes[6]. Cet écosystème est surtout constitué de médias parallèles qui prétendent contester les nouvelles publiées dans les médias grand public. Il comprend plusieurs sites Web et blogues qui font la promotion de théories du complot et d'allégations pseudo scientifiques (p. ex. InfoWars, 21stCenturyWire et SecretsOfTheFed). Fait important, de nombreux sites Web de cet écosystème ne font que regrouper les nouvelles, c'est à dire qu'ils remanient du contenu trouvé ailleurs et le republient dans l'écosystème (p. ex. BeforeItsNews et YourNewsWire). Le système contient aussi quelques sites Web destinés explicitement aux nationalistes et aux suprémacistes blancs (DailyStormer) ou, en apparence, aux activistes de gauche (ActivistPost) qui véhiculent des messages parallèles sur les tueries commises en 2016. Les sites Web de la chaîne RT et de l'agence de presse Sputnik financées par la Russie font aussi partie de cet écosystème, tout comme PressTV de l'Iran.

Il reste à déterminer comment s'emboîtent les différents éléments de ce système dynamique qui consiste à lancer des théories, puis à les amplifier et à les propager. On ne sait pas encore au juste dans quelle mesure ces activités représentent une nouvelle tendance ou sont orchestrées (le cas échéant, par qui et pourquoi). Toutefois, il semble y avoir différents intervenants dont les sources de motivation diffèrent tout en se chevauchant. Voici, en guise de cadre conceptuel préliminaire, six catégories dans lesquelles s'inscrivent ces sources de motivation.

Idéologie sincère. Un ensemble d'acteurs dans ce système est motivé par des considérations idéologiques. Ces acteurs, dont des utilisateurs

des médias sociaux et de petites organisations qui exploitent des sites Web, des blogues et d'autres fils de nouvelles croient vraiment aux messages qu'ils diffusent. Il s'agit en règle générale de messages antimondialistes (les partisans de la gauche diffusent des messages anti impérialistes et antimondialisation, et les partisans de la droite, des messages pronationalistes et anti immigration). Ces acteurs sont aussi très explicites dans leurs critiques et leur méfiance à l'égard des médias grand public. Ils peuvent effectivement être influencés par la propagande politique, bien que la relation de cause à effet soit difficile à établir. Parfois, ils peuvent être perçus comme de simples intervenants qui se contentent de relayer la propagande politique en l'amplifiant au passage. Cependant, de nombreux acteurs réellement motivés par des considérations idéologiques produisent leur propre contenu sans éprouver constamment le besoin de l'introduire directement ailleurs ou de le coordonner avec d'autres messages.

On observe différents intervenants dont les sources de motivation diffèrent tout en se chevauchant.

Propagande politique. Il est possible de considérer que les activités du deuxième groupe d'acteurs dans ce système, notamment la production, le partage et l'amplification délibérés de la désinformation, s'inscrivent dans une stratégie politique. Contrairement aux acteurs motivés par des considérations idéologiques, ceux-ci ne croient pas nécessairement le contenu des messages qu'ils partagent. Ils entremêlent faits et fausses informations dans leurs messages et associent intentionnellement à leurs propres discours d'autres histoires et messages qui sont souvent susceptibles d'intéresser les acteurs motivés par des considérations idéologiques. Ces acteurs aux motivations politiques se servent du potentiel qu'offre l'ère de l'information pour adapter de vieilles stratégies de désinformation. Ils exploitent l'infrastructure technologique d'Internet pour diffuser leurs messages plus rapidement, à un auditoire plus vaste et à un coût plus faible que jamais auparavant. Pomerantsev et Weiss[7] ont signalé dans leurs écrits que la désinformation ne vise pas nécessairement à convaincre, mais à semer la confusion, c'est à dire brouiller l'esprit des gens et attiser la méfiance à l'égard de l'information et de ceux

qui la fournissent. Des signes donnent à penser que cette stratégie entre en jeu dans l'écosystème à l'étude. Un autre objectif de la désinformation est de créer des divisions au sein des démocraties qui s'opposent et de les amplifier, phénomène également présent dans le système.

Incitatifs financiers. D'autres acteurs de ce système sont motivés par des considérations d'ordre financier. Par exemple, de nombreux sites Web vendent de la publicité et des produits de santé. Bon nombre d'entre eux se contentent essentiellement de regrouper des pseudo-médias (ou médias parallèles), en régurgitant du contenu destiné à attirer les utilisateurs (des pièges à clics). D'autres, comme InfoWars, intègrent du contenu original à du contenu emprunté à d'autres sites de l'écosystème, dont celui de RT, et utilisent leur plateforme pour faire le trafic d'une gamme de produits (p. ex. des suppléments nutritifs).

Accroissement de la réputation. Un autre ensemble d'acteurs, notamment dans la sphère des médias sociaux, semble être motivé par l'attention et l'accroissement de la réputation que leur offrent ces plateformes. Les médias sociaux sont conçus de manière à être interactifs, c'est à dire à favoriser une rétroaction circulaire au moyen des fonctions J'aime et Suivre. Dans le monde de la désinformation, notamment chez les partisans de la droite alternative, il semble exister des acteurs qui sont principalement (ou, du moins, dans une large mesure) motivés par l'attention qu'ils obtiennent et la réputation accrue qu'ils croient pouvoir acquérir. Mike Cernovich et Jack Posobiec sont deux exemples bien connus, mais beaucoup d'autres représentants de l'élite de l'externalisation ouverte sur Twitter et ailleurs propagent des messages parallèles et d'autres formes de désinformation politisée et jouissent donc d'une grande visibilité en ligne.

Même si les preuves empiriques à cet effet ne sont pas encore très nombreuses, les deux dernières catégories, qui sont plus conceptuelles, font probablement partie de l'écosystème complexe décrit précédemment.

Divertissement. Certaines personnes font probablement de la désinformation simplement « pour les lulz », comme dirait le groupe Anonymous dont la popularité décline. Ce slogan, qui signifie « pour la rigolade », visait à décrire une forme de plaisanterie espiègle propre aux activités en ligne. Une autre façon de comprendre cette catégorie consiste à étendre au monde réel les pratiques du jeu en ligne. Par exemple, la désinformation peut servir de plateforme de collaboration avec les membres d'une équipe en ligne et de moyen de s'engager dans des missions de piratage culturel (pour propager certaines idéologies).

Autonomisation. La désinformation peut offrir à une personne ou à un groupe privés de droits la possibilité d'exercer de l'influence ou du pouvoir dans le monde au moyen de ses actions en ligne. Cette catégorie comprend les habitués du forum 4chan, qui utilisent la production et la propagation de mèmes graphiques[8] comme armes pour amener des changements politiques dans le monde. Tout comme les bénévoles qui ont l'impression de faire une différence en s'unissant en ligne après des catastrophes pour venir en aide à des personnes, ces acteurs sont motivés par l'idée de collaborer au sein d'une équipe en ligne pour défendre une cause (p. ex. l'élection du candidat qu'ils favorisent). Toutefois, la cause en tant que telle les motive peut être moins que la gratification émotionnelle qui découle du fait d'avoir eu une incidence.

Ces dernières sources de motivation et les acteurs qui leur sont associés ne sont pas sans importance. Selon des études préliminaires, non seulement les stratégies de désinformation intentionnelles exploitent le pouvoir des plateformes de médias sociaux, mais elles trouvent un écho auprès des communautés en ligne qui se forment au sein de ces plateformes. Par exemple, des trolls établis en Russie se faisant passer pour des Américains se sont servis de leurs comptes pour infiltrer les communautés en ligne d'utilisateurs de Twitter de la droite alternative et afin de lancer et d'amplifier leurs messages pendant le cycle électoral de 2016 aux États Unis. Ils ont également infiltré les communautés de gauche qui se sont formées sur la twittosphère autour d'enjeux tels que #BlackLivesMatter dans le but

d'attiser les divisions qui existent aux États Unis. Par ailleurs, les communautés d'activistes en ligne qui se forment autour d'idéologies d'opposition à la guerre ont été la cible d'opérations d'information liées à la Russie qui visaient à diffuser des messages remettant en cause les activités des États Unis et de l'OTAN en Syrie.

S'ils se concentrent sur les activités de coordination explicites d'acteurs étatiques et de collusion avec ces derniers et sous estiment ou négligent les rôles et les motivations de ces acteurs indépendants, les chercheurs, les journalistes et les décideurs risquent de simplifier à outrance ce système complexe, de nuire à l'élaboration de solutions efficaces et de ne pas sensibiliser suffisamment le public au problème. Ils se trouvent ainsi, et c'est là un fait important, à rater l'occasion d'aider les utilisateurs ordinaires de ces systèmes à reconnaître le rôle qu'ils jouent dans le phénomène de la désinformation. Autrement dit, le problème de la désinformation ne peut être simplement attribué à la conception des systèmes technologiques ou aux actions délibérées de trolls financés par des gouvernements. Pour régler le problème, il est aussi nécessaire de tenir compte des gens qui utilisent ces informations ou sur lesquels ces informations ont une incidence, et ce, non seulement à titre de victimes, mais aussi à titre d'agents ayant un rôle dans la création et la propagation du problème et (il est à espérer) dans la recherche d'une solution.

CHAPITRE 2

LA RUSSIE, L'OCCIDENT ET LES ASPECTS GÉOPOLITIQUES DE LA DÉSINFORMATION

La campagne de désinformation menée par le Kremlin et par les réseaux d'oligarques qui y sont liés descend en droite ligne des « mesures actives » du KGB, et la technologie moderne ne fait qu'en augmenter l'ampleur, la vitesse et la puissance. Elle vise à contrôler l'opinion publique en Russie et à miner les démocraties occidentales en fomentant des divisions à l'intérieur de groupes ciblés. Des pirates informatiques, des usines de trolls et des sites Web largement dispersés masquent en partie l'origine commune de nouvelles fausses et déformées.

Un siècle et demi avant que le directeur du KGB, Iouri Andropov, ne fasse de la désinformation un élément central des activités de renseignement des Soviétiques[9], William Blake signalait qu'« une vérité que vous énoncez avec de mauvaises intentions bat tout mensonge que vous pouvez inventer »[10]. Toute désinformation à proprement parler contient fondamentalement des bribes de vérité communiquées avec de mauvaises intentions, et c'est la raison pour laquelle elle est aussi difficile à endiguer.

Dans la présente analyse, plutôt que les mots « Russes » ou « Russie », le terme « Kremlin » ou d'autres termes liés à Vladimir Poutine et à ses acolytes serviront, dans la mesure du possible, à désigner l'adversaire. Personne n'a intérêt à ce que les activités du Kremlin soient présentées comme un conflit entre la Russie et l'Occident. En fait, le principal adversaire du Kremlin a toujours été et demeure la Russie. Pratiquement toutes les mesures prises par le Kremlin contre l'Occident ont d'abord été mises en œuvre en Russie, contre le peuple russe et contre de nombreuses minorités ethniques, nationales et religieuses. Le Kremlin comprend non seulement l'administration présidentielle, mais aussi les réseaux de chefs d'entreprises, de caïds du crime organisé, d'anciens officiers et d'agents et de sources des services de renseignement soviétiques qui ont un lien avec Poutine

et ses plus proches collaborateurs. Cet État à l'intérieur d'un État, qui influe sur les éléments officiels du gouvernement de la Fédération de Russie tout en restant indépendant, a été qualifié d'adhocratie[11]. L'administration présidentielle vit un roulement de personnel constant; les gens accomplissent ce qu'on demande d'eux, puis tour à tour, acquièrent ou perdent la couverture – ou l'air de légitimité – que peut leur offrir une association directe avec l'État russe.

> *(...) le principal adversaire du Kremlin a toujours été et demeure la Russie.*

Peu importe l'entité qui s'y livre, la désinformation constitue une forme agressive de marketing de l'information à l'appui d'objectifs politiques. Le modèle axé sur la segmentation, le ciblage et le positionnement est un élément fondamental de la recherche en marketing et des pratiques connexes depuis au moins les années 1970[12] . Les médias sociaux augmentent de façon radicale la quantité d'informations permettant de cerner des segments de marché et de mettre au point le contenu le plus susceptible d'influencer le public cible. En l'occurrence, la nouveauté ne repose pas tant sur les techniques que sur la facilité et la rapidité avec lesquelles la désinformation peut être dirigée simultanément vers différents segments de la population d'un pays, et ce, à très peu de frais, sans surveillance ni réglementation gouvernementale, ou presque. Un autre facteur important entre en jeu, à savoir la naïveté des entreprises technologiques, des futurologues, de la population en général et des décideurs publics, qui n'arrivent pas à saisir tout à fait le préjudice qu'un adversaire peu scrupuleux peut causer aux démocraties occidentales.

Essentiellement, les méthodes de désinformation s'apparentent aux pratiques de marketing modernes. Toutefois, les objectifs politiques visés et l'absence de contraintes morales ou éthiques les différencient et en sont au cœur. Andropov lui même a défini ainsi la désinformation en fonction de ses effets observables : « La désinformation, c'est comme la cocaïne. Consommée une fois ou deux, elle ne risque pas

de changer votre vie. Toutefois, une consommation quotidienne fera de vous un toxicomane, et donc, une tout autre personne »[13].

Andropov voulait peut-être laisser entendre que la désinformation comportait un aspect physiologique, c'est à dire qu'elle pouvait retenir l'attention et compromettre la capacité mentale de ceux qui la consomment. Il s'agit toutefois d'une question qui mérite d'être approfondie. C'est comme si le cerveau humain comportait un « récepteur de la désinformation » qui, une fois stimulé, le convainc qu'il en veut davantage. En raison de leurs nombreux effets, négatifs pour la plupart, la communication par ordinateur et les expériences connexes viennent sans doute amplifier ce présumé aspect physiologique de la désinformation. L'histoire de l'emploi du terme « désinformation » par les Soviétiques constitue en soi un exemple de désinformation. Il a bel et bien été inventé en Russie, mais, au début des années 1950, les services de renseignement de l'Union soviétique et leurs alliés ont reçu l'ordre de propager la rumeur selon laquelle le terme était d'origine française et décrivait une arme de la guerre de l'information déployée par l'Occident capitaliste contre l'URSS et les démocraties populaires partout dans le monde[14].

Le Kremlin demeure sans contredit un adversaire de l'Occident. Poutine et ses acolytes sont les enfants d'Andropov, ayant été recrutés par le KGB dans les années 1970 dans le cadre des efforts réalisés par Andropov pour régler les nombreux problèmes qui accablaient l'État soviétique en apportant du sang neuf et des idées nouvelles[15]. Même si la technologie de l'information en général et le Web en particulier créent de nouvelles occasions de pratiquer la désinformation, les règles du jeu n'ont pas beaucoup changé. À l'instar des normes du jazz, qui demeurent reconnaissables peu importe les musiciens et les arrangements, les campagnes de désinformation finissent par se ressembler. Lors de l'éclatement de l'Union soviétique, les services de renseignement occidentaux avaient déjà accumulé une somme impressionnante de connaissances relatives à la désinformation et aux techniques plus vastes connues sous le nom de « mesures actives ». Les défections qui ont suivi la chute du bloc communiste et la déclassification d'anciens rapports secrets permettent d'aborder cette

nouvelle ère d'antagonisme en comprenant bien mieux ce que fait le Kremlin, comment il s'y prend et à quelles fins.

L'objectif des mesures actives n'était pas la collecte de renseignements, mais bien la subversion. Elles visaient à fragiliser les pays occidentaux de l'intérieur ainsi qu'à fomenter des divisions entre ces pays, entre les pays membres de l'OTAN et les États neutres d'Europe et entre les pays développés d'Europe et d'Amérique et les pays en développement d'Asie, d'Afrique et d'Amérique latine[16]. Les mesures actives des Soviétiques visaient les dirigeants politiques, d'autre figures influentes, les médias, les chefs d'entreprises et les membres du grand public des pays occidentaux. Les méthodes employées allaient bien au delà du simple marketing de l'information ou de la simple promotion de l'idéologie communiste. De fausses informations délibérément destinées à tromper ont été publiées dans les médias; des documents volés ou falsifiés ont été diffusés grâce à des intermédiaires de confiance; les mouvements politiques perturbateurs ont été dotés de moyens d'action plus efficaces ou ont purement et simplement été créés; des experts ont été formés pour influencer les politiques de manière à servir les intérêts du Kremlin. Les couvertures diplomatiques, commerciales, universitaires et journalistiques ont été utilisées de façon audacieuse. Autant les mesures actives ne peuvent être dissociées de la désinformation, autant elles font partie intégrante des méthodes de gouvernance du Kremlin[17]. Plus ça change, plus c'est pareil.

Cependant, l'adhocratie actuelle au Kremlin offre de nouvelles possibilités à l'Occident, auparavant aux prises avec un État soviétique monolithique. Malgré toute l'attention accordée à une seule usine de trolls du Kremlin à Saint Pétersbourg, il est possible de constater qu'une bonne partie de ce qui peut être observé en matière de désinformation et de mesures actives en ligne peut tout aussi bien provenir, par exemple, d'une agence de publicité de Zurich. À la demande d'officiers actuels du renseignement militaire russe (GRU) à Moscou, un club de « journalisme patriotique » à Omsk, en Russie, peut créer un site Web parallèle qui prétend couvrir les conflits au Moyen Orient. Les femmes à Omsk, qui relèvent d'un conseil d'administration formé d'anciens officiers des Spetsnaz du GRU, ont

recours aux services de pirates informatiques d'origine russe en Espagne qui disposent de serveurs dans un centre de données à Amsterdam et d'une adresse de complaisance à Hong Kong, et ce, en vue de mettre en ligne un site Web à l'intention d'une équipe dont les membres ont été recrutés parmi des analystes à la retraite de services de renseignement de signataires du Pacte de Varsovie. Ce scénario n'est pas rare, et même s'il peut être long de remonter la filière jusqu'à Moscou, la nature hétérogène du personnel impliqué dans de telles opérations a pour conséquence que les techniques employées ne sont pas uniformes, parfois même peu systématiques, ce qui ouvre la porte à des enquêtes[18].

L'attrait pour la désinformation semble être directement lié à l'attrait pour l'autoritarisme.

Que faut il faire? Il existe plusieurs moyens de s'attaquer à la désinformation. Il est possible d'en atténuer les effets les plus pernicieux et de rendre les populations visées plus résistantes. Il est aussi concevable d'en arriver à affronter les acteurs, qu'ils soient ou non parrainés par un État, et à les convaincre d'une manière quelconque de cesser leurs activités. Toutefois, tant et aussi longtemps que les humains seront conditionnés à accepter la désinformation et à voir le pire chez les autres, la victoire totale restera hors de portée. L'attrait pour la désinformation semble être directement lié à l'attrait pour l'autoritarisme. Le pluralisme démocratique en Occident est vulnérable pour les mêmes raisons qu'il est utile. Il ne survivra pas sans effort. Il importe d'inculquer certaines notions dans l'esprit de chaque génération, la première étant que la vérité existe vraiment, c'est-à-dire qu'il existe une réalité objective qui ne peut être éliminée simplement parce qu'on le souhaite. Il importe aussi de comprendre comment la technologie exacerbe le problème de la désinformation et, si possible, de trouver des moyens de modifier la façon dont l'information est communiquée afin d'agir sur la manière dont chacun l'accueille et en fait l'expérience. Tant au pays qu'à l'étranger, les ennemis qui se servent de la désinformation pour porter atteinte à la démocratie et à l'État de droit doivent être affrontés et démasqués pour ce qu'ils sont : des éléments subversifs. Il a tout de même fallu

des siècles d'efforts concertés pour élever l'humanité en l'amenant à résister à ses bas instincts et à ses tendances à la destruction et à l'intolérance. Enfin, ceux qui étudient la désinformation et qui abordent la question publiquement ainsi que les acteurs étatiques et non étatiques qui se livrent à cette activité doivent garder à l'esprit qu'il n'existe pas d'observateurs passifs. Il s'agit d'une guerre totale, sans front, qui ne connaît pas la neutralité. Diviser les gens est sans aucun doute l'un des objectifs du Kremlin, si bien qu'il incombe à chacun de tout faire pour ne pas faire office de pion dans son jeu.

CHAPITRE 3

LE FLAN ORIENTAL DE L'OTAN, NOUVEAU CHAMP DE BATAILLE

La Russie s'est dotée d'une stratégie de l'information exhaustive dans le but d'accroître son influence sur les États périphériques situés entre la mer Baltique et la mer Noire, tout en augmentant ses chances de réussir ses opérations militaires dans le cadre de tout affrontement futur avec les pays qui se trouvent sur le flanc oriental de l'OTAN. La propagation d'informations ciblées et non idéologiques vise à ébranler la volonté des populations visées de résister à la domination russe tout en discréditant les forces de l'OTAN qui se sont engagées à leur venir en aide.

La Russie a déclaré ouvertement une guerre de l'information contre l'Occident en 2013. La première vague d'attaques a été dirigée contre les États situés entre la mer Baltique et la mer Noire (appelés « Intermarium » ou « entre-mers »), c'est à-dire l'Estonie, la Lettonie, la Lituanie et l'Ukraine, soit des pays qui sont demeurés les cibles principales des campagnes d'intimidation et d'agression de la Russie depuis la dissolution de l'URSS en 1991. Par ailleurs, l'oblast de Kaliningrad, enclave russe à l'extérieur de la Russie, fourni une étude de cas unique en son genre illustrant la détermination de la Russie à ériger un « bastion idéologique » anti-occidental au cœur même de l'Europe. Étant donné le rôle essentiel de l'information dans sa vision de la guerre de l'avenir, le Kremlin se sert de sa campagne contre l'Ukraine et les pays baltes comme simple expérience générale en prévision de futurs conflits.

Fabrication d'un cocktail Molotov : la guerre de l'information à la russe

La campagne de désinformation que mène actuellement la Russie contre l'Occident est plus dangereuse et plus évoluée que jamais

auparavant, et ce, pour plusieurs raisons. Premièrement, la stratégie soviétique dans sa version moderne demeure universelle, souple et intelligente. En outre, elle transcende les frontières. Deuxièmement, les campagnes de piratage, les tentatives de compromission (*kompromat*), la destruction délibérée d'informations, la corruption éhontée et les cyberattaques la rendent pratiquement impossible à déceler. Troisièmement, conçue à l'intention de cibles au pays et à l'étranger, cette campagne touche différents auditoires en Russie, dans l'espace postsoviétique et au delà. Quatrièmement, elle est permanente : sous l'appellation d'« affrontement informationnel », elle est conçue de manière à être efficace aussi bien en temps de guerre qu'en temps de paix. Enfin, elle contient parfois des bribes de vérité, ce qui la rend encore plus difficile à contrer.

> *La campagne de désinformation que mène actuellement la Russie contre l'Occident est plus dangereuse et plus évoluée que jamais auparavant, et ce, pour plusieurs raisons.*

La campagne de désinformation russe est extrêmement souple. L'Occident s'évertue à l'inscrire dans un cadre théorique, tandis que la Russie allie théorie et pratique dans une approche multidisciplinaire de militarisation de l'information. Ainsi, à l'ère postmoderne, la guerre de l'information d'inspiration soviétique comporte un volet axé sur la psychologie et l'autre, sur la technologie.

Après l'éclatement de la crise en Ukraine en 2014, les campagnes de désinformation de la Russie ont gagné en complexité et se définissent maintenant en fonction des nouveaux éléments suivants.

Militarisation de l'information. Selon les stratèges militaires russes, la désinformation constituera un élément fondamental des conflits de l'avenir. Des recherches théoriques et des mesures pratiques ont permis la création d'« unités de recherche » et de « cybertroupes ». Selon le ministre de la Défense russe, Sergueï Choïgou, celles ci seront beaucoup

plus efficaces que le département de contre propagande sous l'ère soviétique.

Codification et restauration des mécanismes régissant l'information. L'adoption d'une nouvelle doctrine de l'information en 2016 et d'une stratégie de développement de la société de l'information en 2017 a resserré l'emprise qu'exerce l'État sur le secteur de l'information. En outre, elle a permis de cerner les priorités externes et de confirmer l'état de préparation de la Russie à la guerre de l'information.

Création de la « verticale de l'information ». Chaque citoyen russe, du président à l'exploitant local, fait maintenant partie d'une verticale centralisée qui est responsable de la sécurité de l'information étatique. La mise sur pied de « cyberbrigades » et l'élargissement des responsabilités de la Garde nationale aux domaines de l'information et de la cybersécurité font partie de cette stratégie.

L'Ukraine, laboratoire de la Russie en prévision de futures guerres

La campagne de désinformation agressive de la Russie contre l'Ukraine corrobore le principe de Lénine selon lequel la propagande devrait favoriser l'action plutôt que de se limiter à de belles paroles. Les événements survenus après 2013 devraient être considérés comme une conclusion logique des actions clandestines menées sans relâche par le Kremlin depuis le début des années 90. Lors de l'invasion de l'Ukraine, la Russie a eu recours à une combinaison de méthodes offensives et non offensives simulant un nouveau type de conflit militaire alliant opérations militaires locales (menées par les forces des opérations spéciales), campagnes de désinformation et cyberattaques. La première étape, l'annexion de la Crimée, a servi de tremplin à d'autres opérations dans la région de Donbass. Pour attaquer l'Ukraine et l'Union européenne, la Russie a eu recours à la fois à la guerre axée sur la technologie de l'information (l'occupation du point d'interconnexion Internet de Simferopol et l'interruption des connexions par câble vers le continent qui lui ont permis d'exercer

son infodominance sur la péninsule) et à la guerre psychologique. À ce moment, Moscou a mis l'accent sur la tactique du contrôle réfléchi afin de tenter de forcer la communauté internationale à reconnaître la Russie comme un acteur ayant des intérêts particuliers en Ukraine sans pour autant être une partie au conflit. Au cours de la seconde étape du conflit, qui a débuté en avril 2014, la Russie a élargi sa stratégie et a eu recours à des campagnes de désinformation plus intenses, à des cyberattaques, à des armées de trolls, à des réseaux de zombies, à des logiciels de TI et à des moteurs de recherche (surtout Yandex) pour vaincre l'Ukraine, la discréditer et falsifier les informations. En fait, pour discréditer l'Ukraine aux yeux de l'Occident, la Russie a tenté de la présenter comme une « erreur de 1991 », c'est à dire comme un État déliquescent gouverné par une « junte » illégitime, corrompue, incompétente, russophobe, antisémite et néonazie. En la décrivant ainsi, elle cherchait à atteindre tous les segments de la société occidentale.

La brutalité et les actions du Kremlin reposaient sur les hypothèses suivantes :

- personne ne le défierait dans le dossier de l'Ukraine;
- faibles, fragmentées et dépourvues de vision stratégique, les élites politiques ukrainiennes ne sauraient réagir judicieusement; et
- l'Ukraine n'étant pas un État (homogène), certaines régions appuieraient les actions de la Russie.

Pis encore, pour la majorité des Ukrainiens, l'idée d'être en guerre avec la Russie était inconcevable, attitude que le Kremlin a exploitée dans tout son cynisme. À cet égard, l'exemple ukrainien devrait être reconnu comme un signal d'alarme pour l'ensemble de la communauté européenne et pour les pays baltes en particulier.

Les pays baltes sont-ils les prochaines cibles?

Les trois pays baltes qui forment la partie nord du flanc oriental de l'OTAN constituent une autre cible de choix de la campagne de

désinformation de la Russie. Tout au long des années 1990, les efforts de propagande de Moscou ont porté sur l'interprétation de l'héritage historique de l'Union soviétique, de nombreuses minorités russophones mal intégrées et nostalgiques de cette époque agissant à titre de « fan-club » du Kremlin. Après 2007, l'émergence du concept du « monde russe » a entraîné des changements radicaux : les actions jusque là mal organisées et souvent brouillonnes du Kremlin ont progressivement été remplacées par une stratégie systématique, bien coordonnée et cohérente.

Les opérations de désinformation de la Russie contre les pays baltes visent à montrer que la transformation de ces pays à l'ère postsoviétique et leur intégration dans la communauté euroatlantique ont été un échec. La propagande russe insiste énormément sur la « pauvreté endémique », la « dépopulation » et le « statut semi colonial » de ces pays ainsi que sur l'idéologie d'extrême droite débridée qu'on y trouve. En outre, les élites locales sont qualifiées de russophobes et de paranoïaques. Toujours selon la propagande russe, ces caractéristiques, auxquelles s'ajoute la « servilité aveugle » envers l'Occident, ne permettent pas aux élites politiques locales de prendre des décisions rationnelles, ce qui nuit à leur économie, les transforme en « cordon sanitaire » contre la Russie et les expose à des représailles du Kremlin.

Un autre thème très important de la campagne de désinformation russe est indissociable du rôle de l'OTAN. Les organes de propagande soutenus par le Kremlin diffusent de fausses informations et de fausses nouvelles (en russe et dans les langues locales) dans l'espoir de créer une image répulsive de l'OTAN, dont ils décrivent les soldats (surtout en Lituanie et en Lettonie) comme une bande sauvage de vandales, de pervers sexuels et de violeurs qui, à l'abri des lois locales, agissent comme des envahisseurs (un parallèle manifeste avec l'armée nazie en territoire soviétique). Ce discours déformé sert les objectifs suivants :

- mobiliser la population russe autour du régime politique actuel (« la Russie à titre de forteresse assiégée »);

- présenter la Russie comme une solution de rechange au modèle libéral occidental (« la Russie à titre de gardienne des valeurs conservatrices chrétiennes »);
- raviver les sentiments antiaméricains et anti-OTAN en Europe; et
- fragmenter artificiellement l'Union européenne.

Le renforcement massif du potentiel militaire dans le District militaire Ouest (notamment dans l'oblast de Kaliningrad) constitue un autre moyen de présenter l'OTAN sous un jour défavorable. Il permet de créer un climat d'impunité tout en « prouvant » aux pays baltes que l'OTAN n'est pas en mesure de protéger leur souveraineté et leur intégrité territoriale en cas de conflit. Parallèlement, en intensifiant ses mesures militaires, la Russie tente d'insister sur le fait que les dépenses militaires « excessives » constituent un simple gaspillage d'argent (et une condition imposée par l'OTAN) qui pourrait plutôt être investi dans l'économie.

La crise en Ukraine a eu une incidence profonde sur le comportement de la Russie à l'égard de l'Estonie, de la Lettonie et de la Lituanie. Avec ses plus récentes mesures musclées, le Kremlin a dépeint les pays baltes comme n'étant rien d'autre que le « proche étranger », c'est à dire des entités qui demeurent dans la sphère d'influence de la Russie, n'ayant pas réussi à se joindre à la communauté euroatlantique. Les campagnes de désinformation agressives contre les pays baltes visent aussi à montrer que les tensions croissantes dans la région sont causées par les actions contre la Russie et la russophobie qui se propage dans les pays baltes et en Pologne, ce qui, selon de hauts dirigeants russes, pourrait mener à la troisième guerre mondiale.

Toutefois, la rhétorique belliqueuse et l'intimidation directe ne sont qu'un aspect de l'attitude changeante de la Russie. Depuis 2014, Moscou se sert de plus en plus de Kaliningrad comme d'un instrument lui permettant de diffuser de fausses informations et de s'ingérer de façon agressive dans les affaires intérieures de ses voisins, tout en faisant naître un sentiment anti polonais, anti lituanien et anti OTAN.

Kaliningrad, le phare du « monde russe » en Europe

Différents facteurs limitent la marge de manœuvre de la Russie dans les pays baltes et en Ukraine, et cela pourrait empirer dans le contexte découlant de l'annexion de la Crimée. Situé au cœur de l'Union européenne, Kaliningrad semble être un endroit idéal pour diffuser de la désinformation et exporter des valeurs russes. De premières tentatives infructueuses à cet égard ont été faites de 2003 à 2006. Toutefois, la crise en Ukraine a complètement changé la donne, ayant transformé la perception qu'avait le Kremlin de Kaliningrad et de son rôle dans le conflit idéologique avec l'Occident.

Depuis 2014, l'enclave est à l'avant garde de campagnes intensives de désinformation contre les Lituaniens et les Polonais. Exemple le plus notoire, l'épisode scandaleux à Vilnius à la fin de 2016, lorsque l'ambassade de Russie a diffusé des tracts renfermant de fausses données sur le rendement économique de la Lituanie dans le but d'inciter les habitants à quitter le pays à destination de Kaliningrad.

En plus d'alimenter les troubles internes, Kaliningrad est devenu un rempart pour le soi disant « monde russe » dans la guerre idéologique contre l'Occident, ses valeurs et ses traditions, un monde dans lequel l'Église orthodoxe russe a acquis beaucoup d'influence. Dans un discours prononcé en mars 2015 à Kaliningrad, le patriarche russe Cyrille a qualifié la région de « phare de la Russie » et de rempart contre l'ennemi. La militarisation d'une intensité à couper le souffle (l'oblast est maintenant l'une des régions les plus redoutables en matière de déni d'accès et d'interdiction de zone) jumelée aux mesures prises par la Russie dans le domaine de la sécurité de l'information a transformé Kaliningrad en laboratoire d'essai de nouvelles façons de faire la guerre qui unit, dans une stratégie intégrée, les deux aspects de l'affrontement informationnel de Moscou.

> *Kaliningrad est devenu un rempart pour le soi disant « monde russe » dans la guerre idéologique contre l'Occident.*

Que réserve l'avenir?

De la mer Noire à la mer Baltique, le flanc oriental de l'OTAN est relativement faible et fragmenté et se développe de façon inégale. Compte tenu des leçons tirées de l'expérience en Syrie et en Ukraine, Moscou insistera sur l'adoption d'une stratégie fondée sur l'intégration d'éléments militaires et non militaires. Comme l'a indiqué en 2016 le chef d'État major général Valéri Guérassimov, « les techniques de guerre s'orientent de plus en plus vers la mise en œuvre complexe, forces militaires à l'appui, de moyens politiques, économiques et informationnels ainsi que d'autres moyens non militaires ». Autrement dit, la sécurité de l'information devrait être considérée comme une partie intégrante de la guerre hybride.

En outre, tout porte à croire que la Russie s'est donné un autre objectif stratégique, c'est-à-dire miner la cohésion entre l'Union européenne et les États membres de l'OTAN et provoquer des conflits et de l'animosité entre l'Ukraine et ses partenaires stratégiques au sein de l'alliance euroatlantique. Divers moyens seront employés à cette fin, qu'il s'agisse de groupes de réflexion, d'ONG et de groupes populistes marginaux soutenus par Moscou ou de médias sociaux et d'organes de presse. Le degré de complexité de la propagande russe oblige l'Occident à élargir sa compréhension, souvent simpliste, de la guerre de l'information.

CHAPITRE 4

L'INGÉRENCE ÉTRANGÈRE CIBLANT LES ÉLECTIONS : ARSENAL COMPLEXE, MENACE PERSISTANTE

À la suite des succès du printemps arabe et des manifestations contre la fraude électorale en Russie en 2011 et en 2012, le Kremlin a intensifié son recours aux opérations d'information et au *kompromat*. Il applique de nombreuses techniques pour donner à la désinformation une apparence d'authenticité. Notamment, il fait en sorte que les personnes interviewées à la télévision soient celles qui fourniront une interprétation des événements favorable à Moscou sur les réseaux contrôlés par l'État, et il exploite des techniques de diffusion humaine et automatisée afin de fournir de faux reportages à ceux qui sont prêts à alimenter la dissidence à l'intérieur de régimes politiques étrangers.

Pour bien comprendre les opérations d'information et d'influence que la Russie exécute à l'étranger, il est nécessaire d'étudier l'élément central qu'est « le potentiel de protestation de la population ». La doctrine militaire de la Russie[19] décrit cette expression comme l'une des principales caractéristiques du conflit moderne (non seulement en Russie) au même titre que les actions militaires, les instruments politiques, économiques et informationnels ainsi que les forces spéciales. L'expression a été adoptée après les événements du printemps arabe de 2011 et les vastes manifestations contre la fraude électorale en Russie en 2011 et en 2012. Selon les déclarations de représentants russes, les puissances occidentales avaient organisé ces manifestations pour renverser les régimes favorables à la Russie.

La réaction initiale du Kremlin a été de cibler les Russes afin d'étouffer dans l'œuf toute poussée d'enthousiasme démocratique. Des initiatives comme l'adoption d'une loi sur les agents de l'étranger et la répression d'ONG favorables à la transparence ont vu le jour pendant cette période. En même temps, une usine de trolls formée de tâcherons

russes publiant des messages politiques en ligne contre rémunération a été mise sur pied à Saint Pétersbourg pour inonder de messages favorables au gouvernement les communautés en ligne exprimant leur opposition au Kremlin. La Russie a servi de banc d'essai pour l'application de ces méthodes. En effet, comme c'est souvent le cas, le gouvernement avait comme objectif premier d'assurer sa propre survie. Par la suite, surtout après l'annexion de la Crimée en 2014, les mêmes moyens offensifs ont été employés contre des cibles étrangères, d'abord l'Ukraine, puis l'Occident.

Démarche

L'objectif des opérations d'information et d'influence de la Russie visant les pays démocratiques se résume en deux mots : diffamer et amplifier. Différents éléments des systèmes du Kremlin génèrent ou recueillent des informations destinées à compromettre la cible; d'autres éléments les amplifient tout en conservant la possibilité d'y opposer un démenti plausible. Cette méthode remonte à la période précédant l'ère soviétique et trouve son origine dans la notion de « matériel compromettant » (*kompromat*). Dans les années 1980, les Soviétiques ont publié dans un journal indien une fausse nouvelle selon laquelle la CIA avait créé le SIDA, puis en avaient magnifié l'ampleur à l'échelle mondiale. L'avènement de sites Web et de médias sociaux anonymes a rendu de telles techniques beaucoup plus faciles à utiliser.

Une technique simple consiste à donner une tribune à des commentateurs dans le pays visé qui confirment la validité du discours du Kremlin. Par exemple, en 2014 et en 2015, RT a interviewé un nombre disproportionné de députés du Parlement européen appartenant au Parti pour l'indépendance du Royaume-Uni (UKIP) opposé à l'Union européenne. Au cours du premier semestre de 2017, Sputnik France a donné une place démesurée aux politiciens qui attaquaient Emmanuel Macron. Au cours de l'élection américaine, RT et Sputnik ont interviewé à répétition un universitaire qui prétendait que Google truquait son moteur de recherche à saisie automatique en faveur d'Hillary Clinton.

En pareils cas, ce qui est omis est aussi important que ce qui est inclus. Les personnes interviewées peuvent être et sont habituellement sincères dans leurs convictions. Les techniques de propagande consistent à amplifier celles-ci et à les valider sans tenir compte du revers de la médaille. L'organisme de réglementation des télécommunications britannique a trouvé RT en défaut à cet égard à plusieurs reprises.

> *Ce qui est omis est aussi important que ce qui est inclus.*

Il est aussi important de procéder à une analyse approfondie des « spécialistes » en question. Par exemple, au cours de la période précédant le référendum catalan du 1er octobre 2017, le service espagnol de Sputnik a présenté à la une les gazouillis de Julian Assange, fondateur de Wikileaks, plus que ceux de tout autre commentateur, y compris le président de la Catalogne et le premier ministre d'Espagne. Assange n'a jamais mentionné la Catalogne dans ses gazouillis avant le 9 septembre 2017 et, à ce qu'on sache, n'a pas de compétences particulières dans le domaine des affaires constitutionnelles en Espagne. La décision de Sputnik d'amplifier ses gazouillis, qui attaquaient le gouvernement à Madrid, semble donc être fondée sur son message plutôt que sur ses compétences.

Les faux spécialistes, des commentateurs partisans

Une autre technique consiste à publier les commentaires d'intervenants alignés sur le Kremlin sans mentionner leur affiliation. Par exemple, après la destruction en plein ciel du vol MH17 de la Malaysia Airlines en Ukraine, des journalistes d'enquête du groupe Bellingcat ont recueilli, auprès de sources ouvertes, des éléments de preuve indiquant que l'avion avait été abattu au moyen d'un missile Buk-M1 lancé à partir de la Russie.

En réponse, un groupe de blogueurs nommés les « anti Bellingcat » qui, au départ, étaient anonymes et « indépendants », ont publié un long rapport réfutant les conclusions de Bellingcat. Les médias du

Kremlin ont fait publier ce rapport en plusieurs langues et l'ont diffusé à grande échelle.

Il est ressorti plus tard que, loin d'être indépendant, l'un des deux principaux auteurs était un employé de la société d'État qui fabrique le missile Buk. L'autre était porte parole d'un groupe de réflexion fondé par le Kremlin et lié aux services de renseignement russes.

Des organismes du Kremlin ont également créé de nombreux sites « indépendants » qui dissimulent leurs liens avec le gouvernement de la Russie. Par exemple, NewsFront.info produit du contenu favorable au Kremlin et anti occidental dans plusieurs langues. Selon un dénonciateur interviewé par le journal Die Zeit, le site est financé par le renseignement russe. Baltnews, un ensemble de sites Web dans les pays baltes, prétend être indépendant, mais des liens ont pu être établis avec la société mère de Sputnik. En octobre 2017, il a été révélé qu'un compte Twitter d'extrême droite très actif et influent aux États Unis, @TEN_GOP, était exploité à partir de l'usine de trolls. Ce compte a connu un succès phénoménal – les messages qui y ont été diffusés ont été cités dans les médias grand public et partagés par les principaux assistants de Trump — et a contribué à amplifier la désinformation qui a fini par être citée par Trump lui même.

Au cours du même mois, des liens ont été établis entre le groupe connu sous le nom d'AGITPOL (« régiment de l'agitation ») et l'usine de trolls. Il se présentait comme un collectif d'activistes en ligne et a lancé à répétition des campagnes de mots-clics favorables au Kremlin ou opposées à l'Occident. Il aurait servi, par exemple, à attaquer l'acteur américain Morgan Freeman et à souhaiter un joyeux anniversaire au président Vladimir Poutine. À une occasion, des acteurs inconnus ont créé un site miroir complet du site du quotidien *The Guardian* pour publier un article dans lequel ils affirmaient que l'ancien chef du MI6 avait avoué que le Royaume-Uni et les États Unis avaient tenté de provoquer l'éclatement de la Russie au début des années 2000. Cette fausse nouvelle a vite été révélée comme telle, ce qui n'a toutefois pas empêché la télévision d'État russe de présenter de longs reportages sur cette histoire pour corroborer le discours selon lequel la Russie était assiégée.

Le piratage des courriels de politiciens bien en vue et leur diffusion en ligne constitue, par ailleurs, la technique la plus préjudiciable. Cela est particulièrement nuisible, pour les raisons suivantes :

- toute fuite est implicitement présumée préjudiciable;
- il est facile d'insérer de faux documents parmi des documents authentiques;
- il est possible de laisser filtrer des informations uniquement au moment où elles sont susceptibles de causer le plus de dommages; et
- les médias authentiques qui ne se méfient de rien sont susceptibles d'amplifier les fuites d'information.

Le piratage et la divulgation en ligne des courriels d'Hillary Clinton, candidate du Parti démocrate des États Unis, s'inscrivent tout à fait dans ces tentatives de compromission. Les informations piratées ont été utilisées de façon particulièrement agressive, certaines d'entre elles ayant été publiées tous les jours pendant le mois précédant l'élection. Ces opérations semblaient avoir un double objectif : porter atteinte à Clinton personnellement et mettre en doute la légitimité du processus électoral en général, le tout dans l'espoir de galvaniser le « potentiel de protestation de la population » si Clinton remportait la victoire. Comble de l'ironie, Clinton a perdu l'élection de 2016, et l'ingérence de la Russie a, en fait, nui au président auquel celle ci avait accordé son appui.

L'achat de publicités partisanes pour les diffuser sur les médias sociaux est une autre technique destinée à semer la division qui est en train d'être mise au jour. Conjuguée à l'utilisation de comptes de médias sociaux anonymes et agressifs, cette technique semble être conçue pour dresser les uns contre les autres différents groupes susceptibles de se soulever.

Évolution de la situation

Étant donné qu'elles ne cessent d'être mises au jour, il faut s'attendre à ce que les techniques de désinformation les plus récentes évoluent rapidement et soient adaptées de manière à en dissimuler l'origine plus efficacement et à compliquer l'établissement d'une distinction entre opérateurs humains et systèmes automatisés. Des efforts sont déjà en cours pour favoriser le patriotisme au sein du personnel de l'usine de trolls pour réduire les risques de fuites[20]. Par ailleurs, fait à souligner, si les courriels piratés pendant la campagne de Clinton ont été rendus publics au moyen de Wikileaks, ceux qui ont été piratés pendant la campagne de Macron ont été publiés anonymement sur le site Web 4chan et amplifiés par l'extrême droite américaine, ce qui laisse croire à une volonté de varier les plateformes de diffusion.

> *Les tentatives de piratage s'intensifieront vraisemblablement, surtout de la part d'acteurs anonymes dont les liens avec le Kremlin sont masqués.*

Les comptes de médias sociaux combinent de façon de plus en plus complexe les messages préparés par des humains et les messages automatisés. En règle générale, ces cyborgs affichent des messages à un rythme élevé, souvent des centaines par jour, en les parsemant de messages produits par des auteurs, ce qui les dissimule davantage aux algorithmes de détection de robots et les rend plus difficiles à contrer. Cette tendance s'accélérera sans doute.

Les tentatives de piratage s'intensifieront vraisemblablement, surtout de la part d'acteurs anonymes dont les liens avec le Kremlin sont masqués. L'expérience de 2016 a montré que le piratage et les fuites d'informations peuvent être des armes dévastatrices, mais qu'ils peuvent aussi avoir l'effet inverse si l'identité des responsables est révélée. Les informations contre Emmanuel Macron qui ont filtré ont probablement été publiées anonymement sur 4chan et diffusées par l'extrême droite aux États Unis dans le but de compliquer davantage leur attribution. Puisqu'ils font l'objet d'une surveillance

accrue, les médias appartenant ouvertement au Kremlin, comme RT et Sputnik, risquent d'être délaissés au profit de médias de façade comme NewsFront et BaltNews.

Contre-mesures : bâtir la résilience

Un certain nombre de mesures visant à contrer la désinformation ont déjà été mises à l'essai. La plus simple a été de bloquer l'accréditation de fournisseurs de contenus pseudo journalistiques comme RT et Sputnik, comme on l'a vu dans les pays baltes et en France. Bien qu'elle envoie un puissant message, cette mesure établit aussi un précédent qui prête le flanc aux abus. Les mesures de ce genre ne devraient donc être utilisées qu'en dernier recours.

L'enregistrement des médias contrôlés par l'État est un autre moyen digne d'être étudié. Au moment de la rédaction du présent document, les États Unis auraient sommé RT et Sputnik de s'enregistrer à titre d'agents de l'étranger. En pareils cas aussi, il convient de faire preuve de circonspection : il est important d'étiqueter l'organe sans donner l'impression de vouloir le réduire au silence.

La réglementation des normes journalistiques peut aussi jouer un rôle. Au Royaume-Uni, l'organisme national de réglementation des télécommunications, Ofcom, a déclaré RT coupable d'avoir entravé les normes journalistiques dans un certain nombre d'émissions. Les sanctions ont été symboliques, mais les dommages à la réputation de la chaîne d'information ont été considérables. De telles conclusions de la part d'organismes de réglementation, fondées sur des éléments précis d'émissions individuelles évaluées selon des normes transparentes d'exactitude et d'impartialité, constituent un outil utile dans les efforts visant à contrer toutes les sources de désinformation.

La vérification détaillée des faits joue également un rôle dans la dénonciation de fausses informations et de faux discours. La vérification des faits n'est pas le meilleur moyen de contrer les fausses histoires qui, pour la plupart, font appel à l'émotivité. Toutefois, au fil du temps, une vérification systématique des faits peut contribuer à mettre au jour les sources principales de fausses informations. Il

importe aussi de démasquer les opérations d'influence. Dans un exemple récent, de fausses allégations de viol contre des soldats de l'OTAN dans les pays baltes ont pu être démenties avant qu'elles ne fassent boule de neige. En effet, l'intervention rapide des représentants officiels de l'organisation auprès des médias grand public a permis de mettre au jour cette histoire inventée de toutes pièces[21].

Toutefois, pour que de telles révélations aient l'effet souhaité, 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. Faire abstraction du problème peut avoir des conséquences. Le 7 octobre 2016, le directeur du Renseignement des États-Unis a prévenu que la Russie tentait de s'ingérer dans l'élection. La diffusion d'une vidéo d'Access Hollywood dans laquelle Trump se vantait d'empoigner les femmes par le sexe a vite fait de reléguer cet avertissement au second plan, si bien qu'il n'a attiré l'attention de la population à l'échelle du pays qu'une fois l'élection terminée.

On ne saurait trop insister sur l'importance de sensibiliser et de mobiliser la population. La désinformation se propage mieux au sein des groupes qui ne se méfient pas ou qui ont un penchant pour les fausses informations. Des cours sur la façon de repérer un faux compte de média social, une photo volée ou un article tendancieux sur Internet devraient être donnés sur une échelle beaucoup plus vaste. Les gouvernements pourraient aussi consacrer plus de temps à cerner des segments particuliers de leurs sociétés, à dialoguer avec eux et à les écouter pour comprendre comment et pourquoi de fausses informations arrivent à s'y propager.

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.

CHAPITRE 5

EXAMEN DU BREXIT : ASCENSION ET DÉCLIN D'UN RÉSEAU DE ZOMBIES SUR TWITTER

La recherche sur les réseaux de zombies actifs pendant le référendum sur le Brexit a mis au jour un phénomène de gazouillage hyperpartisan et coordonné qui résultait des activités de deux groupes. Le premier générait automatiquement de grands nombres de gazouillis, publiés ou partagés, tandis que le deuxième communiquait à un auditoire plus ciblé des données générées par les utilisateurs. Le trafic était majoritairement favorable à la sortie de l'Union européenne et interpelait les lecteurs nationalistes et xénophobes. Sans être composé de fausses nouvelles fabriquées, le contenu de ces gazouillis était simpliste et n'était fondé sur aucun fait, imitant le style des tabloïdes et intégrant, en boucle, la rétroaction de l'auditoire. Dans une forte proportion, ces comptes et leur contenu ont été désactivés immédiatement après le référendum.

Le référendum sur l'appartenance du Royaume-Uni à l'Union européenne s'est joué sur un fond de réorientations politiques, de polarisation et d'hyperpartisannerie. Les consommateurs de nouvelles eux se sont scindés en deux groupes, suivant leur segmentation démographique, privilégiant dans un cas les médias grand format et dans l'autre les tabloïdes. Pendant toute la période du référendum, les partis populistes et leurs chefs ont stratégiquement tiré parti de ces éléments, qu'ils ont moussés au maximum pour promouvoir « les valeurs culturelles traditionnelles et multiplier les appels au patriotisme et à la xénophobie tout en insistant sur le rejet des étrangers et la préservation des rôles traditionnels liés au sexe »[22]. Ces circonstances et le climat politique ainsi créé ont offert un terreau fertile à l'utilisation de bots pendant le référendum lié au Brexit.

L'analyse qui suit se penche sur les activités d'un réseau de zombies qui a, tout au long du référendum, publié sur Twitter des liens vers toute une gamme de contenus générés ou sélectionnés par les utilisateurs comportant des informations hyperpartisanes. Ainsi, l'analyse a porté sur trente neuf mots-clics clairement associés à la campagne du référendum entre avril et août 2016[23], ce qui représente 10 millions de gazouillis au total. Par la suite, les profils de plus de 800 000 utilisateurs distincts ont été consultés : des techniques de seuillage et de filtrage ont été appliquées pour discerner les utilisateurs en chair et en os des bots. Le recours à diverses méthodes combinées a permis de cerner un vaste réseau de zombies dont les comptes avaient été désactivés par le responsable du réseau ou encore bloqués ou supprimés par Twitter au lendemain du référendum, de déterminer quelle était la campagne soutenue par le gazouillis, d'obtenir le titre des pages Web associées aux URL figurant dans les gazouillis (le cas échéant) et d'examiner la façon dont les gazouillis ont été partagés et dont les renvois @ ont été utilisés.

Des gazouilleurs éphémères

Il a été établi que, sur les 794 949 profils Twitter qui ont envoyé des gazouillis dans le cadre des campagnes *Vote Leave* (Votez pour partir) et *Vote Remain* (Votez pour rester), 5 p. 100 ont été désactivés, supprimés, bloqués ou rendus privés après le référendum, ou encore ont changé de nom d'utilisateur. La plus grande part des membres de ce groupe (66 p. 100) ont changé de nom d'utilisateur à la suite du référendum, mais ont continué d'intervenir sur Twitter (comptes réorientés ou recyclés), tandis que 34 p. 100 des membres de ce groupe ont subitement été bloqués ou ont quitté Twitter (comptes supprimés). Le plus souvent, dans les comptes recyclés et supprimés, on trouvait principalement du contenu partagé qui a disparu d'Internet peu après le référendum. En mesurant la fréquence relative des mots clés et des mots clics associés à chacune des campagnes, il a également été établi qu'une bonne partie de ces comptes soutenaient la campagne *Vote Leave*. Même si la proportion de messages renfermant des mots clics appuyant les campagnes *Vote Leave* et *Vote Remain* s'établissait à 31 p. 100 et à 11 p. 100 respectivement, dans les comptes recyclés et

supprimés combinés, les mots clics liés au référendum étaient employés dans une proportion de 37 p. 100 par rapport à 17 p. 100.

Une analyse de la langue employée dans les gazouillis permet de mieux comprendre cet écart. En examinant les gazouillis qui emploient des marqueurs textuels comme les mots clics et les mots clés liés aux campagnes *Vote Leave* et *Vote Remain*, on constate que la proportion de gazouillis soutenant la campagne *Vote Leave* est encore plus élevée dans le bassin des comptes supprimés, s'établissant à 41 p. 100 par rapport à 31 p. 100 dans le bassin des comptes actifs, lesquels renferment également une plus grande proportion de gazouillis neutres. Les slogans associés à la campagne *Vote Leave* étaient également beaucoup plus susceptibles d'avoir été publiés sur Twitter par ce bassin de comptes, dans une proportion de 8 contre 1. Le sous groupe de comptes supprimés s'était également montré beaucoup plus actif dans la période précédant le référendum et moins actif à la suite du vote.

Nouvelles hyperpartisanes et hyperéphémères

Lorsque les chercheurs ont tenté de consulter les pages Web partagées par les comptes recyclés et supprimés, ils ont constaté que la plupart des adresses URL partagées (55 p. 100) n'existaient plus, demeuraient sans réponse ou étaient liés à un compte Twitter ou à une page Web qui n'existait plus. Près du tiers (29 p. 100) des adresses URL pointaient vers des statuts, des images ou du contenu multimédia sur Twitter qui n'étaient plus accessibles et dont le compte d'origine avait également été supprimé ou bloqué, ce qui illustre bien la nature périssable du contenu numérique axé sur des enjeux politiques. Par ailleurs, toujours dans le même groupe, 1 p. 100 de tous les liens pointaient vers l'utilisateur @brndstr, l'un des rares comptes figurant dans le réseau de communication des comptes recyclés qui soit encore actif sous le même nom. Ce compte est géré par une entreprise qui se spécialise dans la fourniture de bots en vue de campagnes dans les médias sociaux.

En examinant de plus près les comptes qui fournissaient du contenu au bassin des comptes recyclés, force est de constater le caractère

très éphémère du contenu généré par les utilisateurs. Il est ici question de comptes Twitter qui visaient à répandre des nouvelles douteuses émanant d'un circuit fermé où chaque site s'alimentait de l'autre dans une boucle sans fin : une combinaison de blogues d'extrême droite et de tabloïdes traditionnels. Toutefois, d'après les quelques pages Web qui ont pu être consultées, le contenu publié sur Twitter à partir de ce bassin de comptes recyclés et supprimés ne peut être caractérisé comme de la désinformation ou de fausses nouvelles. Le contenu en question s'apparente davantage à une forme de récit, qui vient brouiller les distinctions entre le type de journalisme traditionnel des tabloïdes et le contenu généré par les utilisateurs : ce dernier, souvent anonyme et dépourvu de faits, mise principalement sur la simplification et l'exploitation du caractère spectaculaire du récit. La plus grande part des hyperliens publiés sur Twitter par les comptes recyclés et supprimés pointent vers du contenu généré par les utilisateurs, lequel est souvent mis en page de la même façon que dans les journaux sérieux par l'entremise de services de traitement du contenu et renferme fréquemment des éléments multimédias sur Twitter.

De la même façon, les rares liens qui étaient toujours accessibles six mois après la tenue du référendum pointaient vers un contenu riche en rumeurs, en événements non confirmés et en histoires à dimension humaine jouant sur l'émotion et le populisme, du journalisme propre aux tabloïdes, à la différence que l'auditoire joue un rôle crucial dans le choix et la distribution du contenu, ajoutant du coup un degré de complexité à toute la démarche. Les sources qui ont été inspectées, même si elles ne sont pas représentatives de l'univers beaucoup plus vaste du contenu publié sur Twitter par cette population d'utilisateurs (contenu qui a hélas en bonne partie disparu de Twitter), ont beaucoup en commun avec le journalisme propre aux tabloïdes hyperpartisans, qui met l'accent sur des articles à dimension humaine très accrocheurs et faciles à partager.

Même si 17 p. 100 des hyperliens pointaient vers des comptes Twitter toujours actifs, l'examen d'échantillons choisis de façon aléatoire a démontré qu'il arrive souvent que le message original ne soit plus disponible, ce qui empêche de déterminer la nature du contenu publié au départ. Par exemple, l'un des profils a généré une chaîne de

plusieurs centaines de gazouillis partagés, mais un examen a permis d'établir que toutes les publications provenaient d'un seul et même utilisateur actif. Même si le compte à l'origine de la chaîne est toujours actif, le gazouillis original a été supprimé (ainsi que la chaîne de gazouillis partagés s'y rattachant). Comme Internet Archive n'a rien conservé au sujet de ce gazouillis en particulier, il est impossible de savoir en quoi consistait le message véhiculé par l'image d'origine. L'ampleur de la suppression de contenu touche aussi bien les hyperliens que la population visée a publiés dans des gazouillis que les comptes des utilisateurs : il s'agit là d'un phénomène nouveau et inquiétant compte tenu de l'importance du référendum et de la controverse qu'il a soulevée.

Le réseau de zombies du Brexit

Les examens menés après le référendum sur la façon dont les bots ont partagé des gazouillis montrent qu'il existait au moins deux groupes de bots fondamentalement différents. Le premier groupe s'appliquait à reproduire du contenu automatisé, le plus souvent des nouvelles hyperpartisanes, ce qui permettait de propager les chaînes de gazouillis partagés beaucoup plus rapidement que les chaînes de gazouillis partagés générés par des utilisateurs actifs. Le deuxième groupe était quant à lui parfaitement intégré aux activités humaines. L'un et l'autre de ces types de comptes sont parvenus à générer des chaînes de taille moyenne (T>50) et grande (T>100), mais leurs façons caractéristiques de partager des gazouillis montrent qu'ils ont été créés et déployés en vue d'atteindre des objectifs profondément différents.

Le premier sous groupe de bots était associé à des comptes qui tiraient parti des habitudes en matière de partage des gazouillis pour amplifier la portée d'un petit groupe d'utilisateurs, mais qui servait rarement, voire jamais, à déclencher une chaîne de partage de gazouillis. À l'inverse, l'autre sous groupe de bots œuvrait à moins grande échelle et partageait uniquement les gazouillis d'autres bots du réseau de zombies, de sorte qu'il produisait de son côté de nombreuses chaînes de taille moyenne qui se propageaient beaucoup plus rapidement que les autres chaînes. Même si des bots ont été utilisés dans les deux

cas, ceux du premier groupe relayaient uniquement les gazouillis d'utilisateurs actifs, tandis que ceux du deuxième groupe se limitaient aux gazouillis d'autres bots (probablement déployés en même temps que le nœud maître). Chacun des sous-réseaux de bots jouait un rôle spécialisé dans le réseau, et ils alimentaient tous deux le bassin plus vaste des comptes ordinaires qui fournissaient de l'information à @vote_leave, c'est à dire le compte Twitter officiel de la campagne Vote Leave et la source la plus importante de diffusion de l'information à cet égard.

> *Les examens menés après le référendum sur la façon dont les bots ont partagé des gazouillis montrent qu'il existait au moins deux groupes de bots fondamentalement différents.*

La rediffusion de gazouillis a principalement eu lieu dans la période menant au vote . Il s'agissait pour la plupart de gazouillis relayés par de véritables utilisateurs, à partir de comptes d'utilisateurs actifs et vers de tels comptes. Les bots ont été employés au cours de la même période, partageant des gazouillis d'utilisateurs actifs comme des gazouillis d'autres bots, principalement pendant la semaine précédant le vote ainsi que la veille du référendum, moment où les partages de gazouillis entre bots ont atteint un sommet. Cette rediffusion a fortement diminué après le référendum, surtout chez les utilisateurs actifs qui ont cessé de lancer des chaînes de partages de gazouillis ou d'y prendre part. Les bots ont mené des activités tout au long de la campagne, mais ont été les plus actifs dans la période du 12 au 15 juillet : ils partageaient d'abord les gazouillis d'utilisateurs actifs, puis reproduisaient du contenu généré par des bots, avant de diminuer graduellement dans les semaines qui ont suivi le retrait, la désactivation ou la suppression du réseau de zombies de la plateforme Twitter[24]. En fait, les nœuds maîtres du sous-réseau bot à bot se sont pour la plupart volatilisés à la suite du référendum. C'est au cours de cette période cruciale que le contenu relayé par ces bots et que les pages Web liées à leur gazouillis sont disparues d'Internet, de la sphère publique de Twitter et des interfaces de programmation d'applications (API) des entreprises.

Conclusions

Le grand nombre de liens pointant vers du contenu généré par des utilisateurs, tout particulièrement des éléments multimédias sur Twitter, ainsi que l'incidence importante des services de traitement du contenu utilisés pour présenter du contenu partagé sur les réseaux sociaux de la même façon que dans des journaux sérieux en ligne, donnent à penser que l'univers des nouvelles hyperpartisanes est conçu selon une approche descendante et s'appuie sur du contenu généré par les utilisateurs. Le contenu publié sur Twitter au sujet du Brexit était davantage axé sur les valeurs nationalistes et nativistes que le contenu publié par la population en général (27 p. 100 par rapport à 19 p. 100). Il demeure cependant que la nouvelle réalité, pour les sites Web hyperpartisans, consiste à tenter de satisfaire les deux extrêmes du spectre politique. Ainsi, ces sites appartiennent souvent à la même entreprise et adaptent les articles en fonction des préjugés de leur auditoire, de façon à conforter les lecteurs dans leur opinion.

Les analyses des réseaux de zombies du Brexit n'ont pas permis de confirmer au moyen de données solides que de « fausses nouvelles » ont été propagées à vaste échelle, mais ont plutôt permis d'établir que des bots avaient été placés de façon stratégique pour produire de l'information hyperpartisane sélectionnée par les utilisateurs. Les résultats de la présente étude ont aussi permis de relever un nouveau jalon dans le journalisme sensationnaliste : la capacité d'intégrer une boucle de rétroaction de l'auditoire, tout en effectuant une transition de l'identité éditoriale d'un tabloïde imprimé traditionnel à du contenu choisi aussi bien généré par les utilisateurs que créé par une équipe de rédaction. Les organes de presses hyperpartisans incarnent donc parfaitement la tendance actuelle : produire du contenu viral, soit des articles courts, très visuels, faciles à partager et accessibles au moyen d'appareils mobiles, du contenu qui, en confirmant les préjugés de son public cible, peut être assimilé à une balkanisation du lectorat en fonction des intérêts de groupes de même tendance.

CHAPITRE 6

DÉCRÉDIBILISER LES « FAUSSES INFORMATIONS » SUR LA SYRIE GRÂCE À DES MÉTHODES AXÉES SUR LES SOURCES OUVERTES

Lorsqu'elle est intervenue militairement en Syrie, la Russie a protégé le régime Assad tout en rejetant toute accusation d'usage de tactiques illégales et de crimes de guerre dans le secteur. Toutefois, l'étude du cas de la Syrie montre bien qu'il est possible d'utiliser la technologie pour empêcher la Russie de militariser l'information au moyen de cette même technologie. Les sources ouvertes fournissent toutes des fragments numériques qui peuvent être rassemblés et entre lesquels il est possible d'établir des renvois pour réfuter la propagande et fournir des preuves directes des tactiques russes.

De l'analogique au numérique

Fausses nouvelles, intoxication, propagande, quel que soit le terme utilisé, le défi que représente la désinformation a atteint un nouveau degré de complexité dans un monde hyperconnecté. L'époque où les informations ne circulaient que dans une direction, c'est-à-dire des gouvernements, des éditeurs et des diffuseurs vers le public, est révolue. De nos jours, tout utilisateur d'un téléphone intelligent peut être à la fois diffuseur, consommateur, journaliste et lecteur. Il n'y a que dix ans que ce changement radical s'est amorcé, mais déjà plus de 3,8 milliards de personnes ont accès à Internet, 2,9 milliards utilisent les médias sociaux, dont 2,7 milliards sur une plateforme mobile.

Cette révolution, qui fournit de nouveaux outils puissants qui permettent d'étudier les conflits, les crises et la désinformation, incite un mouvement de soi-disant Sherlock numériques à se pencher sur des méthodes pour percer le brouillard de la désinformation. Les articles publiés en ligne permettent maintenant d'avoir accès à des zones de conflit et à des points chauds autrefois hors de portée.

Conscients des possibilités qu'offre ce nouveau contexte, les acteurs hostiles de la désinformation travaillent sans relâche pour exploiter ces informations et miner les principes fondamentaux de la réalité.

Rappel des faits dans le conflit syrien

Le rôle joué par la Russie en Syrie montre bien les difficultés qui se posent lorsqu'un acteur étatique utilise la désinformation et la duperie pour soutenir ses activités d'agression. Au cours des dernières années, le recours à de telles méthodes a permis au président russe Vladimir Poutine de passer d'une aventure de politique étrangère à une autre tout en militarisant l'information contre les sociétés occidentales.

En 2014, Poutine a ordonné l'annexion de la presqu'île ukrainienne de la Crimée en supervisant une guerre clandestine dans l'est de l'Ukraine et en soutenant les intermédiaires russes au moyen d'armes, de combattants et d'unités militaires entières. Quand la guerre s'est retrouvée dans une impasse, Poutine a tourné les yeux vers la Syrie. Après une rapide campagne diplomatique et un renforcement tout aussi rapide de ses forces militaires, il a lancé des frappes aériennes contre le pays déchiré par la guerre. La campagne militaire russe a permis aux forces d'Assad de reprendre le terrain perdu, tâche dont elles se sont acquittées avec énormément de brutalité et au prix d'immenses souffrances humaines. Loin de raccourcir la guerre, elle l'a exacerbée et, ce faisant, a envoyé de nouvelles vagues de réfugiés inonder la Turquie et l'Europe. Rien de tout cela n'aurait été possible sans le voile de désinformation sous lequel Poutine et le régime Assad ont dissimulé leurs actions et leurs atrocités.

Le voile

Poutine a affirmé cyniquement que la présence de la Russie en Syrie visait à lutter contre Daech, nourrissant ouvertement le mythe selon lequel Moscou luttait contre le terrorisme, le régime Assad n'avait pas commis d'atrocités et l'Occident était à l'origine du soulèvement syrien. Pour réussir à maintenir le voile en place, il a appliqué trois stratégies :

1. *Nier les faits.* La façon la plus simple de répondre aux allégations de frappes aveugles et de victimes civiles était de nier les faits. Pendant toute la durée du conflit, au mépris des preuves, tant Damas que Moscou ont carrément rejeté toutes ces allégations.

2. *Militariser les victimes.* Parallèlement à la campagne de déni, les représentants officiels de la Syrie et de la Russie ont faussé à maintes reprises la nature de leurs cibles, faisant passer des civils pour des combattants. Ce maquillage de civils en cibles militaires légitimes s'appliquait à des villes complètes comme à de simples immeubles. En brouillant sans cesse la distinction entre les forces liées à al-Qaïda et les autres groupes, Moscou et Damas ont réussi à donner l'impression que tous les groupes qu'ils prenaient pour cible étaient des extrémistes.

3. *Attaquer les témoins.* Il est devenu particulièrement clair pendant le siège d'Alep en 2016 que des témoignages oculaires pourraient discréditer les efforts de la Russie et de la Syrie pour militariser les victimes : des frappes aériennes avaient visé des immeubles civils et tué des civils. Les dirigeants syriens et russes ont donc commencé à attaquer la crédibilité de ces témoins de la souffrance, dont l'un des plus importants était l'organisation d'aide humanitaire d'abord appelée Défense civile syrienne, mais vite surnommée « Casques blancs » en raison de la couleur du casque de ses membres. Lorsqu'ils ont vu le jour à Alep, au début de 2013, les Casques blancs étaient une organisation de secours[25]. Comme le conflit s'intensifiait et que les journalistes indépendants n'avaient plus accès aux lignes de front, ils sont devenus peu à peu l'une des principales sources attestant la véritable nature des bombardements, publiant des images des frappes aériennes et de leurs conséquences captées au moyen de caméras GoPro. Cela les a menés tout droit à l'affrontement avec le gouvernement et ses alliés.

Ceux qui cherchent à propager de la désinformation laissent une empreinte numérique qui se démarque nettement de celles de la

réalité, ce qui donne la possibilité de recueillir des preuves au moyen des sources ouvertes, des médias sociaux et des techniques d'informatique judiciaire qui exploitent la puissance de l'ère numérique et par l'application d'une approche de l'information axée sur les faits et la vérification. Il est alors possible de limiter les opérations de l'agresseur en en exposant la fausseté et en levant le voile qui recouvre ses crimes et ses atrocités.

> *Ceux qui cherchent à propager de la désinformation laissent une empreinte numérique qui se démarque nettement de celles de la réalité.*

Lever le voile

Des séquences publiées dans les sources ouvertes montrent l'utilisation répétée de bombes à sous-munitions, pourtant interdites, ainsi que des frappes contre des cibles interdites, dont des mosquées, des hôpitaux et des usines de traitement de l'eau en Syrie. En comparant et en utilisant les masses d'informations disponibles sur ces attaques et ces atrocités, il est possible d'en déterminer le nombre et l'ampleur à l'échelle de la Syrie, de reconstituer la structure de chacun des incidents et d'évaluer les conséquences de multiples attaques sur différentes installations. Cet examen devient un outil particulièrement puissant pour répondre aux fausses affirmations de la Russie, ce qui permet de lever le voile qui entoure la désinformation.

Au cours des dernières semaines du siège de la ville stratégique d'Alep, le porte-parole du Kremlin Dmitri Peskov a soutenu qu'il n'y avait aucune preuve de frappes contre des hôpitaux, et Assad a affirmé qu'il n'existait pas de telle politique de ciblage. Toutefois, des preuves vérifiées (notamment des témoignages, des séquences de nouvelles, des vidéos filmées par des caméras de sécurité et par les sauveteurs ainsi que des photos) donnent à penser que le gouvernement Assad et ses alliés, dont la Russie, avaient effectivement pour politique de viser les hôpitaux syriens. Ainsi, l'hôpital M2 soutenu par la Société médicale syro-américaine (SAMS) dans le quartier d'al-Maadi aurait été victime d'au moins douze attaques entre les mois de juin et de

décembre 2016. Un examen des fragments numériques relatifs à l'incident (par exemple, les images et vidéos de sources ouvertes, les images satellitaires des environs de l'hôpital et la séquence du système de télévision en circuit fermé qui a été publiée) permet de confirmer que l'hôpital M2 a été touché à maintes reprises entre les mois de juin et de décembre 2016, les dommages subis étant conformes à l'utilisation de l'artillerie et de bombes parachutées. L'équipement et les véhicules utilisés par l'hôpital ont été endommagés et détruits, et les attaques ont gravement réduit la capacité de l'hôpital de servir la population locale.

Plus le public était sensibilisé à la situation critique des hôpitaux d'Alep, plus les représentants officiels niaient toute responsabilité. Entre le 28 septembre et le 3 octobre 2016, l'hôpital al Sakhour soutenu par la SAMS (également connu sous le nom d'hôpital M10) a été la cible de trois frappes distinctes qui ont endommagé les immeubles et tué des employés et des patients. Au cours d'une conférence de presse, le ministère russe de la Défense a nié que l'hôpital ait été la cible d'attaques. Son porte-parole, le lieutenant-général Sergei Rudskoy, a présenté des images satellitaires, qu'il a affirmé avoir été prises entre le 24 septembre et le 11 octobre, et déclaré qu'« il est possible de constater que l'hôpital n'a pas changé, ce qui prouve que toutes les accusations de frappes aveugles proférées par de prétendus témoins oculaires ne sont finalement que des mensonges. » L'évolution des dommages causés à l'hôpital après chaque attaque est cependant très claire dans les images satellitaires de la région et dans les sources ouvertes, ce qui prouve que les images du ministère russe de la Défense étaient trompeuses[26].

Comme les frappes contre des hôpitaux, les rapports de frappes incendiaires ont été niés vigoureusement. À la fin de 2015, le major-général Igor Konachenkov, porte-parole du ministère russe de la Défense, a explicitement nié l'utilisation de bombes incendiaires et affirmé que le rapport d'Amnesty International qui dénonçait l'utilisation de telles armes était truffé de « fausses informations » et de « clichés »[27]. Toutefois, le 18 juin 2016, RT (autrefois Russia Today) a diffusé une preuve saisissante depuis Hmeimim, base aérienne principalement russe située au sud-est de la ville de Lattaquié. Un

reportage sur la visite du ministre russe de la Défense à la base montrait des soldats montant des bombes à sous munitions incendiaires RBK 500 ZAB-2,5S/M sur un bombardier russe Su-34, chasseur d'attaque au sol exploité uniquement par la Russie en Syrie[28]. Cette partie de la vidéo a été retranchée de la version du reportage téléchargée sur YouTube par R[29].

À l'instar des frappes contre des hôpitaux, certaines des attaques à la bombe incendiaire signalées ont été solidement documentées et peuvent être vérifiées indépendamment. Une de ces attaques a été commise entre les villes de Rastane et de Talbiseh, dans la province de Homs, dans la nuit du 1er au 2 octobre 2016. Des médias locaux favorables à l'opposition ont téléchargé sur leur page Facebook une vidéo qui montrerait le moment de l'impact de la bombe incendiaire[30]. Dans les jours qui ont suivi, la Défense civile syrienne – les Casques blancs – a publié sur sa page Facebook des photos sur lesquelles il serait possible de voir des fragments d'armes[31]. Au moyen de photos de référence et des inscriptions qui figuraient sur ces vestiges, le Conflict Intelligence Team (CIT), groupe russe d'informatique judiciaire, a établi avec certitude qu'il s'agissait d'une bombe à sous-munitions incendiaires RBK-500 ZAB-2,5S/M[32].

L'enveloppe de la bombe portait une inscription en caractères cyrilliques : RBK 500 ZAB-2,5S/M. « ZAB » est l'abréviation du terme russe Зажигательная Авиационная Бомба (« bombe incendiaire aéroportée »). De plus, les vestiges de la bombe ressemblaient aux photos de référence de bombes incendiaires et à sous-munitions disponibles dans les sources ouvertes. Un gros fragment ressemblait fortement au couvercle (le nez) et à l'enveloppe cylindrique d'une bombe à sous-munitions de la série RBK-500, et il a été déterminé que les fragments plus petits provenaient de deux types différents de sous-munitions incendiaires : le ZAB-2,5S et le ZAB-2,5(M). Comme ces types d'armes n'avaient pas été répertoriés avant l'intervention de la Russie en Syrie, le CIT en a conclu que la frappe aérienne avait probablement été menée par les Forces aériennes russes. Le CIT n'a pas été en mesure d'établir si les immeubles ciblés étaient habités ou non : s'ils l'étaient, a-t-il soutenu, l'attaque aurait été illégale selon les conventions[33].

Les occasions

Même si le conflit en Syrie fait toujours rage et si Vladimir Poutine a réussi à acculer la communauté internationale à une impasse sur la façon de résoudre la crise, la campagne de désinformation de la Russie en Syrie montre des faiblesses qui sont autant d'occasions d'obliger les régimes et les gouvernements autocratiques à rendre des comptes.

À une époque hyperconnectée, réfuter un seul événement à la fois ne permet pas de faire beaucoup progresser la lutte contre la désinformation, sans compter que le problème de base demeure. Se contenter d'exposer les arguments contraires pour contrer la désinformation permet uniquement de traiter les symptômes sans attaquer la source du problème ni les méthodes employées dans les campagnes d'information. De plus, l'absence de résilience numérique, de lignes directrices gouvernementales et de programmes de sensibilisation pour munir les décideurs et les citoyens des outils adéquats laisse les sociétés vulnérables aux forces malveillantes qui savent comment profiter d'un tel vide.

> *Réfuter un seul événement à la fois ne permet pas de faire beaucoup progresser la lutte contre la désinformation.*

Il est nécessaire d'adopter une démarche qui permette aux gens non seulement de découvrir des informations sur la guerre de Poutine en Syrie, mais aussi de les vérifier eux-mêmes. Une telle démarche est aux antipodes de la campagne de désinformation opaque de la Russie, qui repose sur des discours idéologiques plutôt que sur des faits vérifiables. Les sociétés occidentales doivent s'armer de méthodes qui les aident à faire la distinction entre les faits et la fiction.

Seule une société civile ayant des assises solides peut être à même de dénoncer de façon crédible les crimes commis par des régimes. Plus Internet prendra de l'expansion, plus il sera essentiel d'adopter des solutions hyperconnectées pour entamer une démarche axée sur les méthodes afin de démasquer la désinformation pratiquée par des acteurs comme la Russie au Moyen Orient. Plus important encore,

plus les maîtres de la désinformation auront recours à l'intelligence artificielle et à l'apprentissage profond, plus il sera crucial de pouvoir compter sur une forte résilience numérique pour les décrédibiliser.

CHAPITRE 7

CONCEPTION CHINOISE DE L'INFORMATION ET DE L'INFLUENCE

Sous Xi Jinping, la Chine a intensifié ses efforts pour contrôler le cyberespace afin de renforcer l'autorité du Parti communiste sur la scène intérieure et d'exercer sa puissance douce à l'étranger. Ses activités de propagande ont été couronnées de succès sur son territoire; elles ont façonné les opinions de la population, qui est isolée de l'Internet mondial. À l'étranger, la Chine se représente efficacement comme une puissance montante, mais la propagande visant à faire connaître les objectifs de sa politique étrangère à l'échelle mondiale ne donne pas toujours les résultats voulus.

La Chine a entamé une nouvelle phase dans ses relations internationales qui témoigne d'un sentiment croissant de puissance et d'accomplissement, souvent formulé dans des expressions comme « atteindre le sommet » ou « revenir au centre de l'échiquier mondial ». Ce sentiment se manifeste par une tendance accrue à rejeter les normes occidentales (ou à les remplacer par des normes « aux couleurs de la Chine ») et à revendiquer un rôle d'avant-plan à l'échelle mondiale. Sur la scène intérieure, cela suppose le resserrement et la multiplication des contrôles de l'information. Sur la scène internationale, cela se traduit par des efforts pour exercer son pouvoir de persuasion.

À sa position défensive de longue date, qui consiste à éviter les risques politiques liés à l'information et aux technologies de l'information (TI), et qui est au cœur de l'héritage léniniste du Parti communiste chinois (PCC), s'ajoutent maintenant des activités visant à transformer l'opinion et les règles mondiales pour mieux servir les intérêts de la Chine et la vision du monde du Parti. La politique de l'information de Beijing vise à réduire les risques pour la stabilité politique et l'autorité du Parti, à promouvoir la technologie et le contenu chinois,

à redéfinir les règles mondiales en faveur des intérêts de la Chine et à défendre le pays contre la prétendue hégémonie des États-Unis. Au cours des dernières années, la Chine s'est dotée de politiques et de règlements visant à faciliter sa mainmise sur le contexte de l'information dans le pays, notamment la Stratégie nationale de sécurité du cyberespace publiée en 2016. Elle est également devenue beaucoup plus sûre d'elle dans son rejet des valeurs universelles, qu'elle affirme être plutôt « occidentales ».

Les dirigeants chinois voient dans Internet une menace existentielle pour la stabilité et le maintien du régime du PCC. Cette vision s'est intensifiée sous Xi Jinping. Ce dernier a hérité en 2012 d'une crise à évolution lente qui menaçait la continuité, et son gouvernement a réagi fermement. Ses efforts pour assurer la stabilité économique, endiguer la corruption, réformer l'Armée populaire de libération et imposer de vastes contrôles d'Internet ont renforcé son autorité et réduit le risque d'instabilité politique.

La menace que représente Internet est maintenant aussi vue comme une occasion. Depuis la révolution communiste, la Chine utilise la propagande et l'information pour avoir la haute main sur sa population, mais depuis l'arrivée au pouvoir du président Xi, elle cherche à atteindre un auditoire mondial de la même façon. Cet objectif témoigne de sa conviction d'être résolument engagée sur la voie pour supplanter les États-Unis à titre de nation la plus puissante au monde et, par conséquent, étendre et peut-être imposer ses valeurs. Beijing a entrepris de s'affirmer par la persuasion il y a une dizaine d'années, lorsque l'ancien chef du PCC Hu Jintao a appelé à rendre « l'idéologie socialiste plus attirante et harmonieuse ». Les représentants officiels du Parti parlent du retour imminent de la Chine au sommet des puissances douces à mesure qu'elle accède à un statut de « ténor du discours » correspondant à sa puissance économique[34].

Pour lutter contre la menace que représente l'information, la Chine a notamment entrepris d'isoler ses réseaux nationaux le plus possible, de bâtir des industries nationales pour produire des technologies chinoises et de remplir les médias d'informations et de nouvelles contrôlées par le gouvernement. Elle a recours à la censure et aux

trolls pour orienter les médias sociaux de façons favorables au régime et dommageables aux États-Unis. Très efficace pour les auditoires chinois, cette démarche est cependant presque totalement inefficace pour les auditoires étrangers.

La Chine a une vision cohérente du cyberespace qui place la souveraineté de l'État au cœur de sa politique d'information. Elle défend une vision très différente de l'ordre mondial selon laquelle elle réaffirme la primauté de la souveraineté nationale et dévalue les ententes internationales qui limitent la souveraineté, particulièrement la Déclaration universelle des droits de l'homme. Elle n'est d'ailleurs pas seule à cet égard : elle reçoit un soutien important de quelques pays non alignés et, bien sûr, de la Russie. Il existe une corrélation entre la disposition d'un pays à restreindre la liberté d'expression et la probabilité qu'il partage les opinions de la Chine sur Internet et le cyberespace.

Il existe une corrélation entre la disposition d'un pays à restreindre la liberté d'expression et la probabilité qu'il partage les opinions de la Chine sur Internet et le cyberespace.

L'accent sur la souveraineté a été accompagné d'une réorganisation majeure de l'appareil du gouvernement et du Parti pour faire face au cyberespace, dont la création en 2014 d'un Groupe dirigeant central sur la cybersécurité et l'informatisation dirigé par le président Xi et de l'Administration chinoise du cyberespace (ACC). Parmi les autres mesures visant à renforcer le contrôle intérieur figurent la restriction des réseaux privés virtuels (RPV), la perturbation du service qu'ils offrent ainsi que l'imposition de nouvelles limites aux médias sociaux par la suppression d'articles et la fermeture de comptes. Le Groupe dirigeant établit les politiques que l'ACC met en œuvre, améliorant le contrôle que Beijing exerce sur les réseaux chinois et les utilisateurs d'Internet. Ces changements découlent du vif intérêt du président Xi envers l'élargissement de la mainmise de la Chine au cyberespace, qui est qualifié (tout comme la corruption) de menace considérable pour la stabilité politique et le régime du PCC.

La Chine se sert de sa Conférence mondiale sur Internet (CMI) pour recueillir des appuis pour ses idées de « cybersouveraineté » et d'approche multilatérale de la gouvernance d'Internet, mais depuis 2014 (année de la première CMI), elle lui a donné une orientation plus nationale qu'internationale. Cette réorientation témoignait premièrement de l'échec de la CMI à attirer un auditoire étranger d'influence et, deuxièmement, de la confiance accrue de Beijing dans sa capacité de gérer Internet et d'étendre sa souveraineté aux réseaux même s'il n'est pas en mesure d'élargir sa mainmise sur la gouvernance d'Internet. En règle générale, de nombreux décideurs chinois croient qu'ils vont atteindre leurs objectifs avec le temps, étant donné que la tendance est favorable à la Chine dans les événements internationaux. Cette tendance pourrait expliquer, en partie, pourquoi la CMI tenue du 3 au 5 décembre 2017 a attiré des leaders technologiques bien connus de partout dans le monde.

C'est le Parti, et non l'individu, qui jouit de la primauté. La Stratégie nationale de sécurité du cyberespace précise que : « la souveraineté nationale s'étend au cyberespace, et la cybersouveraineté est devenue une part importante de la souveraineté nationale ». Lors de la CMI de 2016, le président Xi a défini les éléments de la cybersouveraineté de la façon suivante : « respecter le droit de chaque pays de choisir comment il développe Internet, son modèle de gestion et ses politiques publiques connexes, et de participer sur un pied d'égalité à la gouvernance internationale du cyberespace, c'est-à-dire éviter les situations d'hégémonie et l'ingérence dans les affaires internes des autres pays[35] ». Les opinions de la Chine sur la souveraineté réaffirment le rôle dominant de l'État dans une approche de la mondialisation qui cherche à modifier les règles, les institutions et les normes de façons favorables à ses propres intérêts et plus conformes à ses propres points de vue politiques.

Beijing a réussi à étendre sa souveraineté à Internet. Il bloque l'accès aux sites étrangers qu'il n'approuve pas et le trafic qui en provient. Tout aussi important, il oriente les nouvelles intérieures de façons favorables au Parti, mettant l'accent sur la force, la croissance économique, le prestige grandissant de la Chine et, récemment, la sagesse de Xi Jinping. Il est facile de faire peu de cas de l'efficacité de

ces efforts, et une proportion considérable des internautes chinois se moquent des positions officielles ou se disent sceptiques à leur égard. La Chine utilise toute la gamme des médias – la presse écrite, la télévision, les films et Internet – pour servir son discours. Un sondage réalisé par la Pew Foundation et l'Académie chinoise des sciences sociales révèle qu'en ligne, les Chinois s'intéressent surtout au divertissement, aux sports et aux nouvelles de source chinoise et qu'en fait, la propagande est efficace.

Toutefois, le PCC craint aussi de perdre prise sur le sentiment nationaliste. Il s'agit d'un outil imprécis que Beijing utilise avec prudence. Des Chinois disent que les médias sociaux et les « révolutions de couleur » représentent une menace, parce qu'ils pourraient susciter des désordres intérieurs, mais croient que le Parti est en voie d'apprendre à les prendre en charge et à les utiliser à ses propres fins, par exemple en utilisant des fonctionnaires (l'équivalent chinois des trolls médiatiques russes) pour publier des millions de messages favorables au Parti et aux politiques chinoises dans les médias sociaux[36]. La Chine a trouvé des façons d'utiliser la révolution informatique pour élargir le contrôle social par la surveillance omniprésente des activités menées dans les secteurs urbains et en ligne.

Ce comportement souverain s'exprime dans la façon dont la Chine aborde les négociations multilatérales sur la cybersécurité, les normes de TI et la gouvernance d'Internet. Elle cherche à promouvoir la souveraineté de l'État et à servir ses intérêts commerciaux et sécuritaires. Dans sa nouvelle Stratégie nationale de sécurité du cyberespace, la Chine insiste sur la « concurrence de plus en plus féroce » pour « s'arroger le droit d'élaborer des règles ».

À l'ONU et ailleurs, les Chinois sont prudents et inflexibles dans les négociations internationales sur la cybersécurité, préoccupés par la nécessité de se protéger contre les États-Unis, qu'ils perçoivent comme un adversaire hostile et technologiquement supérieur dont les gestes sont, dans une large mesure, non entravés par le droit international et motivés par des projets visant à perturber la société chinoise. Beijing cherche à conclure des accords internationaux qui réduiraient

le risque politique et iraient dans le sens d'un renforcement de l'autorité gouvernementale sur Internet. Si la Chine justifie en partie son opposition aux normes par un rejet des valeurs « occidentales », elle bloque aussi les accords sur les normes qui pourraient servir à justifier des représailles contre elle à la suite de cyberactivités.

Promouvoir la technologie de l'information chinoise

Depuis son ouverture à l'Occident il y a plus de trente ans, Beijing cherche à se doter d'une solide industrie de la TI. Il s'agit d'une part importante de sa stratégie pour faire face à la cybermenace et au risque qui pèse sur sa sécurité informationnelle. Ses motivations pour élargir son industrie de la TI sont à la fois commerciales et politiques. La Chine emploie diverses stratégies pour supplanter les entreprises occidentales de TI, dont des barrières non tarifaires, des règles de sécurité, des mandats d'approvisionnement, l'acquisition (tant licite qu'illicite) de technologies étrangères, des investissements stratégiques et l'achat d'entreprises occidentales.

La Chine a accru sa participation à l'élaboration des normes internationales en matière de TI (qui relevait auparavant des entreprises occidentales), et ce, pour bénéficier d'un avantage commercial et pour réviser les normes, les protocoles et les architectures de façon à améliorer la capacité du gouvernement à gouverner le cyberespace. Pour certains, la course à l'élaboration des normes « 5G » des réseaux mobiles Internet est « la chance de la Chine de prendre la tête de l'innovation mondiale [37] ».

> *Un haut représentant chinois a déjà fait remarquer qu'il n'y aurait pas de Baidu si la Chine n'avait pas bloqué Google sur le marché chinois.*

Dans l'espoir de répéter le succès de Huawei, la Chine utilise des investissements gouvernementaux et des obstacles à l'entrée pour produire des champions dominants à l'échelle internationale. Elle a une stratégie bien financée pour créer une industrie chinoise destinée à supplanter les fournisseurs étrangers. Un haut représentant chinois a déjà fait remarquer qu'il n'y aurait pas de Baidu si la Chine n'avait

pas bloqué Google sur le marché chinois. Toutefois, même si elle lui permet de contrôler l'utilisation des médias sociaux par la population chinoise, sa politique de création d'entreprises de contrepartie et de blocage de services occidentaux (comme Weibo au lieu de Twitter) est inefficace à l'étranger.

Exercer sa puissance douce

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. Particulièrement efficace pour persuader le monde de son inévitable ascendant économique et pour exposer les lacunes des États-Unis, la propagande n'a cependant pas réussi à persuader un auditoire étranger que la Chine est une solution de rechange attirante.

Son inconfort face à la prédominance des médias occidentaux (comme la BBC ou CNN) et à leur capacité de créer un discours mondial a amené la Chine à créer des concurrents pour contester l'« hégémonie de l'information ». *Global Times* a été refait en 2009 pour fournir du contenu en langue anglaise reflétant une vision plus positive de la Chine et faisant état de critiques parfois virulentes des États-Unis. Des opinions semblables sont professées sur CCTV (la télévision centrale chinoise), qui diffuse des émissions en huit grandes langues étrangères, avec l'objectif explicite de jeter un éclairage plus favorable sur les événements en Chine. Des entreprises chinoises soutenues par l'État ont acheté des organes de presse (comme le South China Morning Post) dont elles pourraient réorienter les reportages et les politiques éditoriales en ce sens. Les administrateurs de l'acheteur chinois Alibaba ont affirmé que leur objectif était d'améliorer l'image de la Chine et d'offrir une solution de rechange au prisme des organes de presse occidentaux, qu'ils qualifient de tendancieux[38].

Les médias chinois utilisent les méthodes de leurs pendants occidentaux pour modeler les opinions nationales et étrangères tant de la Chine que des États-Unis de façons favorables à Beijing, allant

jusqu'à diffuser une vidéo de musique rap chinoise entrecoupée de déclarations officielles chantant les louanges du président Xi et du XIX[e] Congrès du PCC, dont même les mots d'ouverture sont en anglais. Si ces opérations d'information sont très efficaces pour influencer les opinions d'un auditoire chinois, elles le sont beaucoup moins dans d'autres arènes culturelles et linguistiques. Une application ludique permettant aux utilisateurs d'utiliser un téléphone intelligent pour « applaudir » le président Xi est devenue virale en Chine, mais a suscité peu d'intérêt à l'étranger.

La Chine a adopté une approche à la fois ferme et douce pour amener les entreprises occidentales qui ne veulent pas s'aliéner Beijing ou perdre leur accès au marché à s'autocensurer jusqu'à un certain point. Les producteurs de films occidentaux prennent garde de ne pas offenser les censeurs chinois (ainsi, dans la nouvelle version de *L'Aube rouge*, ce n'est soudainement plus l'Armée populaire de libération qui envahit les États Unis, mais bien l'armée nord-coréenne, ou encore, dans *Seul sur Mars*, la Chine sauve la NASA). La rediffusion des émissions qui présentent les États Unis sous un jour défavorable, comme *House of Cards* de Netflix, est autorisée en Chine (et de nombreux Chinois y voient un quasi-documentaire).

L'efficacité de ces efforts pour modifier les opinions étrangères sur la Chine reste à démontrer. Il est trop tôt pour évaluer l'effet des achats de médias effectués par le pays, mais Alibaba a acheté le *South China Morning Post* dans le but explicite d'offrir une couverture plus favorable de la Chine. La création d'Instituts Confucius, tentative maladroite d'exercer la puissance douce de la Chine aux États-Unis, où se trouvent la plupart d'entre eux, a donné des résultats mitigés, s'attirant des critiques de toutes parts sans améliorer de façon notable les opinions américaines sur la Chine[39]. De même, les efforts de la Chine pour influencer les opinions australiennes au moyen de dons politiques et par l'entremise d'organisations d'étudiants ou d'immigrants suscitent des préoccupations. Le message de la Chine demeure surtout attirant pour les Chinois qui vivent à l'étranger.

Contrairement à la Russie, la Chine n'a pas érigé en doctrine la pratique de la désinformation et l'obtention d'un « effet cognitif ».

Elle semble vouloir étendre aux auditoires étrangers les techniques qu'elle a mises au point pour exercer un contrôle interne. De prime abord, il semble que ses efforts sont plus efficaces à l'endroit de sa propre population. Beijing n'a pas réussi à concevoir de solution de rechange attrayante. Ses propres contraintes idéologiques, qui contiennent de plus en plus d'éléments du culte de la personnalité tel qu'il existait à l'époque de Mao, ne convainquent pas les auditoires étrangers. Les outils les plus efficaces de la Chine pour exercer une influence demeurent un mélange de coercition sur la scène intérieure et de pressions financières sur les auditoires étrangers.

> *Les outils les plus efficaces de la Chine pour exercer une influence demeurent un mélange de coercition sur la scène intérieure et de pressions financières sur les auditoires étrangers.*

Toutes ces activités laissent entrevoir une stratégie de contrôle de l'information cohérente et élaborée, dont la supervision est centralisée et qui vise à réduire au minimum les risques politiques et à servir le programme et le discours de la Chine à l'échelle internationale. La conception qu'a l'État chinois de l'information et de la TI comme des outils n'a pas d'égal dans les démocraties occidentales.

CHAPITRE 8

TROLLAGE PATRIOTIQUE : L'IMPACT DES MÉDIAS SOCIAUX AUX PHILIPPINES

Le réseau social d'actualité Rappler.com a documenté la dernière campagne présidentielle aux Philippines. Les médias sociaux ont été instrumentalisés pour mener une campagne extrêmement ciblée qui a permis à Rodrigo Duterte de remporter l'élection, puis qui a été retournée contre les détracteurs du président, les chefs de l'opposition et les médias traditionnels. Le gouvernement a ainsi réussi à étouffer les voix indépendantes en faveur de ses propres messages.

Une coalition de recherche internationale[40] propose la définition suivante d'une pratique qui a cours aux Philippines, le trollage patriotique : « l'utilisation de campagnes de harcèlement et de propagande haineuse en ligne, ciblées et parrainées par un État dans le but précis de réduire au silence et d'intimider des personnes »[41]. Comme près de 97 p. 100 des Philippins qui ont accès à Internet utilisent Facebook, leur vulnérabilité à de telles campagnes a été décelée et est exploitée ouvertement.

Avec l'aide de spécialistes des données, les journalistes de *Rappler* ont recensé dans les médias sociaux des centaines de sites Web et des millions de comptes et de groupes qui propagent constamment et méthodiquement de la désinformation aux Philippines. Ils ont ainsi constitué une base de données contenant plus de 11 millions de profils personnels et de 250 millions de commentaires publics (en mars 2017). Leur travail a démontré l'émergence et l'évolution d'un réseau complexe de trollage patriotique visant à faire élire et à soutenir Rodrigo Duterte, gagnant les élections présidentielles de 2016.

Pour essayer de comprendre l'ampleur et la puissance de ce réseau, *Rappler* a passé trois mois à retracer manuellement un échantillon constitué de 26 faux comptes Facebook formant un réseau de

« désinformation populaire planifiée ». Il s'est révélé que ces comptes avaient influencé jusqu'à trois millions d'utilisateurs. De plus, en novembre 2016, *Rappler* a recensé plus de 50 000 comptes Facebook contrôlés directement par le réseau de propagande, notamment de faux comptes (dont certains bénéficiaient clairement d'une gestion centralisée), des trolls rémunérés et de véritables partisans travaillant à convaincre leurs parents et amis. En avril 2017, des liens clairs avec l'État ont commencé à se dégager, plus particulièrement avec le bureau responsable des médias d'État, le Bureau des opérations de communication présidentielles (BOCP), qui relève du secrétaire Martin Andanar.

Au milieu de 2017, le trollage patriotique constituait le fondement de l'écosystème informationnel du gouvernement philippin, discréditant les institutions, les politiciens et les journalistes qui critiquaient ou remettaient en question ses décisions. La priorité de cet écosystème est de défendre le président Duterte, qui est maintenant le dirigeant philippin le plus puissant des trois dernières décennies, jouissant de cotes de popularité élevées. Duterte dispose d'une super majorité à la chambre basse du Congrès, nommera 13 des 15 juges de la Cour suprême et a essentiellement démantelé toute opposition efficace.

L'évolution de la machine et de ses cibles

La première campagne menée dans les médias sociaux en vue de faire élire un président aux Philippines a exploité la colère collective et légitime entre classes économiques. Ce réseau de campagne a joué un rôle clé dans l'élection du chef du pays, Rodrigo Duterte. Divisé en quatre groupes géographiques distincts, le réseau de diffusion sur Facebook recevait quotidiennement des messages d'un groupe de messagerie central qui travaillait avec des psychologues à élaborer des messages qui feraient appel aux émotions et dont la propagation deviendrait virale. Ironiquement, les réseaux créés dans les médias sociaux pendant la campagne ont été militarisés uniquement après l'intronisation de Duterte, le 30 juin 2016. Le président a alors décidé de boycotter les médias traditionnels pendant environ un mois, déclenchant la deuxième phase. Au cours de celle-ci, la machine a évolué, appliquant des stratégies plus ciblées et virulentes qui ont

transformé les comptes créés pour la campagne dans les médias sociaux en comptes destinés à attaquer les dirigeants de l'opposition et les médias traditionnels. Mettant à profit sa base imposante, elle a su, avec succès, réprimer le mécontentement et influencer l'opinion publique au sujet de politiques controversées, comme la guerre contre la drogue déclarée par le président Duterte, les théories conspirationnistes, la politique étrangère, la loi martiale et d'autres initiatives gouvernementales.

L'objectif du président Duterte était clair et efficace : faire perdre toute crédibilité à quiconque remettait en question ou critiquait le gouvernement. Les attaques brutales dirigées en ligne contre l'un ou l'autre citoyen, politicien ou journaliste, en vue d'en faire des exemples, ont eu un effet paralysant qui en a empêché de nombreux autres de s'exprimer. Une des premières cibles a été la sénatrice Leila de Lima, ancienne secrétaire à la Justice et ancienne chef de la Commission des droits de la personne des Philippines. D'autres politiciennes ont ensuite été prises pour cible en janvier 2017, dont la vice-présidente Leni Robredo et la sénatrice Risa Hontiveros.

> *La première campagne menée dans les médias sociaux en vue de faire élire un président aux Philippines a exploité la colère collective et légitime entre classes économiques.*

Le plus grand réseau de télévision du pays, ABS-CBN, et le plus grand journal, le *Philippine Daily Inquirer*, ont été les premières cibles médiatiques d'une campagne efficace visant à modérer les reportages critiques. L'*Inquirer* a été visé en raison de sa « liste des victimes », un tableau des personnes tuées au cours de la guerre contre la drogue. Peu après ces attaques concertées, l'*Inquirer* a cessé de tenir sa liste à jour, et les deux groupes médiatiques se sont rétractés sur le nombre de morts. En se fondant sur les chiffres publiés par la police, *Rappler* soutient que quelque 7 000 personnes ont trouvé la mort dans la guerre contre la drogue entre le 1er juillet 2016 et le 31 janvier 2017, soit environ 1 000 personnes par mois. Devant la condamnation croissante de la communauté internationale, le gouvernement des

Philippines a commencé à estomper les chiffres réels en modifiant ses définitions et en classant les décès faisant l'objet d'une enquête dans une nouvelle catégorie créée par la police.

Ces activités ont été suivies d'un des programmes de liaison les plus médiatisés du Palais présidentiel ou du BOCP. Sous le mot-clic #RealNumbersPH, le gouvernement a collaboré activement avec les blogueurs de la machine de propagande dans les médias sociaux pour exercer des pressions sur les médias traditionnels afin qu'ils modifient leurs chiffres de façon à ce qu'ils correspondent aux nouveaux « chiffres officiels ». Au cours de ces mois, quiconque soulevait sur Facebook la question de l'augmentation du nombre de morts dans la guerre antidrogue était attaqué brutalement. L'objectif final était de réduire les critiques au silence, créant efficacement ce que la théorie des communications de masse appelle une « spirale du silence[42] ».

> *Les attaques brutales dirigées en ligne contre l'un ou l'autre citoyen, politicien ou journaliste, en vue d'en faire des exemples, ont eu un effet paralysant qui en a empêché de nombreux autres de s'exprimer.*

Des journalistes et des groupes médiatiques qui avaient déjà pu s'enorgueillir des plus hautes cotes de crédibilité de toutes les institutions publiques et privées aux Philippines ont été attaqués et avilis systématiquement, d'abord dans les médias sociaux, puis par les représentants officiels du gouvernement (dont le président Duterte). Bon nombre des thèmes qui avaient été utilisés pour la première fois pendant la campagne électorale ont été repris et amplifiés, y compris les suivants : les journalistes sont corrompus, les organisations médiatiques appartiennent à des oligarques qui ont des intérêts particuliers, les manchettes sont des pièges à clics qui procurent des gains économiques en eux-mêmes. En 2016, le président Duterte a menacé publiquement et à maintes reprises ABS-CBN et le *Philippine Daily Inquirer*.

Le trollage patriotique a été tourné vers *Rappler* et son PDG après que l'entreprise eut publié un dossier en trois parties sur la propagande dans les médias sociaux au début d'octobre 2016. Étayé par des données, ce dossier dévoilait publiquement pour la première fois la véritable portée de la machine de propagande. Celle-ci a riposté immédiatement, réclamant des attaques contre le PDG de *Rappler* qui ont pris la forme de messages haineux (jusqu'à 90 à l'heure)[43] et d'une campagne dans les médias sociaux sous le mot-clic #UnfollowRappler qui a révélé l'ampleur de sa puissance dans le monde virtuel.

En novembre 2016, les données et le comportement en ligne démontraient que la machine pouvait mettre à sa disposition et influencer un peu plus de 52 000 comptes, un nombre important comparativement aux 30 000 comptes Facebook fermés au cours de la période qui a précédé les élections en France[44]. Soit dit en passant, Facebook a plus tard souligné que son travail pendant les élections en France avait été inspiré en partie par les données que *Rappler* lui avait fournies dès le mois d'août[45].

Détruire la confiance

La troisième vague d'attaques a commencé au début de janvier 2017, visant d'abord la vice présidente Leni Robredo et d'autres dirigeantes à coups de demi-vérités, de mensonges éhontés, de sexisme et de misogynie. Les femmes sont des cibles privilégiées qu'il est possible d'attaquer, de railler et de tourner en ridicule efficacement, souvent au moyen de jurons et d'insultes sexuelles dégradantes. Ces attaques presque constantes ont divisé davantage encore la société philippine et amplifié la spirale du silence.

Les comptes dans les médias sociaux qui soutenaient le gouvernement et qui auraient été financés par lui ont travaillé activement à miner la confiance envers l'opposition, alors pratiquement inexistante, le journalisme et d'autres sources d'informations fiables, cherchant à les remplacer par la voix du gouvernement amplifiée par les médias sociaux. Les sites de fausses nouvelles sont passés de 15 à plus de 300 en quelques mois, propagés par de faux comptes, des robots et des

« guerriers du clavier » semant la confusion et la méfiance, et offrant au gouvernement le plus formidable des mégaphones.

En février 2017, la machine de propagande s'est concentrée sur *Rappler* dans des attaques presque quotidiennes visant à présenter la jeune entreprise comme la propriété ou le pantin d'intérêts étrangers et cherchant à influencer l'évolution de la situation aux Philippines. Malgré des dénis répétés, de nombreux partisans de Duterte ont cru ce discours martelé à maintes reprises par des blogueurs favorables au président et réitéré plusieurs mois plus tard par le président lui-même dans son bilan annuel sur la situation actuelle.

Au milieu de l'année, les attaques contre les médias se sont intensifiées. Le président Duterte a de nouveau attaqué publiquement ABS-CBN et le *Philippine Daily Inquirer* pendant que la machine de propagande essayait de promouvoir le mot-clic #ArrestMariaRessa et de présenter *Rappler* comme un outil d'ingérence étrangère dans les médias sociaux.

Attaques commanditées par l'État

À ce moment-là, il était clair que la machine de propagande en ligne servait de signe avant coureur et de ballon d'essai aux messages et aux attaques du gouvernement contre ceux qu'il considérait comme ses détracteurs. *Rappler* a identifié trois principaux créateurs de contenu de la machine propagandiste, qui segmentait la société philippine en fonction de caractéristiques économiques : Sass Sassot pour les articles pseudo-intellectuels destinés au 1 p. 100 supérieur, Thinking Pinoy (RJ Nieto) pour la classe moyenne et Mocha Uson pour le peuple.

Le gouvernement a bouclé la boucle en offrant des postes de fonctionnaire à Mocha Uson et à RJ Nieto : le premier a été nommé secrétaire adjoint responsable des médias sociaux au BOCP, tandis que le second est employé du ministère des Affaires étrangères et du ministère des Transports. Leurs réseaux sont aussi la première ligne d'alerte et de défense du gouvernement en matière de gestion de crise. Le 23 mai 2017, le gouvernement philippin a instauré la loi martiale sur l'île de Mindanao, modifiant considérablement le

contexte. Il en a fait l'annonce à Moscou au cours d'une visite d'État en Russie, à laquelle participaient Mocha Uson et RJ Nieto, et il a aidé à préparer le terrain pour la quatrième vague d'attaques combinant mesures gouvernementales en ligne et dans le monde réel en vue de limiter la liberté de presse.

Le 17 juillet, le *Philippine Daily Inquirer* a tenu une assemblée générale et informé ses employés que le journal serait vendu à Ramon Ang, homme d'affaires ayant des liens étroits avec le président Duterte. Ce fait nouveau est survenu après que des poursuites eurent été intentées contre la famille propriétaire de l'*Inquirer*, que les membres du conseil d'administration eurent été menacés de poursuites en vertu des lois sur l'impôt et qu'un boycott informel de la publicité eut fait chuter les revenus du journal d'au moins 40 p. 100.

Une semaine plus tard, dans son bilan annuel de la situation actuelle, le président Duterte a attaqué *Rappler*[46] de même qu'ABS-CBN, les Nations Unies, Barack Obama, la Cour pénale internationale et d'autres. Il est revenu à la charge contre *Rappler* trois fois au cours des trois semaines suivantes. Les incidents de harcèlement ont commencé la même semaine, un des blogueurs favorables à Duterte publiant tous les états financiers de *Rappler* sur Facebook. Ce geste a été suivi d'un nombre sans précédent de demandes et d'appels de la Securities and Exchange Commission, qui a chargé un comité spécial d'amorcer une enquête.

Le rôle des géants américains de la technologie et le chemin à parcourir

L'ironie, bien sûr, tient au fait que la plus grande menace pour la démocratie aux Philippines est facilitée par des entreprises américaines : Facebook[47], Google et Twitter. YouTube, deuxième moteur de recherche en importance au monde, exploité par Google, est aussi une plateforme de prédilection efficace pour les attaques vidéo. L'explosion de l'information et de la boîte noire que sont les algorithmes a démoli le rôle de gardien du journalisme, retirant le discours collectif aux rédacteurs humains pour le confier aux machines et aux algorithmes.

Selon un rapport publié en novembre par Freedom House, il ressort des plus récents rapports et analyses que ce retour en arrière de la démocratie se produit dans au moins trente pays[48]. À court terme, la protection de la démocratie incombe à ces entreprises américaines qui doivent apprendre à faire face aux répercussions des systèmes complexes qu'elles ont créés. À moyen terme, il est nécessaire d'améliorer les connaissances médiatiques et de reconnaître l'existence de ce monde d'informations exponentielles qui met dans le même sac vérités et mensonges. À long terme, l'éducation est la clé.

> *À moyen terme, il est nécessaire d'améliorer les connaissances médiatiques et de reconnaître l'existence de ce monde d'informations exponentielles qui met dans le même sac vérités et mensonges.*

Les géants de la technologie doivent intégrer la démocratie dans leurs algorithmes et empêcher les gouvernements autocratiques de constituer des armées en ligne. Il s'agit d'une proposition difficile, compte tenu des intérêts économiques concurrentiels des plateformes et de leurs mandats de croissance.

CHAPITRE 9

LUTTE CONTRE LA DÉSINFORMATION EN UKRAINE

StopFake.org, qui a d'abord été un moyen de réfuter les faux reportages russes sur l'Ukraine, est maintenant devenu un centre international d'information sur la propagande du Kremlin. Son équipe de journalistes a mis en œuvre de nombreux outils pour débusquer les messages de la Russie, discréditer la propagande russe et offrir des programmes de formation axés sur l'éducation aux médias.

Le site StopFake.org consiste en un projet de vérification des faits qui a pour but de débusquer les fausses nouvelles de façon à contrer la désinformation et la propagande russes. Des professeurs, des étudiants et des diplômés de l'école de journalisme de l'Académie Mohyla à Kiev ont lancé le site en 2014 par suite de l'annexion de la Crimée et de la guerre de la Russie contre l'Ukraine dans le Donbass. Au départ, il s'agissait de vérifier les informations et de contrer la désinformation et la propagande dans les médias concernant les événements en Ukraine. Le projet a pris de l'ampleur et s'est transformé en un réseau d'information qui s'emploie à examiner et à analyser soigneusement tous les aspects de la propagande du Kremlin.

Jusqu'à présent, les trente membres de l'équipe ont débusqué plus d'un millier d'articles des médias grand public russes (chaînes de télévision, journaux, agences de presse) en onze langues. Le contenu – des publications texte, audio et vidéo, des émissions de télévision et de radio sous licence, un journal local du Donbass et un documentaire – est suivi par 230 000 abonnés sur les médias sociaux et par de nombreux autres intéressés en personne. Le site StopFake.org détient les archives les plus vastes sur les fausses nouvelles russes, et l'équipe responsable vérifie les faits et effectue des recherches en plus de démystifier, de corriger, de traduire et de diffuser l'information.

Surveiller, débusquer, archiver et préciser les principaux messages

La guerre à laquelle la Russie se livre contre l'Ukraine témoigne des activités modernes de propagande du Kremlin dans le monde tout en s'inscrivant dans le droit fil des méthodes soviétiques, actualisées dans le but d'accroître leur incidence et leur efficacité.

La télévision demeure l'un des principaux outils d'ingérence et de désinformation en Russie et à l'étranger. Margarita Simonian, rédactrice en chef de RT, explique l'importance de ce mode de communication de la façon suivante : « Dans une certaine mesure, si [un pays] n'assure pas une diffusion à l'étranger, c'est comme s'il n'avait pas d'armée. En période de paix, l'armée n'est pas nécessaire. En revanche, si une guerre éclate, il est impossible de monter une armée en une semaine[49]. » Bien avant le début de l'annexion de la Crimée, l'exploitation de la télévision russe constituait un moyen des plus utiles pour influencer l'opinion publique en Ukraine. Toutes les grandes chaînes étaient accessibles librement en Ukraine, et des installations techniques sous le contrôle de l'État ukrainien servaient à transporter et à amplifier les signaux. Le contenu télévisuel russe était très populaire en Ukraine en raison de la proximité linguistique des deux pays et d'une économie des médias partiellement intégrée.

> *(...) la désinformation témoigne des activités modernes de propagande du Kremlin dans le monde tout en s'inscrivant dans le droit fil des méthodes soviétiques (...)*

À la même époque, d'autres segments du système médiatique russe dominaient l'univers médiatique ukrainien. Peu à peu, les médias d'information en ligne, les médias sociaux et l'industrie du divertissement partagée, entre autres, ont commencé à faire office d'armes, et les médias russes se sont employés à fabriquer et à diffuser de faux textes, des titres manipulateurs, des images truquées, des allégations trompeuses et des documents contrefaits ainsi qu'à mettre en scène des imposteurs se faisant passer pour des experts, des sources

médiatiques et des témoins. Tout ce contenu a donné lieu à une série de faux messages qui ont été relayés en Russie, en Ukraine et partout dans le monde dans le but de déprécier divers aspects de la vie en Ukraine. Pour maximiser les effets de la désinformation, les mêmes messages étaient répétés, traduits et amplifiés dans les médias sociaux.

L'équipe responsable du site StopFake.org a principalement pour but de débusquer les faux messages, de faire connaître ses conclusions à différents auditoires et de créer des archives. Des analyses préliminaires de 500 articles de désinformation produits par des agents de propagande russes sur l'Ukraine en 2014 et en 2015 ont fait ressortir d'importants messages fabriqués de toutes pièces. Voici quelques exemples :

- informations présentant l'Ukraine comme un État fasciste et déliquescent dont le territoire se désagrège continuellement, qui est perpétuellement en conflit ou qui risque toujours d'être annexé par ses voisins et l'Occident;
- fausses informations sur les relations politiques ou économiques de l'Ukraine avec ses partenaires à l'étranger, notamment au sujet de la délégitimisation de l'Union européenne et de l'Organisation du Traité de l'Atlantique Nord, de l'assistance que prêtent à l'Ukraine des pays étrangers et de leurs intentions là-bas; et
- informations selon lesquelles la Russie ne s'ingère pas dans les affaires de l'Ukraine, dont des messages niant l'occupation russe et l'implication de la Russie dans l'écrasement du vol MH17.

Une analyse approfondie a révélé que Zvezda TV, propriété du ministère russe de la Défense, était à l'origine du plus grand nombre de fausses nouvelles sur l'Ukraine (79 cas). Les deuxième et troisième rangs étaient occupés respectivement par Ukraine.ru (73 cas), un site Web de Russie qui appartient à l'agence de presse Novosti, propriété des autorités russes, et l'agence de presse RIA Novosti elle même (62 cas).

L'ensemble du système médiatique russe sert l'objectif du Kremlin lorsqu'il s'agit de fabriquer et de diffuser de fausses nouvelles.

Tant les médias qui relèvent de l'État que ceux qui appartiennent au secteur privé (mais sous contrôle de l'État) jouent un rôle dans le système de propagande russe, le rôle principal revenant à la télévision et à Internet. Fait important, les analyses montrent que l'ensemble du système médiatique russe sert l'objectif du Kremlin lorsqu'il s'agit de fabriquer et de diffuser de fausses nouvelles. Ce système représente une pierre angulaire de l'infoguerre à laquelle la Russie se livre en Ukraine.

Démonter les activités d'agitation et de propagande de la Russie et sensibiliser l'opinion publique au pays et à l'étranger

Le Kremlin répand sa propagande dans des langues autres que le russe et partout dans le monde. Les russophones sont certes plus susceptibles de suivre les médias nationaux russes, mais l'agence de presse RT (anciennement appelée Russia Today) mène des activités en cinq langues et l'agence Sputnik, en 31 langues. Qui plus est, des sites Web non retraçables et des trolls sont actifs dans beaucoup d'autres pays et dans une multitude de langues. Comme la propagande russe déborde les frontières linguistiques et géographiques, la sensibilisation du public constitue une grande priorité.

Au début de 2017, une enquête de StopFake.org a mis au jour la perception qu'ont les Ukrainiens de la propagande russe et leur résilience à son égard :

- la majorité des citoyens ukrainiens (58,3 p. 100) croient qu'il y a un risque de propagande russe en Ukraine;
- les Ukrainiens considèrent les chaînes de télévision, les médias en ligne et les réseaux sociaux russes comme les principaux modes de diffusion de la propagande du Kremlin (45 p. 100, 34,5 p. 100 et 19,8 p. 100 respectivement);

- la majorité des citoyens ukrainiens (59,7 p. 100) s'estiment aptes à faire la distinction entre le vrai et le faux dans les médias; et
- dans l'ensemble, 42,1 p. 100 des répondants se sont dits d'avis que la désinformation est un problème grave dans les médias russes.

Le retrait des ondes de 75 chaînes de télévision russes accessibles en Ukraine a grandement contribué à soustraire la population ukrainienne du réseau de propagande du Kremlin. Ce retrait, ordonné par un tribunal ukrainien au début de la guerre du Donbass en 2014, a entraîné une forte baisse du pourcentage de téléspectateurs visionnant les chaînes de nouvelles russes en Ukraine : de 12 p. 100 en 2015, ce pourcentage est passé à 7 p. 100 en 2016 et à 5 p. 100 en 2017.

En outre, la diminution de la popularité des médias russes en Ukraine résulte des restrictions dont font dorénavant l'objet les entreprises de médias sociaux russes là bas. En mai 2017, le président ukrainien Petro Porochenko a signé un décret qui prévoit une large gamme de sanctions, dont l'interdiction d'exploitation des réseaux sociaux russes en Ukraine. L'incapacité des fournisseurs de services Internet ukrainiens à offrir l'accès aux réseaux sociaux russes a eu une incidence considérable. En effet, selon SimilarWeb, le nombre de visites par jour sur le site VKontakte en Ukraine a connu une baisse de 60 p. 100 en 2017 – passant de 9,8 millions à 3,8 millions – et le nombre de visites quotidiennes sur le site Odnoklassniki (« camarades de classe ») a chuté de 64 p. 100 – passant de 4,6 millions à 1,6 million. Ces deux sites de réseautage social hébergeaient des milliers de groupes anti ukrainiens et diffusaient de la propagande, en plus de servir d'outils opérationnels pour recueillir des fonds et retenir les services de mercenaires en vue de la guerre dans le Donbass.

Le nombre de visiteurs sur le moteur de recherche russe Yandex – qui offre un éventail de services personnalisés et recueille des données de géolocalisation et autres sur les utilisateurs ukrainiens – a diminué de 65 p. 100 : de 5,9 millions, il est passé à 2 millions de visites par jour. Mail.ru, l'un des services de courriel les plus utilisés en Ukraine, a perdu 55 p. 100 de sa clientèle ukrainienne. Les militaires qui

composaient la majeure partie de cette clientèle voyaient régulièrement apparaître de fausses nouvelles russes dans la section publicitaire du site.

Diffuser le savoir et promouvoir l'éducation aux médias

En Ukraine, l'équipe de StopFake.org s'emploie également à améliorer l'éducation aux médias auprès de divers groupes cibles, tout particulièrement les habitants du Donbass et de la Crimée (bien qu'il lui soit difficile, pour des raisons évidentes, d'établir un lien avec eux).

En 2015, l'équipe a organisé des formations sur l'éducation aux médias à l'intention du grand public dans l'est et le sud de l'Ukraine. Le projet prévoyait des formations destinées aux formateurs, la conception d'un programme de cours et d'un guide de formation ainsi qu'une série de séances de formation intensives d'une journée pour les groupes susceptibles de faire les frais de la propagande russe. La formation s'accompagnait dans les médias locaux et nationaux (télévision, radio, bannières sur les sites Web de nouvelles et de réseaux sociaux, et publicités à l'extérieur) d'une vaste campagne de promotion de l'éducation aux médias dans le cadre de laquelle les citoyens se voyaient offrir des outils pour vérifier les faits. Le projet a permis à plus de 15 000 personnes de suivre une formation sur les compétences de base nécessaires pour porter un œil critique sur les médias.

Les Ukrainiens ont toujours du mal à comprendre les problèmes associés à l'ère de la postvérité. Selon un sondage de février 2017, la plupart des répondants, surtout ceux parmi les groupes d'âge inférieurs et intermédiaires, connaissaient et comprenaient le concept des fausses nouvelles, mais il s'agissait tout de même d'un concept flou pour bon nombre d'entre eux. Tous les répondants, même les plus jeunes, ont souligné que l'expression ne faisait pas partie de leur langage courant et ont affirmé l'associer à l'argot des jeunes et des adolescents. En revanche, le concept de propagande était compris de la plupart des répondants, surtout ceux des groupes d'âge intermédiaires et supérieurs qui s'étaient intéressés à la politique pendant l'ère soviétique. Comme les jeunes sont les plus susceptibles

d'utiliser les plateformes de médias sociaux, de telles conclusions mettent en évidence le caractère essentiel des cours sur l'éducation aux médias.

Pour internationaliser ses travaux, l'équipe de StopFake.org collabore avec de nombreux organismes et réseaux de vérification des faits partout en Europe. Elle entend ainsi faire connaître l'exemple de l'Ukraine, sensibiliser la population mondiale à la désinformation russe et à l'ingérence du Kremlin dans les processus politiques et décisionnels et lancer un débat politique sur la désinformation dans d'autres pays.

CHAPITRE 10

LA RENTABILITÉ DU FAUX : LES ACTEURS NON ÉTATIQUES ET L'INDUSTRIE DE LA DÉSINFORMATION

Les entrepreneurs de fausses nouvelles profitent de la publicité fondée sur le nombre de clics qui vise les lecteurs de nouvelles sensationnalistes et ceux qui consultent l'actualité uniquement sur les sites d'agrégation de nouvelles. Ces entreprises maximisent leur lectorat et leur potentiel de piège à clics en achetant les pages de groupes comptant un nombre suffisant de membres correspondant au profil démographique ciblé. La vérité, la fausseté et la teneur du contenu de leurs nouvelles n'ont aucune importance : leur seul objectif est d'attirer des lecteurs qui verront les publicités.

Le présent rapport repose principalement sur une longue entrevue menée auprès d'un Kosovar dénommé Burim (nom fictif), âgé de vingt-quatre ans, qui est titulaire d'un baccalauréat en informatique. Il a travaillé dans le domaine des technologies de l'information pour une entreprise privée à Pristina, la capitale du Kosovo, de même que dans le domaine de la publicité. Depuis janvier 2016, Burim est le propriétaire-exploitant d'un commerce en ligne spécialisé dans la désinformation et les pourriels.

Réalisée au Kosovo en juin 2017, l'entrevue, qui s'inscrivait dans une vaste démarche, devait servir à mettre en lumière le phénomène de la désinformation, grâce à un aperçu de la vie, des motivations, des croyances et des angoisses d'une personne comme Burim. La production de désinformation est un phénomène sans nul doute étroitement lié aux technologies qui permettent de publier et de consommer du contenu. Or, comme il s'agit également d'un choix qui est fait sciemment, souhaitons que le présent article apporte un éclairage utile sur les motivations profondes des personnes qui agissent ainsi.

Public cible

Le commerce de Burim vise principalement à attirer l'attention, et Facebook est la seule plateforme qu'il utilise pour y parvenir. À tous moments, Burim « possède » environ une dizaine de pages Facebook. L'une d'elles semble être celle d'un groupe évangélique, et un grand portrait du Christ y est bien en évidence. « Je l'ai achetée, affirme-t-il. Cet homme d'Albanie a développé cette page en publiant de l'information religieuse authentique. Il a réussi à obtenir 100 000 mentions "J'aime". Puis, il m'a transféré la page en échange de 2 000 euros. » Burim possède d'autres pages : une porte sur des endroits abandonnés; une autre vise à mobiliser des collectivités dans une ville du sud des États-Unis; une achetée tout récemment appartenait au départ à un groupe spécialisé dans la communication de conseils et d'informations sur les régimes et le végétalisme; une traitait de minimaisons et une autre encore était une page vérifiée — elle contenait un crochet bleu et un logo — qui avait quelque chose à voir avec la confiance. C'était rendu assez difficile de vraiment savoir de quoi traitait à l'origine la plupart des pages de Burim. Cependant, même si les groupes étaient bizarres en soi, leur public était gigantesque : 90 000 mentions « J'aime », 240 000 mentions « J'aime », 26 000 mentions « J'aime ». Dans sa quête de fidélisation d'un public, Burim pourrait, du moins en théorie, présenter son contenu à près d'un million de personnes.

Il a acquis les groupes de différentes façons. Il avait une page maîtresse qu'il avait lui-même créée et dans laquelle il a investi 20 000 euros en publicité ciblée sur Facebook afin de faire grimper le nombre de membres à un peu plus de 100 000. Cette page, la plus honnête qu'il ait jamais possédée, visait précisément à transmettre au quotidien les histoires virales et en vogue. Or il a acheté la plupart de ses groupes. Dans certains cas, Burim communique directement avec l'administrateur d'un groupe afin de savoir s'il est prêt à vendre : « Quand je tombe sur quelque chose d'intéressant, j'essaie de l'acheter ». Mais la plupart des groupes ont été achetés auprès de réseaux informels qui se livrent eux-mêmes à l'achat et à la vente de pages, dans le but premier de produire des pièges à clics et des pourriels.

« Nous ne savons jamais à l'avance si les groupes fonctionneront, explique Burim. C'est pourquoi nous publions d'abord un peu de contenu, puis nous attendons trois ou quatre heures pour voir combien de personnes seront incitées à cliquer pour en savoir davantage. Voilà comment nous déterminons si une page sera ou non utile. » Burim et son équipe testent chacun des groupes nouvellement acquis; ils vérifient le nombre de clics et de publications partagées que suscite le contenu. Les utilisateurs Facebook ciblés sont « de préférence des Américains sans habileté numérique et habituellement âgés de 30 ans ou plus ». Les groupes dont les publics sont trop jeunes de même que tous les groupes soupçonnés de comporter un trop grand nombre de membres versés en technologie sont délibérément évités. « Nous cherchons à joindre des personnes qui ne comprennent pas le monde numérique ni les pièges à clics. » Si le contenu ne pique pas la curiosité des internautes, le groupe est rapidement vendu, et le capital ainsi libéré peut être investi dans un autre groupe.

Contenu

Burim emploie sept personnes : celles-ci font circuler du contenu par l'entremise de ses groupes, mais n'en rédigent pas. Au plan économique, il n'y a aucun intérêt à créer du contenu alors qu'il est si facile de le voler ailleurs. Ses employés trouvent plutôt du contenu qui a été grandement partagé, habituellement par l'entremise d'un nombre infini de commerces similaires aux leurs, et se l'approprient. Il est particulièrement difficile de retracer l'origine de la plupart des récits qu'ils partagent. Lorsqu'il circule d'un endroit à un autre, le contenu fait souvent l'objet de changements subtils. Il est parfois raccourci, parfois exagéré ou simplifié. Burim compare ce processus à un lave linge : le contenu est sans cesse en mouvement et chaque « lavage » semble le modifier légèrement — rétrécissement, déformation, exagération ou enjolivement—, au point d'en occulter l'origine désormais sans importance.

Le contenu politique n'intéresse pas particulièrement son public cible. « Les récits de meurtres et les histoires scabreuses sont, essentiellement, celles qui obtiennent le meilleur rendement! », d'affirmer Burim, d'un ton jovial. Il fait défiler une longue suite

d'articles : « Toiletteur toujours en liberté après avoir brutalisé un chien et lui avoir fracturé toutes les côtes »; « Il sort du coma au bout de douze ans et murmure un terrible secret à ses parents [vidéo] »; « Treize bienfaits pour la santé de feuilles de laurier consumées »; « Déceler rapidement la maladie d'Alzheimer à début précoce avec du beurre d'arachides. À voir absolument! » Certains n'ont été partagés que des centaines de fois par l'entremise de ses groupes, tandis que beaucoup d'autres l'ont été des milliers de fois, voire des dizaines de milliers de fois pour quelques-unes. Selon Burim, il ne fait que donner aux gens les articles sur lesquels ils veulent cliquer, et le contenu en dit long sur les espoirs, les craintes, les plaisirs coupables et les tentations de son public : être en santé (grâce à des trucs et à des conseils faciles); exprimer son indignation à l'égard de situations (clairement) abusives. En somme, le ridicule, le tragique et le sordide.

Qualifier cette activité de « fausses nouvelles », c'est passer à côté de l'essence même de ce phénomène. Les récits ne sont ni délibérément faux, ni délibérément vrais. Ils visent d'abord et avant tout à susciter l'intérêt du plus grand nombre d'internautes. « Je me moque de ce que le groupe fait, a affirmé Burim. Je ne lis même pas le contenu. À vrai dire, c'est la première fois que je le lis. C'est un ramassis d'absurdités. » Que le contenu soit vrai ou faux importe peu. « Je m'en moque », a-t-il répété, tout en continuant de faire défiler le contenu sans fin produit par son commerce. Il s'est arrêté un instant, le curseur immobilisé au-dessus d'un récit provoquant un emballement soudain et immense chez les internautes au point d'être partagé non pas des dizaines, mais des centaines de milliers de fois. « Tout ce qui m'importe, c'est le trafic. »

> *Ils visent d'abord et avant tout à susciter l'intérêt du plus grand nombre d'internautes.*

Argent

Lorsqu'ils cliquent sur l'un des récits que son équipe a publiés, les internautes sont réorientés vers les activités lucratives du commerce de Burim. Il compte environ une dizaine de pages Web ailleurs que

sur Facebook et change les adresses URL pour éviter de se faire repérer. Ces pages ressemblent à des versions rudimentaires d'un journal en ligne, les articles complets étant accessibles sous diverses rubriques : « Accueil », « Santé », « Bricolage », « Animaux », « Alimentation », entre autres choses.

La publicité programmatique, en plein essor, élargit l'horizon de Burim et de ses semblables. Elle constitue une solution de rechange à la publicité de marque traditionnelle qui passe par les médias radiotélévisés. Des logiciels sont utilisés pour acheter des espaces publicitaires partout où un membre du public cible apparaît sur Internet, souvent repéré grâce à des témoins, aux données d'identification d'un appareil ou à des fournisseurs spécialisés dans les technologies publicitaires. Le but n'est pas de vendre des espaces publicitaires sur un site Web, et encore moins dans un journal, mais plutôt des espaces publicitaires que verront les personnes visées, où qu'elles se trouvent. Cela étant, Burim n'a pas eu à essayer de vendre des espaces publicitaires directement à des agences. Il pouvait les vendre par l'entremise d'intermédiaires de publicité programmatique et, à l'instar de tout journal (légitime), il a tiré ses revenus principalement de Google AdSense, soit de la publicité paiement au clic.

Burim réalise grâce à ses activités commerciales des gains allant de 400 à plusieurs milliers d'euros par jour; où que l'on soit, de tels revenus constituent un salaire décent, mais au Kosovo, ils représentent une somme très importante. Burim a le sens des affaires et de l'entrepreneuriat. Pour parler des décisions qu'il prend, il emploie les termes « risque calculé », « investissement » et « récompense ». Les pertes qu'il a subies par suite de la fermeture de certains de ses groupes ne constituent à ses yeux que des risques professionnels.

Tendances futures

La concurrence s'intensifie, selon Burim. Pas moins de 200 à 300 personnes exercent des activités similaires au Kosovo, en Macédoine et en Albanie. Même s'il se voit comme l'un des précurseurs de

l'industrie, Burim peine de plus en plus à obtenir les clics prisés que ses compétiteurs, dont le nombre ne cesse de croître, et lui se disputent désormais.

Comme c'est le cas dans tant d'autres domaines, une multitude de petits acteurs agiles ont récemment fait leur apparition : de jeunes entreprises spécialisées dans les fausses nouvelles. Un petit nombre d'acteurs prennent de l'expansion et d'autres disparaissent. « Je m'attends à ce qu'il y ait une consolidation », a-t-il affirmé. Il sait également que Facebook s'efforce de contenir le flux incessant des pièges à clics et de le forcer à mettre fin à ses activités. Pour lui, ce n'est qu'un autre risque professionnel.

Le repérage et la publication de contenu, des tâches encore principalement manuelles, seront automatisés davantage et plus axés sur les données si les acteurs prennent bel et bien de l'expansion et sont mieux outillés. Les technologies qui ont été mises en œuvre pour des médias journalistiques légitimes (notamment BBC Trending ou Buzzfeed) permettent de repérer rapidement les récits qui sont largement partagés ou susceptibles (selon des mesures comme la « propagation virale ») de l'être ultérieurement. Il est facile de s'imaginer l'usage que feront de ces technologies des commerces comme celui de Burim pour repérer et republier le contenu le plus viral et le plus facile à partager, et ainsi damer le pion à leurs rivaux.

Conclusions et contre-mesures

De bien des façons, Burim représente l'antithèse du journalisme sérieux. Pour lui, le contenu n'est pas pertinent, la provenance importe peu, le récit se recycle et la vérité est tout à fait accessoire. Or il n'est que le produit de courants beaucoup plus généraux qui ont secoué le journalisme grand public ainsi que des commerces comme le sien. Il va sans dire que les personnes âgées de 55 ans et plus regardent principalement les informations télévisées et consultent pour la plupart d'entre elles différentes sources pour comprendre ce qui se passe dans le monde[50]. Toutefois, les gens se tournent maintenant surtout vers Internet, plus que vers tout autre médium, pour s'informer, et une majorité accède aux nouvelles par des moyens

indirects, c'est-à-dire une passerelle, qui va des moteurs de recherche et des agrégateurs aux sites de réseaux sociaux et aux assistants numériques à commande vocale. Ces recherches sont souvent organisées de façon algorithmique, et ces algorithmes tentent de présenter du contenu précis et calculé le plus susceptible de présenter un intérêt pour le lecteur. D'abord et avant tout, la montée de la publicité programmatique signifie que les revenus sont générés par les clics. Tout le contenu rassemblé sous un même flux, classé en fonction de l'intérêt généré et des clics, fait en sorte que les coûts et les risques rattachés au journalisme sérieux tranchent de plus en plus avec les avantages qui s'y rattachent.

> *Les coûts et les risques rattachés au journalisme sérieux tranchent de plus en plus avec les avantages qui s'y rattachent.*

En Occident, les informations de qualité médiocre diffusées en ligne sont assimilées à une atteinte au débat politique et au journalisme sérieux. L'entretien avec Burim a toutefois fait la lumière sur le revers de la désinformation en ligne. En effet, de dire l'interprète en se penchant en avant : « Il a l'accent de la classe ouvrière rurale de Lipjan ». Burim exerce peut-être des activités néfastes, voire dangereuses, pour la vie publique, mais il y voit un ascenseur social, un moyen de se sortir de la pauvreté rurale et la solution la plus prometteuse parmi les quelques-unes qui s'offrent à lui.

Il n'est pas étonnant que des solutions techniques soient envisagées pour faire obstacle à la désinformation en ligne, celle-ci étant perçue comme un problème technique. Or le problème est également d'ordre social et économique. Tant les entreprises de technologie que les gouvernements devraient s'employer à trouver des façons de mettre à profit l'esprit d'initiative et l'intelligence de personnes comme Burim et de mobiliser ces acteurs pour mener des activités à vocation sociale plus utiles à la société.

NOTES DE FIN DE DOCUMENT

1 Solution de rechange à la publicité de marque traditionnelle sur les canaux des médias électroniques, la publicité programmatique cible les clients individuellement au moyen de témoins de connexion, de codes d'identification d'appareils et de logiciels algorithmiques, automatisant la vente d'espaces publicitaires par un système d'enchères en temps réel.

2 J. Voelz, « Transnationalism and Anti-Globalism », *College Literature*, volume 44(4), 2017, p. 521-526.

3 J. Stringer, « Why did anti-globalisation fail and anti-globalism succeed? », *open Democracy*, 2017; sur Internet : https://www.opendemocracy.net/jacob-stringer/why-did-anti-globalisation-fail-and-anti-globalism-succeed.

4 Antifa est un groupe d'action politique d'extrême gauche plus ou moins bien organisé qui prétend être antifasciste. En 2017, il a organisé plusieurs manifestations et contre manifestations pour dénoncer les activités politiques de la droite alternative et a été critiqué en raison de son recours à des méthodes violentes. Comme dans le cas de ses opposants de la droite alternative, certaines de ses activités en ligne ont été liées aux opérations d'information de la Russie.

5 S. Zannettou et coll., « The Web Centipede: Understanding How Web Communities Influence Each Other Through the Lens of Mainstream and Alternative News Sources », 2017; sur Internet : https://arxiv.org/pdf/1705.06947.pdf.

6 K. Starbird, « Examining the Alternative Media Ecosystem Through the Production of Alternative Narratives of Mass Shooting Events on Twitter », *Proceedings of the Eleventh International Conference on Web and Social Media*, 2017, p. 230-239, ISBN : 978-1-57735-788-9.

7 P. Pomerantsev et M. Weiss, « The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money », *The Interpreter*, Institute of Modern Russia, 2014.

8 J. Giesea, « It's time to embrace memetic warfare », *Defence Strategic Communications Journal*, volume 1 (1), Centre d'excellence pour la communication stratégique de l'OTAN, 2015.

9 Cela a mené à un décret d'Andropov daté du 12 avril 1982, dans lequel il ordonne à tous les officiers du renseignement étranger du KGB, peu importe leurs affectations en cours, de prendre des mesures actives pour faire en sorte que Ronald Reagan perde sa campagne de réélection. Voir Christopher M. Andrew, *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB*, New York, Basic Books, 1999, p. 242.

10 William Blake, *Auguries of Innocence*, 1803 (date approximative); sur Internet : https://www.poetryfoundation.org/poems/43650/auguries-of-innocence. Observation attribuable à : « Russian disinformation campaign: What it takes », CNN, octobre 2017.

11 Mark Galeotti, « What Exactly are "Kremlin Ties"? », *Atlantic Monthly*, juillet 2017.

12 Michman, Gable et Gross, *Market Segmentation: A Selected and Annotated Bibliography*, American Marketing Association, Chicago (Illinois), 1977.

13 Marko Mihkelsoni, *Disinformation across ages: Russia's old but effective weapon of influence*, Euromaidan Press, juillet 2017.

14 Pacepa et Rychlak, *Disinformation*, WND Books, 2013, p. 39. Dans cet ouvrage, les auteurs citent la *Grande Encylopédie soviétique,* State Scientific Publishing House, 1952.

15 Fiona Hill et Clifford G. Gaddy, « How the 1980s Explains Vladimir Putin », *Atlantic Monthly*, février 2013.

16 Eerik-Niiles Kross, « America, welcome to the war », *Politico EU*, août 2016.

17 Témoignage de Robert M. Gates, directeur adjoint du Renseignement, CIA, devant le sous comité des Affaires européennes du Comité des affaires étrangères du Sénat des États Unis, 12 septembre 1985.

18 Bien qu'elles soient hypothétiques au sens le plus strict du terme, les opérations décrites ici ressemblent de manière frappante à de réelles opérations d'information du Kremlin que l'auteur a observées directement et sur lesquelles il a fait enquête.

19 Traduit en ligne à partir du site Web https://rusemb.org.uk/press/2029. Le paragraphe 15a énumère les caractéristiques des conflits modernes.

20 Kate Davies, « Revealed: Confessions of a Kremlin troll », *Moscow Times*, 18 avril 2017; sur Internet : https://themoscowtimes.com/articles/revealed-confessions-of-a-kremlin-troll-57754.

21 « Why the "fake rape" story against German NATO forces fell flat in Lithuania », *DW*, 23 février 2017; sur Internet : http://www.dw.com/en/why-the-fake-rape-story-against-german-nato-forces-fell-flat-in-lithuania/a-37694870.

22 Inglehart, R. F. et Norris, P. (2016), *Trump, Brexit, and the Rise of Populism: Economic Have-nots and Cultural Backlash*; document présenté lors de la réunion annuelle de l'American Political Science Association (Association américaine des sciences politiques), à Philadelphie, aux États Unis. Adresse : https://research.hks.harvard.edu/publications/getFile.aspx?Id=1401.

23 Par exemple, #voteleave et #voteout (Voter pour quitter), #voteremain et #votein (Voter pour rester), #leaveeu (Quitter l'UE), #bremain (Rester dans l'UE), #strongerin (Plus fort ensemble), #Brexit, #euref (Référendum sur l'UE).

24 Le referendum du Brexit a eu lieu le 23 juin 2016.

25 Matthieu Aikins, « Whoever Saves a Life », *Matter*, 15 septembre 2014; sur Internet : https://medium.com/matter/whoever-saves-a-life-1aaea20b782#.b60t2sth9.

26 Eliot Higgins, « Fact-Checking Russia's Claim that It Didn't Bomb Another Hospital in Syria », *Bellingcat*, 9 novembre 2016; sur Internet : https://www.bellingcat.com/news/mena/2016/11/09/fact-checking-russias-claim-didnt-bomb-another-hospital-syria/.

27 « Amnesty International Report on "Civilian Deaths" Based on Fakes, Clichés », *Sputnik News*, 23 décembre 2015; sur Internet : https://sputniknews.com/middleeast/201512231032213565-amnesty-intl-report-fake/.

28 Vidéo publiée sur YouTube par RT, 18 juin 2016; sur Internet : https://www.youtube.com/watch?v=dNbIRD8Cq48&feature=youtu.be&t=44; Ruslan Leviev, « Sputnik, RT and Russian MoD Expose Cluster Bombs at Hmeymim Airbase », *Conflict Intelligence Team*, 7 juin 2016; sur Internet : https://citeam.org/sputnik-rt-and-russian-mod-expose-cluster-bombs-at-hmeimim-airbase.

29 Lizzie Dearden, « Russia-Backed Broadcaster RT Cuts Footage Proving Use of Incendiary "Cluster Bombs" in Syria », *The Independent*, 21 juin 2016; sur Internet : http://www.independent.co.uk/news/world/middle-east/russia-today-syria-war-cluster-bomb-footage-censorship-video-vladimir-putin-a7093141.html.

30 *Motasem homs*, vidéo publiée sur YouTube, 1er octobre 2016; sur Internet : https://www.youtube.com/watch?list=PL3vE7Lp4BcaFpsYlpO92RwSoIj83BnFIq&v=MZY7UvrnxUw.

31 Article publié sur la page Facebook de la Défense civile syrienne à Homs, 2 octobre 2016; sur Internet : https://www.facebook.com/SCD.HOMS/posts/603882693122910.

32 « New Evidence of Russian Incendiary Bombs Use in Syria », *Conflict Intelligence Team*; sur Internet : https://citeam.org/new-evidence-of-russian-incendiary-bomb-use-in-syria/.

33 Pour un examen de l'aspect juridique de cette question, voir par exemple la dépêche suivante sur l'utilisation de bombes incendiaires en Syrie : « Syria/Russia: Incendiary Weapons Burn in Aleppo, Idlib », *Human Rights Watch*, 16 août 2016; sur Internet : https://www.hrw.org/news/2016/08/16/syria/russia-incendiary-weapons-burn-aleppo-idlib.

34 David Bandurski, « China, Rhetorical Giant on the Move », *China Media Project*, 22 juin 2017; sur Internet : http://chinamediaproject.org/2017/06/24/china-rhetorical-giant-move/.

35 Ministère des Affaires étrangères de la République populaire de Chine, 16 décembre 2015, sur Internet : http://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml.

36 Henry Farrell, « The Chinese government fakes nearly 450 million social media comments a year. This is why », *The Washington Post*, 19 mai 2016; sur Internet : https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/?utm_term=.9d718382c7fd.

37 « China's chance to lead global innovation may lie with 5G mobile technology development », *South China Morning Post*, 1er octobre 2017; sur Internet : http://www.scmp.com/tech/enterprises/article/2113581/chinas-chance-lead-global-innovation-may-lie-5g-mobile-technology.

38 David Barboza, « Alibaba Buying South China Morning Post, Aiming to InfluenceMedia », *The New York Post*, 11 décembre 2015; sur Internet : https://www.nytimes.com/2015/12/12/business/dealbook/alibaba-scmp-south-china-morning-post.html.

39 Elizabeth Redden, « New Scrutiny for Confucius Institute », *Inside Higher ED*, 26 avril 2017; sur Internet : https://www.insidehighered.com/news/2017/04/26/report-confucius-institutes-finds-no-smoking-guns-enough-concerns-recommend-closure; https://www.nas.org/projects/confucius_institutes; http://www.pewresearch.org/fact-tank/2016/03/30/6-facts-about-how-americans-and-chinese-see-each-other/.

40 *Rappler* fait partie de cette coalition internationale de recherche dirigée par Camille François.

41 Carly Nyst, « Patriotic trolling: How governments endorse hate campaigns against critics », *The Guardian*, 12 juillet 2017.

42 Une définition et une discussion de la spirale du silence se trouvent à l'adresse suivante : https://masscommtheory.com/theory-overviews/spiral-of-silence/.

43 Julie Posetti, « Online Harassment: Lessons from the Philippines », *Global Investigative Journalism Network*, 13 juillet 2017; sur Internet : https://gijn.org/2017/07/13/fighting-online-harassment-lessons-from-the-philippines/.

44 Jen Weedon, William Nuland et Alex Stamos, « Information Operations and Facebook », 27 avril 2017; sur Internet : https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

45 Conversation avec Facebook, 13 juin 2017.

46 Kristine Daguno-Bersamina, « Duterte uses SONA time to lash out at media », *Philippine Star*, 24 juillet 2017; sur Internet : http://www.philstar.com/headlines/2017/07/24/1721155/duterte-uses-sona-time-lash-out-media.

47 Shan Wang, « Facebook rules the Internet in the Philippines. Rappler walks the line between partnership and criticism », *Nieman Journalism Lab*, 19 juillet 2017; sur Internet : http://www.niemanlab.org/2017/07/facebook-rules-the-internet-in-the-philippines-rappler-walks-the-line-between-partnership-and-criticism/.

48 Tony Romm, « Governments in 30 countries manipulated media online to silence critics, sow unrest or influence elections », *Recode*, 14 novembre 2017; sur Internet https://www.rappler.com/technology/news/188536-philippines-freedom-house-freedom-of-net-2017.

49 Simonyan, Margarita, « Russian media from within », *Russia Today*, 18 octobre 2011; sur Internet : https://daily.afisha.ru/archive/gorod/archive/ministry-of-truth-simonyan/.

50 Reuters Institute Digital News Report 2017; accessible à l'adresse suivante : https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf.

ANNEXE A

ORDRE DU JOUR

QUI DIT QUOI?

DÉFIS SÉCURITAIRES DÉCOULANT DE LA DÉSINFORMATION AUJOURD'HUI

Atelier non classifié du programme de liaison-recherche
du Service canadien du renseignement de sécurité (SCRS)

20 novembre 2017, Ottawa

PROGRAMME

8 h 30 – 8 h 45	Mot de bienvenue, mise en contexte et objectifs de l'atelier
8 h 45 – 9 h 30	**Mise en contexte** – *Russie, Occident et la géopolitique de la désinformation : à quoi s'attendre?*
9 h 30 – 11 h	**Module 1** – *Le mouvement de désinformation d'aujourd'hui et les acteurs non étatiques à son origine*
11 h – 11 h 15	Pause
11 h 15 – 12 h 15	**Module 2** – *La Chine et les Philippines : leçons retenues et points à considérer dans l'avenir*
12 h 15 – 13 h 15	Repas du midi
13 h 15 – 14 h 45	**Module 3** – *Rôle de la Russie dans le mouvement de désinformation : pratique actuelle et perspectives d'avenir*
14 h 45 – 15 h	Pause
15 h – 16 h	**Module 4** – *La voie à suivre : comment limiter, contrer ou prévenir les effets de la désinformation*
16 h – 16 h 15	**Synthèse** – *Les répercussions continues sur la sécurité nationale de la désinformation*
16 h 15 – 16 h 30	Mot de la fin
16 h 30	Fin de l'atelier

ANNEXE B

LA LIAISON-RECHERCHE AU SCRS

Le renseignement dans un monde en évolution

On dit souvent que le monde évolue de plus en plus rapidement. Analystes, commentateurs, chercheurs et autres – associés ou non à un gouvernement – acceptent peut-être ce cliché, mais la plupart commencent seulement à comprendre les conséquences très réelles de ce concept pourtant abstrait.

La sécurité mondiale, qui englobe les diverses menaces pour la stabilité et la prospérité géopolitiques, régionales et nationales, a profondément changé depuis la chute du communisme. Cet événement a marqué la fin d'un monde bipolaire organisé selon les ambitions des États-Unis et de l'ancienne URSS et les tensions militaires en résultant. Détruisant rapidement la théorie de « fin de l'histoire » des années 1990, les attentats terroristes contre les États-Unis en 2001, ainsi que des actes terroristes subséquents dans d'autres pays, ont depuis modifié ce qu'on entend par sécurité.

La mondialisation, l'évolution rapide de la technologie et la sophistication des moyens d'information et de communication ont eu une incidence sur la nature et le travail des gouvernements, y compris des services de renseignements. En plus des conflits habituels entre États, il existe désormais un large éventail de problèmes de sécurité transnationale découlant de facteurs non étatiques, et parfois même non humains. Ces problèmes vont du terrorisme, des réseaux illégaux et des pandémies à la sécurité énergétique, à la concurrence internationale pour les ressources et à la dégradation mondiale de l'environnement. Les éléments de la sécurité mondiale et nationale sont donc de plus en plus complexes et interdépendants.

Notre travail

C'est pour mieux comprendre ces enjeux actuels et à venir que le SCRS a lancé, en septembre 2008, son programme de liaison-recherche. En faisant régulièrement appel aux connaissances d'experts au moyen d'une démarche multidisciplinaire, axée sur la collaboration, le Service favorise une compréhension contextuelle des questions de sécurité pour le bénéfice de ses propres experts ainsi que celui des chercheurs et des spécialistes avec qui il s'associe. Ses activités visent à établir

une vision à long terme des différentes tendances et des divers problèmes, à mettre en cause ses hypothèses et ses préjugés culturels, ainsi qu'à affiner ses moyens de recherche et d'analyse.

Pour ce faire, nous :

- nous associons activement à des réseaux d'experts de différents secteurs, dont l'administration publique, les groupes de réflexion, les instituts de recherche, les universités, les entreprises privées et les organisations non gouvernementales (ONG), tant au Canada qu'à l'étranger. Si ces réseaux n'existent pas déjà, nous pouvons les créer en collaboration avec différentes organisations;

- stimulons l'étude de la sécurité et du renseignement au Canada, favorisant ainsi une discussion publique éclairée à propos de l'histoire, de la fonction et de l'avenir du renseignement au Canada.

Dans cette optique, le programme de liaison-recherche du Service emprunte de nombreuses avenues. Il soutient, élabore, planifie et anime plusieurs activités, dont des conférences, des séminaires, des études, des exposés et des tables rondes. Il participe aussi activement à l'organisation du Global Futures Forum, un appareil multinational du renseignement et de la sécurité qu'il soutient depuis 2005.

Nous n'adoptons jamais de position officielle sur quelque question, mais les résultats de plusieurs de nos activités sont publiés sur le site Web du SCRS au www.csis-scrs.gc.ca. Par la publication des idées émergeant de nos activités, nous souhaitons alimenter le débat et favoriser l'échange d'opinions et de perspectives entre le Service, d'autres organisations et divers penseurs.