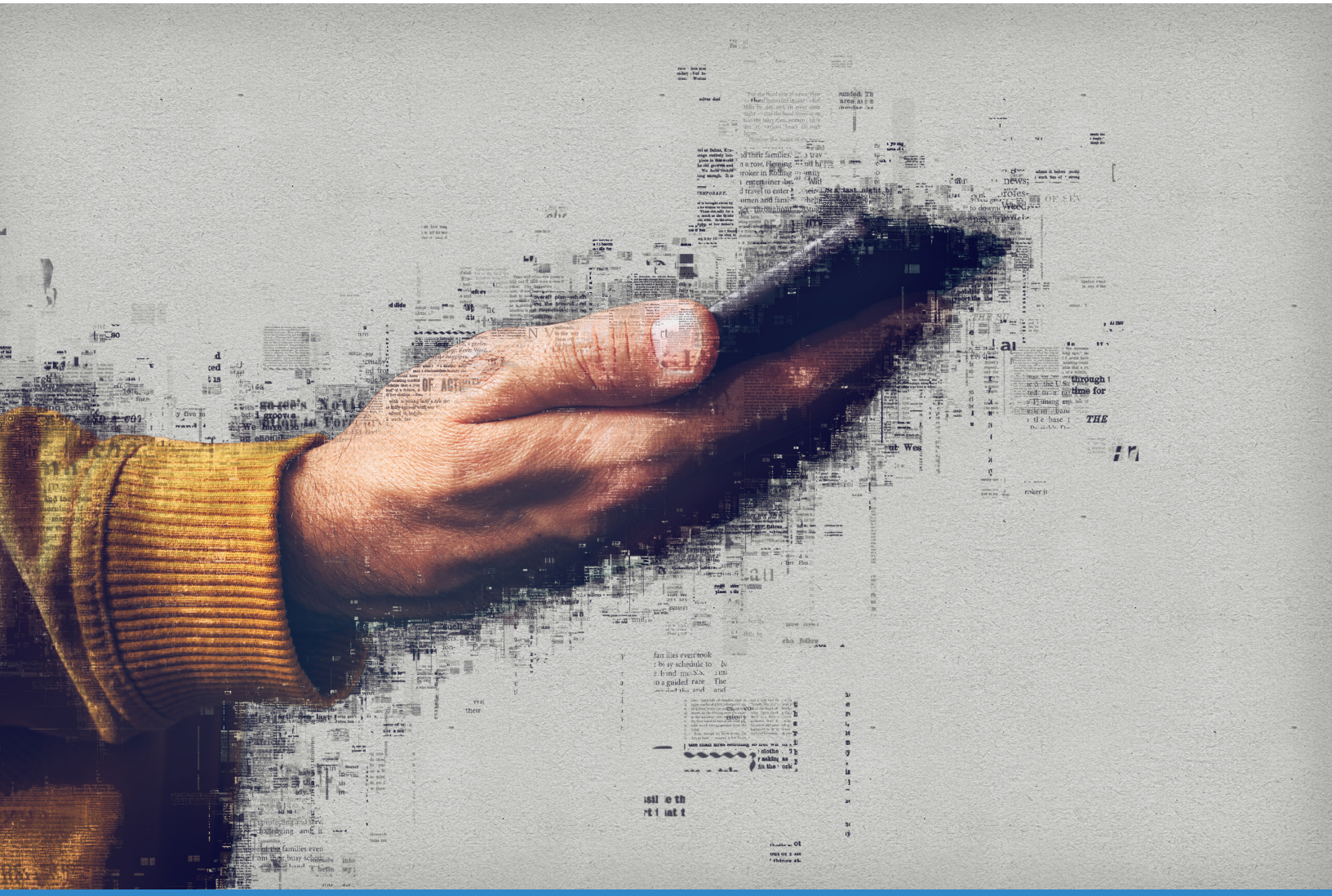

DEZINFORMATSIYA :

L'axe dangereux de la désinformation, de la tromperie et de la perturbation russes et chinoises

DAVE MCMAHON, GNS | NOVEMBRE 2023
Contributeur au Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa

uOttawa
Laboratoire sur l'intégrité de l'information
Information Integrity Lab

SOMMAIRE

La Russie et la Chine misent sur la mésinformation, la désinformation et la malinformation (MDM) pour tromper et manipuler afin d'atteindre leurs objectifs politiques, économiques et militaires. Les écosystèmes de désinformation exploités par la Russie et la Chine utilisent des tactiques dissimulées et évoluées. Le Kremlin mise sur une approche décentralisée non coordonnée, diffusant des approximations afin de créer des tempêtes de désinformation sur les réseaux sociaux pour amplifier son message. Les messages d'influence russes sont un tissu de fabrications, de complots et des demi-vérités. La Chine, de son côté, utilise un partenariat cohérent entre l'industrie, le gouvernement et l'armée pour atteindre ses objectifs. Cela représente un vaste écosystème de désinformation composé de couches imbriquées de services de renseignement, d'entreprises de façade, d'instituts de recherche appartenant à l'État par procuration, d'unités militaires, d'universités, d'installations de recherche, d'entrepreneurs militaires privés, d'organisations criminelles transnationales et de médias contrôlés par l'État.

Il faudrait pouvoir contrer la complexité et la sophistication des menaces étrangères posées par la MDM par la résilience et par des contre-mesures actives dans le cadre d'une stratégie nationale de protection des infrastructures cognitives et de maintien de la paix fondé sur les renseignements qui fait appel à tous les intervenants. À l'heure actuelle, ces réseaux de désinformation ne peuvent être révélés, attribués et ciblés que grâce au renseignement de sources ouvertes (OSINT). Par conséquent, en complément des mesures prises par les entités gouvernementales, le secteur privé peut continuer à jouer un rôle central dans la lutte contre la désinformation, l'influence et l'ingérence étrangères.

INTRODUCTION

À l'ère de la concurrence stratégique, la guerre contre la vérité par la désinformation posera les plus grands défis de notre vie. Or, la défense de la vérité exige une connaissance approfondie des capacités de l'adversaire, du savoir-faire et de l'intention. Ces renseignements sur les adversaires seront principalement obtenus grâce à des renseignements de source ouverte. L'un des plus grands défis sera l'attribution – qui se trouve derrière une campagne de désinformation et pourquoi. L'attribution est souvent intentionnellement confondue par ceux qui l'ont créée, tant par des moyens techniques que par la tromperie et des erreurs d'orientation, faisant en sorte que la désinformation semble être un discours légitime protégé comme la liberté d'expression. L'attribution est essentielle à la formulation d'une réponse par le gouvernement canadien, le secteur privé et la société civile.

La désinformation est un genre de désinformation diffusée de manière délibérée pour tromper les gens, tandis que la malinformation est de l'information qui est vraie et souvent privée ou confidentielle et qui est divulguée intentionnellement pour causer un préjudice réel. Ces tactiques sont devenues si courantes qu'elles ont maintenant leurs propres noms familiers comme « divulgation malveillante de données personnelles » et « alerte malveillante ».

Le problème de la désinformation n'est pas nouveau. Il s'est manifesté sous de nombreuses formes depuis aussi longtemps que les gens cherchent à se tromper les uns les autres. Elle a longtemps été utilisée par les États comme arme dans la guerre militaire, politique et économique. Un livre blanc publié en 1993 sur la guerre de l'information par le ministère de la Défense nationale du Canada a présenté le concept de « maintien de la paix fondé sur les renseignements » – une approche probablement typiquement canadienne à cet égard.[1]

Le livre blanc de 1993 expliquait que le défi du maintien de la paix fondé sur les renseignements consiste à utiliser la puissance du cyberespace, et à tirer parti de la grille d'information mondiale et de son contenu, pour agir efficacement dans les nouveaux réseaux sociaux et espaces politiques afin de protéger les systèmes de vérité. Si les opérations cyberphysiologiques peuvent influencer la composante humaine et si la guerre de l'information vise à détruire les systèmes de connaissance, de vérité et de croyance, alors

l'objectif premier du maintien de la paix fondé sur les renseignements serait de nous aider à comprendre les processus cognitifs qui valident ce que sont, en fin de compte, des connaissances dignes de foi et de concevoir des contre-mesures à la radicalisation, à l'influence étrangère et à l'ingérence dans le processus démocratique. La théorie de l'information parle du média et du message. Les moyens techniques sont tout aussi importants dans la guerre cognitive. La cybersécurité est le champ de bataille moderne des idées, de l'influence et de la tromperie.

Trois décennies plus tard, une étude de 2020 commanditée par l'OTAN sur la guerre cognitive a qualifié la désinformation de « l'armement des sciences du cerveau », qui peut pirater le « biogiciel » humain en exploitant les vulnérabilités humaines et ensuite construire socialement un comportement.

L'influence et ingérence étrangère, la désinformation, la tromperie et la perturbation sont des outils enchevêtrés de l'appareil gouvernemental moderne, qui sont amplifiés par la cybersécurité.

GÉRER LES MENACES

La Russie et la Chine maintiennent de vastes écosystèmes de désinformation et mènent des opérations sophistiquées à grande échelle contre des publics cibles nationaux et mondiaux. Les gouvernements de ces deux pays exercent un contrôle sur les médias nationaux et ciblent les membres des diasporas au moyen de programmes et de plateformes en langue maternelle. La désinformation est largement répandue dans les diasporas chinoises au moyen de médias sociaux comme WeChat. Le Kremlin utilise VKontakte (VK), un service russe de médias sociaux et de réseaux sociaux basé à Saint-Pétersbourg, pour diffuser ses messages. De même, Telegram, lancé en 2013 par les fondateurs de VK, est une autre plateforme populaire exploitée par la machine de propagande étatique russe.

Le cantonais, le taishanais et le mandarin sont les principales langues non officielles parlées au Canada. Plus de 1,7 million (4,6 %) de Canadiens parlent un dialecte chinois. Le Département hyperactif du front uni du travail de Beijing, consacre d'énormes ressources à cultiver des liens étroits avec les éléments super-riches du bloc mandarin, tout en brimant et en intimidant les réformistes de la diaspora, les réfugiés ouïghours, les Hongkongais favorables à la démocratie, les adeptes du Falun Gong et les défenseurs de l'autonomie taïwanaise.[2]

Les diasporas pourraient ne pas avoir accès aux médias traditionnels en raison d'une barrière linguistique. La dépendance aux médias sociaux comme WeChat ou VK crée une « chambre d'écho » qui est encore amplifiée par les algorithmes de plateforme. Les groupes ont tendance à endosser une croyance de leur communauté pour rechercher la reconnaissance sociale dans des groupes qu'ils connaissent. Par conséquent, les communautés de la diaspora sont piégées dans le cercle vicieux des modèles de consommation renforcés. De même, le discours des médias sociaux dans des langues autres que l'anglais ou le français demeure généralement opaque pour le public canadien, les médias grand public et le gouvernement qui ne peuvent en prendre connaissance; par conséquent, la désinformation sur ces plateformes, en particulier l'ingérence étrangère menée par la désinformation, est insidieuse et pratiquement invisible.

Le ciblage des communautés autochtones anglophones du Canada par des adversaires est un peu plus nuancé. Ici, l'influence étrangère est souvent dirigée vers des groupes marginaux. La Russie cible les groupes de gauche et de droite au Canada, ainsi que ceux qui sont enclins à croire aux conspirations. Pour sa part, la Chine mise plutôt sur la culture conscientisée et le racisme. Comme l'a fait remarquer le National Post, « l'affirmation voulant que les inquiétudes concernant l'ingérence électorale sont une démonstration de "racisme" fait partie d'une tactique de propagande bien connue de la Chine ».[3]

La Russie et la Chine utilisent la désinformation comme arme pour perturber et nuire à l'économie canadienne et au cadre sociopolitique démocratique. Leur objectif est d'habiliter les nœuds de désinformation nationaux (auxquels participent de vrais Canadiens) et d'alimenter l'opposition par division au Canada. Les deux puissances utilisent également des agents d'espionnage, d'influence et d'interférence traditionnels, y compris une interférence technique délibérément cyberfacilitée contre les infrastructures essentielles et l'exploitation des chaînes d'approvisionnement. Les attaques de Nortel, d'ASN.1 et de Solar Winds en sont des exemples.

Dans les pages suivantes, nous comparerons plus en détail la façon dont la Russie et la Chine utilisent la désinformation.

RUSSIE

Le terme russe dezinformatsiya est dérivé du titre d'un département de « propagande noire » du KGB. La « propagande noire » est définie comme une forme de propagande faussement accréditée, associée à des opérations psychologiques secrètes. La principale caractéristique de la propagande noire (secrète) est que l'auditoire n'est pas conscient qu'il est influencé. La propagande grise n'identifie pas sa source, tandis que la propagande blanche (rhétorique ouverte) tend à être, du moins superficiellement, du matériel promotionnel sournois.

L'utilisation russe de **dezinformatsiya** a commencé par un « bureau spécial de désinformation » formé en 1923 pour propager de fausses informations afin de tromper intentionnellement l'opinion publique au sein de l'URSS. La « confrontation de l'information » est le terme utilisé dans les cercles stratégiques et militaires russes pour décrire leur approche de l'utilisation de l'information en temps de paix et en temps de conflit, tandis que le terme « mesures actives » est utilisé pour décrire les méthodes de guerre politique russes de longue date.

Au départ, la propagande russe a été conçue pour faire appel à l'idéologie socialiste; en effet, certains ont trouvé les principes du communisme attrayants. Mais le récit communiste s'est depuis effrité avec la chute du mur de Berlin. Aujourd'hui, la Russie est vue dans de nombreuses parties de l'Occident comme le grand antagoniste. Le Kremlin et ses mandataires induisent en erreur et influencent l'opinion publique d'une manière qui profite au gouvernement russe en propageant délibérément des informations fausses ou trompeuses par divers canaux, notamment les médias sociaux, les médias d'information et d'autres formes de communication, y compris la radio, la télévision et la production cinématographique.

La désinformation russe utilise souvent une combinaison de demi-vérités, d'un double discours,[4] de projections psychologiques, de théories du complot et de mensonges audacieux pour semer la confusion et la discorde et miner la confiance du public envers les institutions démocratiques. Le récit russe peut être incongru ou bizarre, destiné à semer la confusion et le chaos.

Parfois, la propagande anti-occidentale ou la désinformation sont utilisées pour soutenir les objectifs de la politique étrangère russe, comme la promotion d'un sentiment prorusse, la promotion des intérêts géopolitiques de la Russie (« l'urgence de dénazifier l'Ukraine » en est un exemple) ou la déstabilisation de gouvernements et de partis politiques rivaux dans des États fragiles comme ceux de l'Afrique. En bref, la Russie cherche à créer des opportunités par le chaos.

La Russie est opportuniste dans les campagnes de désinformation

Parmi les exemples de campagnes de désinformation russes, mentionnons la promotion de théories du complot bizarres et la propagation de faussetés sur la pandémie de COVID-19 et la sécurité de la 5G ou l'utilisation de faux comptes de médias sociaux pour influencer les élections. Ces campagnes impliquent souvent l'utilisation de robots, de trolls et d'autres systèmes automatisés pour amplifier leur message à la fois dans les canaux traditionnels et dans les mouvements conspirationnistes locaux comme QAnon, pour les rendre plus crédibles.

Fait intéressant, la Chine a tenté de promouvoir l'adoption de la technologie 5G chinoise dans le cadre de l'initiative Belt and Road (la ceinture et la route), alors que les efforts de la Russie vont dans la direction opposée. En effet, certains Canadiens, qui ont cru dans la désinformation russe au sujet de la 5G, ont incendié des tours cellulaires.

Le Global Engagement Centre du département d'État américain explique que l'écosystème russe de désinformation et de propagande vise à rallier des fonctionnaires, à s'introduire dans des canaux et des plateformes de communication de substitution ou de sources mal attribués pour créer et amplifier de faux récits.[5] L'écosystème se compose de cinq piliers principaux : les communications officielles du gouvernement, les messages mondiaux financés par l'État, la culture de sources d'information substitutive, l'utilisation malveillante des médias sociaux et la cyberdésinformation. Le Kremlin a la responsabilité directe d'encourager ces tactiques et ces plateformes dans le cadre de son approche d'utilisation de l'information comme arme.

Le département d'État américain soutient en outre que la Russie investit massivement dans ses canaux de propagande, ses services de renseignement et ses mandataires pour mener des cyberactivités malveillantes afin de soutenir leurs efforts de désinformation. Elle tire également parti des médias qui se font passer pour des sites d'information ou des institutions de recherche pour diffuser ces récits trompeurs.

Il n'y a pas qu'une seule plateforme médiatique pour la propagande et la désinformation, et il n'y a pas d'uniformité des messages entre les différentes sources. Les messages individuels dans le système peuvent sembler contradictoires. L'approche écosystémique convient à cette dynamique parce qu'elle ne nécessite pas d'harmonisation entre les différents piliers.[6] Cette situation crée une ambiguïté stratégique au sein de l'écosystème de l'information.

La volonté de la Russie d'utiliser une approche décentralisée non coordonnée de la désinformation offre au Kremlin trois avantages perçus. Tout d'abord, elle facilite l'introduction de nombreuses variations d'un récit faux. Cela permet aux piliers de l'écosystème d'adapter les récits pour cibler de nouveaux publics. Deuxièmement, les mandataires peuvent propager des messages dangereux tandis que les seigneurs du Kremlin restent anonymes. Troisièmement, elle crée un effet d'amplification médiatique entre les différents canaux pour augmenter leur portée et leur résonance. Cet effet multiplicateur médiatique peut parfois créer des tempêtes de désinformation ou des infodémies.

Le Kremlin externalise une grande partie de sa guerre cognitive, et une grande partie de cette externalisation va à une seule entité : le groupe Wagner.

GROUPE WAGNER ET DÉSINFORMATION

Au nord-ouest de Saint-Pétersbourg se dresse le gratte-ciel le plus septentrional du monde : le Centre Lakhta. Les médias locaux l'appellent « la tour de Sauron » – qui regarde constamment vers l'ouest, source sombre d'influence maligne, de désinformation et de mensonges. Il s'agit de l'ancien siège de la Russian Internet Research Agency (agence de propagande russe sur Internet, officiellement dissoute en juillet 2023, mais dont les opérations se poursuivent sur un autre front), une usine à trolls parrainée par l'État anciennement détenue par le lieutenant oligarque de Vladimir Poutine, Yevgeny Prigozhin, qui dirigeait également le groupe Wagner.

Le groupe Wagner est une société paramilitaire russe privée et une organisation criminelle transnationale sanctionnée[7] liée à des campagnes de désinformation visant à promouvoir les intérêts russes. En fait, il existe des preuves d'un ancien canal de communication secret[8] entre Yevgeny Prigozhin et le Bureau de l'administration présidentielle de la Fédération de Russie. Parmi les exemples des campagnes de désinformation menées par le groupe Wagner, mentionnons la diffusion de fausses informations sur le conflit en Syrie et la création de faux comptes de médias sociaux pour influencer les élections dans d'autres pays. Les campagnes de désinformation du groupe Wagner sont considérées comme une menace pour les sociétés démocratiques, car elles peuvent miner la confiance du public à l'égard des institutions et créer des divisions entre les citoyens. Le groupe a des liens

étroits avec le gouvernement russe et a été inculpé dans un éventail d'activités, y compris des violations des droits de l'homme, des crimes de guerre, de l'ingérence électorale, de la propagande et d'autres formes de désinformation.

Un autre acteur clé était l'Internet Research Agency (IRA), qui a été fondée et financée par Wagner. Elle était connue sous divers pseudonymes : Internet Research LLC, RIA, RIAN et RIAFAN. L'IRA et son successeur, l'Agence fédérale de presse (FAN), faisaient partie du « projet Lakhta » russe. La seule entité qui est actuellement encore en activité officielle est l'Agence fédérale de presse (FAN) qui fonctionne avec un nouvel ensemble de domaines de façade conçus pour masquer l'origine du contenu malveillant. L'IRA a été liquidée par ordre présidentiel de Vladimir Poutine en 2014, lorsque la Russie a envahi la Crimée, pour créer « Agence Rossiya Segodnya » (Agence Russie Aujourd'hui) qui a absorbé tous les employés de l'IRA. L'agence nouvellement créée a également absorbé FAN le jour de l'invasion de la Crimée, créant « RIA FAN », le nouvel ajout étant officiellement inscrit sous le nom d'organisme Rossiya Segodnya le 8 avril 2014.

Ces usines à trolls gérées par l'État de l'ancienne IRA ont contribué[9] à fomenter des discussions polarisées en ligne, à saper les démocraties libérales, à interférer dans les élections, à attiser le mouvement anti-vaccin et le déni des changements climatiques, à diffuser des messages fracturés et à attaquer violemment les organisations antidopage. En d'autres termes, ils propagent de la mésinformation et de la désinformation, pour éroder, perturber et dégrader la confiance dans le système démocratique, saboter la croissance industrielle du Canada et saper les valeurs fondamentales et la qualité de vie canadiennes.

Les récits d'influence russe ont combiné de pures fabrications, des complots et des demi-vérités pour amplifier leurs messages.[10] La désinformation menée par la Russie est adaptée pour capter les publics canadiens avec des récits qui les interpellent. Alors que nous, en Occident, considérons la cybersécurité comme un assemblage technique de « uns » et de « zéros », nos adversaires considèrent la cybersécurité comme un élément de base : un domaine de connaissance et d'influence. La doctrine Gerasimov russe[11] (guerre hybride) combine des tactiques militaires, technologiques, diplomatiques, économiques, culturelles, d'information, et autres dans le but d'atteindre des objectifs stratégiques, par le vol de propriété intellectuelle, la désinformation et la tromperie.

CHINE

La Chine s'efforce de devenir une superpuissance mondiale des médias et de la désinformation grâce à un arsenal de tactiques, y compris les médias d'État, les campagnes de désinformation et les infrastructures numériques. Le gouvernement chinois utilise une approche pansociétale pour recueillir des renseignements et propager la désinformation. Cela la distingue de tout ce qui est entrepris par les gouvernements occidentaux.[12]

La Chine s'engage dans la tromperie systémique et stratégique, la désinformation, l'influence et l'ingérence à travers sa collaboration industrielle dans l'Initiative Belt and Road, la stratégie des Trois guerres, le programme « 1000 talents » et des activités de front unifié (nous en reparlerons plus loin).

Beijing travaille également à influencer l'opinion publique dans le cadre d'accords de partenariat des médias d'État à l'étranger. Les journalistes des médias d'État chinois ont été chargés d'exploiter l'ambiguïté de leurs marques personnelles pour pousser la propagande d'État. En outre, le fait d'inonder les plateformes de médias sociaux comme Twitter de « quantités massives de pourriels [rend] plus difficile pour les journalistes et les observateurs indépendants d'accéder à l'information sur ce qui se passe », explique Kurlantzick, un chercheur principal pour l'Asie du Sud-Est au Council on Foreign Relations.

La Chine recrute des millions de ses citoyens pour agir comme « guerriers du clavier » pour influencer l'opinion publique en ligne et manipuler la vérité à grande échelle, comme les usines à trolls en Russie. Ces recrues sont connues sous le nom d'« armée des 50 centimes » parce qu'elles sont payées 0,5 yuan par publication.

Récemment, Beijing a adopté des tactiques secrètes et malveillantes à la russe et une diplomatie en ligne agressive dite du « loup guerrier »[13] et attaque directement les médias occidentaux. À titre d'exemple, les médias d'État chinois détournent le blâme des origines de la COVID-19 en répandant la rumeur selon laquelle le virus était une arme biologique américaine. La diplomatie Twitter

ou Twiplomacy chinoise a énormément varié dans le contenu et les formes d'engagement, suggérant un manque d'approche de coordination de la part du corps diplomatique chinois.

Beijing s'améliore dans la désinformation sur les médias sociaux mondiaux. Son influence secrète, son ingérence et la désinformation gagnent du terrain en polarisant les débats publics en Occident, tout comme les tactiques russes. Les réseaux chinois résistent aux efforts de déconfinement et gagnent du terrain auprès des véritables utilisateurs. Pourtant, ils se font prendre à exécuter de faux comptes et campagnes sur les médias sociaux. Par exemple, l'enquête Spamouflage Dragon, une campagne sur les réseaux sociaux ciblant les manifestations à Hong Kong, a supprimé 23 000 comptes Twitter liés à la Chine impliqués dans une gamme d'« activités manipulatrices et coordonnées ».[14]

Ironiquement, la désinformation en ligne entrave les grandes initiatives chinoises en matière de suprématie des données et d'intelligence artificielle, qui reposent sur la véracité des mégadonnées. En d'autres termes, les propres fonds de données de la Chine sont compromis par de fausses données que la Chine elle-même diffuse sous forme de désinformation.

MANDATAIRES

Dans de nombreux pays étrangers, l'industrie nationale et le crime organisé font partie intégrante de l'appareil militaire et de renseignement de leur pays.[15] La Russie, la Chine et l'Iran utilisent leur industrie pour obtenir des capacités à un rythme opérationnel beaucoup plus rapide que le Canada et pour mener des campagnes de désinformation au nom de l'État.

L'écosystème russe de la guerre de l'information est à la fois vaste et complexe. Comme les poupées russes, les Matryoshka, elle se compose de couches imbriquées d'entités commerciales, d'instituts de recherche appartenant à l'État, d'unités militaires, d'universités et d'installations de recherche de l'ère soviétique associées à l'appareil de sécurité de l'État, développant des capacités de renseignement électromagnétique et de cryptographie. Compliquant les choses, l'État russe encourage et emploie activement des pirates informatiques criminels.

De même, les usines à trolls pour les opérations de désinformation et d'influence fonctionnent indépendamment des acteurs décentralisés et des campagnes participatives. Les services de renseignement russes comme le Service fédéral de sécurité, le Service du renseignement étranger et la Direction principale du renseignement sont tous des acteurs actifs dans cet espace, avec l'Agence de recherche sur Internet (IRA) et le Groupe Wagner. Souvent, ces organisations collaborent, mais se livrent aussi concurrence, les unes contre les autres et contre l'industrie. Il ne semble pas y avoir d'autorité centrale.

Un bon exemple de ce qui précède est un reportage récent du journal The Guardian,[16] qui confirme la recherche indépendante de Sapper Lab concluant que la société privée de guerre de l'information NTC Vulkan reçoit des directives opérationnelles des services de renseignement russes pour des opérations offensives de cyberattaques et de désinformation. Le GRU 74455 (Renseignement militaire) a été inscrit comme « partie d'approbation » pour les activités portant sur les documents secrets de l'entreprise. Celle-ci a été impliquée dans des pannes d'électricité en Ukraine, a perturbé les Jeux olympiques en Corée du Sud, a lancé l'exploit informatique Notpetya[17] et créé le programme Sandworm pour contrôler Internet et propager de la désinformation. L'armée russe a engagé cet entrepreneur privé pour construire des outils similaires pour la propagande nationale automatisée. Le sous-système ulkan NTC Amezit a permis à l'armée russe de mener des opérations secrètes de désinformation à grande échelle dans les médias sociaux et sur Internet en créant des comptes qui ressemblent à de vraies personnes en ligne, ou avatars. Ces avatars ont des noms et des photos personnelles volées, qui sont ensuite élaborées sur des mois pour produire une empreinte numérique réaliste. [18] Sandworm soutenu par le GRU a également été un acteur influent en tant que groupe de pirates informatiques.

John Hultquist, vice-président de l'analyse des renseignements à la firme de cybersécurité Mandiant, a déclaré que les preuves suggèrent que « la Russie voit les attaques contre les infrastructures civiles essentielles et la manipulation des médias sociaux comme une seule et même mission ».

La Chine utilise également des mandataires de l'industrie. L'industrie chinoise, le gouvernement central, les services de renseignement et l'armée forment un partenariat cohérent autour d'initiatives nationales conjointes : l'initiative Belt and Road, le

plan 1000 talents, le Front uni du travail, la stratégie de fusion militaro-civile et la stratégie Trois guerres. Il n'y a pas d'analogie en Occident d'une telle intensité de partenariat public-privé intégré à une stratégie nationale unifiée.

L'initiative chinoise Belt and Road[19] vise à modifier l'équilibre entre la puissance économique, technologique et militaire mondiale. Le Plan des 1000 Talents recrute des experts internationaux de premier plan en recherche scientifique, innovation et entrepreneuriat. Le Front uni du travail[20] recueille des renseignements sur des personnes et des organisations à l'intérieur et à l'extérieur de la Chine, y compris au Canada, et gère les relations avec elles et tente d'influencer ou d'intimider[21] des personnes et des organisations à l'intérieur et à l'extérieur de la Chine, y compris au Canada, en misant sur l'industrie, le gouvernement, l'armée, les services de renseignement et le crime organisé. La stratégie de fusion militaro-civile de la Chine[22] fait en sorte que les entreprises deviennent des bienfaiteurs directs du renseignement. La stratégie des trois guerres de la Chine[23] est un calcul de guerre précinétique politique et d'information de l'Armée populaire de libération (APL) englobant la guerre des médias ou de l'opinion publique, la guerre psychologique et la guerre juridique. Huawei est un chef de file de l'initiative Belt and Road.
Depuis quelques décennies, il y a eu nombre d'incidents publiés sur l'ingérence étrangère de la Chine. Parmi les activités alléguées d'ingérence rapportées dans les médias et dans des rapports universitaires publiés, mentionnons l'utilisation de la désinformation stratégique, la coercition économique, les enlèvements politiques, des tentatives de façonner et de diviser l'opinion publique en misant sur les médias sociaux et d'autres moyens, ainsi que le ciblage de citoyens et d'institutions canadiens à des fins d'espionnage. Dans un essai paru en janvier 2019 dans The Hill Times, l'ambassadeur de la Chine au Canada, Lu Shaye, affirmait que la colère canadienne à propos de l'enlèvement de Michael Kovrig et Michael Spavor par Beijing était « due à l'égotisme occidental et à la suprématie blanche ».

Les récentes campagnes de désinformation chinoises dans notre pays ont porté sur le traitement des citoyens canadiens d'origine chinoise, sur des allégations de racisme systémique contre le Canada et sur le ternissement de la réputation du Canada dans le commerce international. La récente campagne de « camouflage de pourriel » lancée contre des personnalités clés dans les sphères politique et médiatique du Canada est un phénomène plus dirigé visant l'influence politique.

DIVERGENCE ET CONVERGENCE

Il convient de noter qu'historiquement, les objectifs, les tactiques et les stratégies de désinformation russes et chinoises ont différé de plusieurs façons. Les campagnes de désinformation russes ont tendance à être davantage axées sur la mise à mal des institutions démocratiques et sur la création d'animosité et de chaos. Les campagnes de désinformation russes sont également plus agressives et provocatrices, avec l'utilisation généralisée de robots, de trolls et de systèmes automatisés pour amplifier leur message. Parfois, personne ne gagne à la désinformation russe.

Les campagnes de désinformation chinoises, en revanche, ont tendance à se concentrer davantage sur la promotion de l'image et des intérêts de la Chine sur la scène mondiale. Elles font souvent appel à des médias contrôlés par l'État pour promouvoir les réalisations de la Chine et minimiser ses faiblesses, ainsi qu'à la diffusion de la propagande approuvée. Les campagnes de désinformation chinoises ont également tendance à être plus ingénieuses et sophistiquées, avec l'utilisation d'informations et de récits sélectifs pour façonner l'opinion publique de manière plus subtile et nuancée. Elles sont souvent liées à une influence secrète, à de l'ingérence et à de l'espionnage. À l'inverse, la désinformation russe n'est pas bien coordonnée en matière d'influence, d'ingérence délibérée ou de cyberespionnage. Bien que les réponses chinoises récentes à l'ingérence étrangère aient montré beaucoup moins de maturité, il y a eu un virage vers des tactiques secrètes et malveillantes à la russe et des tactiques agressives de type « loup guerrier ».

Une autre différence clé entre la désinformation russe et chinoise est leur approche face à la censure. Alors que les deux pays censurent fortement l'information et contrôlent leurs médias, l'approche de la Chine tend à être plus centralisée et systématique, avec un accent sur le contrôle du flux d'information à l'intérieur du pays. La Chine a un meilleur contrôle technique de son environnement informationnel. L'approche de la Russie est plus décentralisée et ponctuelle, avec l'utilisation d'une gamme de tactiques pour contrôler l'information et réprimer la dissidence.

Bien que les intérêts russes et chinois divergent de manière importante, ils collaborent de plus en plus sur les récits qui sont fournis aux publics nationaux, diffusant de la désinformation et de la propagande similaires. James Rubin, coordinateur pour le Global Engagement Center et envoyé spécial des É.-U., affirme que la Chine dépense des milliards pour la désinformation pro-Russie.[24] Une grande partie de ce processus ne semble pas être planifiée ou coordonnée. Nous constatons que les opérations d'information chinoises sont en soutien direct aux récits et aux objectifs russes.

CANADA LA CIBLE PERMISSIVE

BLa Russie et la Chine exercent une influence et une ingérence actives dans les affaires canadiennes depuis des décennies.[25] [26]

Il a été confirmé que des agents russes ont diffusé de fausses informations sur les plateformes de médias sociaux lors des élections fédérales canadiennes de 2019 pour miner le processus. La désinformation aurait visé à la fois les groupes de droite et de gauche, dans l'intention d'exacerber les tensions existantes et de perturber le processus démocratique.

De plus, un rapport de Global News en 2020 affirmait qu'un réseau de sites Web liés à la Russie avait diffusé des renseignements trompeurs sur la COVID-19 au Canada.[27] Le rapport alléguait que les sites Internet diffusaient des théories du complot et de la désinformation sur les origines et la propagation du virus, en plus de promouvoir des traitements et des remèdes non éprouvés. Selon un rapport du Conseil des académies canadiennes, la désinformation liée à la COVID-19 a contribué à plus de 2800 décès canadiens et a coûté 300 millions de dollars.[28] C'est quatre fois plus que le nombre de Canadiens morts dans les guerres depuis la Seconde Guerre mondiale. Bref, la désinformation peut tuer.

Comme il est mentionné dans The Conversation, « les Canadiens sont exposés à la propagande pro-Kremlin. Un peu plus de la moitié des Canadiens (51 %) ont signalé qu'ils se sont retrouvés face à au moins une affirmation fausse et persistante au sujet de la guerre entre la Russie et l'Ukraine dans les médias sociaux, poussée par les comptes du Kremlin et des pro-Kremlin.[29] L'affirmation la plus répandue, mentionnée par 35 % des Canadiens, était que le nationalisme ukrainien est un mouvement néonazi. »

Selon The National Observer,[30] [traduction] « les manifestants locaux qui ont participé au soi-disant convoi de la liberté du Canada l'an dernier ont été aidés par les organes de propagande financés par l'État russe pour exploiter leurs griefs, amplifier les divisions sociales et délégitimer le gouvernement Trudeau ». Ironiquement, le gouvernement chinois aurait tenté en même temps de faire élire les libéraux.

Les sites intermédiaires jouent un rôle important dans la diffusion de la désinformation. Le département d'État américain a identifié la plateforme montréalaise Global Research comme étant un puissant site intermédiaire mandataire du Kremlin amplifiant la propagande et la désinformation russes. CBC a précisé que Global Research « propose un recueil toujours croissant de théories du complot, comme le mythe selon lequel les attentats du 11 septembre et la pandémie de COVID-19 étaient tous deux prévus pour contrôler la population.[31] Le site héberge également des articles attribués par des experts à une agence d'espionnage russe. »

Le Service canadien du renseignement de sécurité (SCRS) et le Centre de la sécurité des télécommunications (CSTC) ont tous deux rendu publiques leurs préoccupations sur la façon dont les campagnes de désinformation parrainées par l'État russe faussent les efforts du Canada pour aider l'Ukraine à se défendre. La désinformation russe est considérée comme une menace sérieuse pour les sociétés démocratiques, car elle peut miner la confiance du public à l'égard des institutions et créer des divisions entre les citoyens.

EXTRÊME GAUCHE ET DROITE

Dans un rapport conjoint, le Centre for Artificial Intelligence, Data, and Conflict (CAIDAC) a enquêté sur l'armement de l'extrême droite et de l'extrême gauche du Canada par les Russes.[32]

Les recherches ont révélé que les communautés d'extrême droite et d'extrême gauche du Canada sont de plus en plus polarisées et que leur rhétorique est passée des différences au sujet des politiques à la définition des opposants comme des ennemis qui

constituent une menace existentielle pour le pays. Les réseaux d'extrême droite et d'extrême gauche au Canada font partie des communautés politiques les plus actives en ligne. Les réseaux favorables à la Russie ont produit vingt-sept fois plus de contenu et se sont mobilisés pour communiquer avec les députés canadiens trois fois plus que les Canadiens légitimes.[33]

Le chercheur Marcus Kolga, fondateur de Disinfowatch, écrit que le gouvernement russe surveille continuellement les sociétés occidentales en vue d'exploiter les enjeux controversés. Une fois que de tels problèmes sont identifiés, les porte-parole et les intermédiaires russes injectent et amplifient ces récits dans notre environnement d'information pour intensifier les divisions politiques.[34]

L'analyse a révélé que les opérations d'influence russes intégraient des récits sophistiqués avec des images et des vidéos incendiaires adaptées aux publics canadiens et aux Canadiens moyens qui amplifient involontairement les opérations d'influence russes. La nature réactive de la campagne sur les tendances, ainsi que l'ampleur et le volume des récits produits, suggère un effort bien financé par le gouvernement russe et ses mandataires. Les comptes prorusses ont intensifié les opérations d'influence au Canada trois mois avant l'invasion [de l'Ukraine] et ont bâti un écosystème de soutien.[35]

ÉTUDES DE CAS

LES OLYMPIQUES

La Russie a lancé une lutte sans merci contre l'Agence mondiale antidopage (AMA), basée à Montréal, après les Jeux olympiques de Sotchi en 2014. Ces efforts impliquaient la désinformation, l'influence, l'intimidation, la coercition, la calomnie et les cyberattaques. En 2018, les États-Unis ont inculpé des agents russes du GRU de piratage international et d'opérations connexes d'influence et de désinformation.[36] Parmi les conspirateurs figurait une équipe de piratage « à accès rapproché » des services de renseignement russes qui a voyagé à l'étranger pour compromettre les réseaux informatiques utilisés par les responsables antidopage et sportifs.

L'AGRICULTURE

La Chine continue de menacer le secteur agricole canadien et la salubrité des aliments par des pratiques d'espionnage, d'ingérence délibérée, d'influence, de désinformation et de piratage parrainé par l'État.[37] En 2019, la Chine affirmait faussement avoir trouvé de la ractopamine dans un lot de produits porcins exportés du Canada. L'Agence canadienne d'inspection des aliments (ACIA) et la GRC ont enquêté sur cette affirmation[38] et ont conclu que les allégations étaient sans fondement; pis encore, les certifications d'exportation avaient été contrefaites. Dans le même ordre d'idées, la Chine a répandu de la désinformation selon laquelle ses inspecteurs ont trouvé des ravageurs dans des échantillons de canola canadien[39]; or, c'est un fait bien connu qu'il s'agit de la principale culture commerciale pour de nombreux agriculteurs des Prairies. La Chine importe pour 2,8 milliards de dollars de canola canadien par année, ce qui représente environ 40 % des exportations canadiennes de cette culture. Lorsque la désinformation ne tue pas, elle peut avoir de graves dommages financiers.

Contre-mesures

Le gouvernement du Canada a pris des mesures pour répondre aux préoccupations concernant l'ingérence étrangère, notamment en créant un groupe de travail spécialisé et en adoptant une loi pour renforcer la sécurité électorale et la prévention de l'ingérence étrangère. Il reste à voir si des agents secrets russes et chinois signeront bientôt le registre visant la transparence en matière d'influence étrangère[40].

Il est reconnu que certaines des initiatives les plus évoluées pour lutter activement contre la désinformation, l'influence et l'ingérence étrangères sont menées par le secteur privé, soit des membres de l'industrie, des universitaires et des participants à la recherche sur la sécurité, des journalistes d'enquête et des représentants de la société civile.

Des contre-mesures sont appliquées à quatre points stratégiques : le public, le message, l'infrastructure et les acteurs malveillants.

Public cible

Building resiliency within the target audience starts with security awareness education, critical thinking and promoting access to authoritative sources of information. Fact-checking, media literacy programs and increased transparency in social media advertising can help the audience make informed decisions.

Message

Nous pouvons lutter contre les messages toxiques grâce à des filtres antipourriel basés sur le contenu et soutenus par l'intelligence artificielle (IA), discréditer et prévenir les publications et suspendre les comptes d'influenceurs malveillants. Le contre discours est très efficace, mais il doit toujours être fondé sur la vérité dans le cadre d'une stratégie de maintien de la paix fondé sur les renseignements ou d'une opération mondiale de paix et de stabilisation.

Infrastructure

Les campagnes de désinformation s'appuient sur le cyberespace pour propager et amplifier leur message au moyen de réseaux de sémantiques. Le cyberespace offre également un moyen efficace de se cacher à travers des réseaux de brouillage et qui masquent l'attribution. Le dénombrement des éléments d'infrastructure mondiale de désinformation étrangère nécessite des renseignements de source ouverte et des ressources de ciblage efficaces. Au bout du compte, le démantèlement d'infrastructures malveillantes s'est avéré une stratégie plus efficace que la poursuite de milliards de messages toxiques consommés par un public cible.

Acteurs malveillants

L'auteur de la menace se situe au sommet de la chaîne alimentaire. Qu'il s'agisse d'un service de renseignement ennemi (HIS), d'une organisation paramilitaire, d'une usine à trolls ou d'une personne d'influence, pour pouvoir cibler l'auteur de la menace il faut une attribution solide étayée de renseignements sophistiqués. Cela en vaut la peine, les conséquences sont variées : sanctionner des entreprises et des particuliers, geler des actifs, démanteler des réseaux financiers, perturber le commandement et le contrôle, maintenir un engagement persistant ou donner suite à des mises en accusation et à des poursuites. Depuis quand même un bon moment, l'industrie perturbe et démantèle activement les réseaux ennemis, exposant les acteurs et poursuivant avec efficacité.

Conclusion

La Russie et la Chine exploitent de vastes écosystèmes de désinformation complexes et évolués qui sont principalement externalisés à des mandataires de l'industrie. Les deux acteurs des États-nations et leurs mandataires échangent des tactiques, des techniques et des procédures de désinformation tout en menant simultanément des campagnes contraires, ce qui indique que le système est quelque peu décentralisé, voire chaotique, et donc difficilement ciblé.

La désinformation est souvent révélée grâce au renseignement de sources ouvertes (OSINT) et contrecarrée par des effets ouverts. Par conséquent, en complément des mesures prises par les entités gouvernementales, le secteur privé peut continuer à jouer un rôle central dans la lutte contre la désinformation, l'influence et l'ingérence étrangères. Les principaux points seront les suivants :

- renforcer la résilience du public par la sensibilisation, l'éducation et la pensée critique;
- créer et diffuser un contre-discours fondé sur la vérité pour discréditer et prévenir la désinformation, la mésinformation et la malinformation;
- dénombrer et éliminer les infrastructures malveillantes;
- cibler, exposer, sanctionner et poursuivre les acteurs malveillants.

Des acteurs étatiques comme la Russie et la Chine utiliseront des moyens de plus en plus sophistiqués pour propager la désinformation dans des démocraties comme le Canada et à leur sujet. La lutte contre cette désinformation et l'ingérence étrangère qui touchent les Canadiens est un sport d'équipe qui exige la collaboration et la coordination entre le gouvernement et le secteur privé.

References

1 Le Cadre conceptuel de la guerre de l'information des Forces canadiennes, élaboré par le Capc Robert Garigue, Ph.D., en 1994 en tant que commandant adjoint du Groupe des opérations d'information des Forces canadiennes (GOIFC), avait prévu la guerre sémantique et la cyberdéception. Les concepts demeurent valables aujourd'hui. M. Garigue est ensuite devenu chef de la sécurité de Bell Canada et l'un des visionnaires hautement reconnus en cybersécurité de l'époque.

2 National Post. 7 avril - Beijing apologists have conjured a racist bogeyman. It's total nonsense, Terry Glavin, publié le 31 mars 2023, https://nationalpost.com/opinion/beijing-apologists-have-conjured-a-racist-bogeyman-its-total-nonsense

3 National Post. 7 avril - Beijing apologists have conjured a racist bogeyman. It's total nonsense, Terry Glavin, publié le 31 mars 2023, https://nationalpost.com/opinion/beijing-apologists-have-conjured-a-racist-bogeyman-its-total-nonsense

4 Le double discours est un langage qui obscurcit, déguise, déforme ou inverse le sens des mots. On parle ici d'ambiguïté intentionnelle dans le langage ou d'inversions du sens.

5 Centre mondial d'engagement du Département d'État des États-Unis, piliers de l'écosystème russe de la propagande de désinformation https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/

6 Ibid. Département d'État des États-Unis

7 Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization https://home.treasury.gov/news/press-releases/jy1220

8 Les 99 appels du chef mercenaire russe à Poutine ont révélé : que les liens du chef de Wagner Yevgeny Prigozhin avec le Kremlin sont confirmés par une série d'enregistrements téléphoniques et de courriels, Daily Mail, 14 août 2020 https://www.dailymail.co.uk/news/article-8627033/Russian-mercenary-leaders-99-calls-Poutine-revealed.html

9 L'IRA mise en accusation par le département de la Justice des États-Unis https://www.justice.gov/file/1035477/download

10 Adam B. Ellick et Adam Westbrook, « Operation Infektion: Russian Disinformation from the Cold War to Kanye », New York Times, 12 novembre 2018.

11 RUS Chef de l'état-major général des forces armées russes

12 La Chine mène depuis des décennies une guerre d'espionnage totale, le 28 mars 2023 www.foreignpolicy.com

13 La diplomatie du loup guerrier est un style de diplomatie coercitive adopté par les diplomates chinois pendant l'administration de Xi Jinping, reconnue pour être conflictuelle et combative. Le terme provient du film d'action chinois Wolf Warrior 2.

14 https://www.axios.com/2019/09/25/spamouflage-dragon-china-hongkong-social-media-campaign

15 Adversary innovation and procurement at operational tempo, Sapper Labs 11 avril 2023 https://www.sapperlabs.com/post/adversary-innovation-and-procurement-at-operational-tempo

16 La fuite des fichiers Vulkan révèle les tactiques de cyberguerre mondiale et nationale de Poutine https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics 30 mars 2023

17 Des variantes de Petya ont été détectées pour la première fois en mars 2016, elles étaient propagées au moyen de pièces jointes infectées par courriel. En juin 2017, une nouvelle variante de Petya a été utilisée pour une cyberattaque mondiale visant principalement l'Ukraine. La nouvelle variante se propage via l'exploit EternalBlue, qui croit-on, aurait été développée par la National Security Agency (NSA) des États-Unis, et a été utilisée plus tôt dans l'année par le rançongiciel WannaCry. Kaspersky Lab a appelé cette nouvelle version NotPetya.

18 Ibid Guardian

19 « China's Massive Belt and Road Initiative. » Conseil des relations étrangères, Conseil des relations étrangères, www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative. Consulté le 20 novembre 2023.

20 https://en.wikipedia.org/wiki/United_Front_Work_Department

21 https://www.primetimecrime.com/Articles/RobertRead/sidewinder.pdf

22 https://2017-2021.state.gov/military-civil-fusion/index.html

23 https://warontherocks.com/2018/01/chinas-three-warfares-perspective/

24 https://www.theguardian.com/world/2023/feb/28/china-spends-billions-on-pro-russia-disinformation-us-special-envoy-says

25 https://www.cbc.ca/news/politics/some-politicians-under-foreign-sway-csis-1.909345

26 https://www.thestar.com/politics/federal/2023/03/06/chinese-interference-in-canada-chinese-canadians-say-they-reported-it-for-years-and-were-ignored.html

27 https://globalnews.ca/news/8450263/infodemic-covid-19-disinformation-canada-pandemic/

28 https://www.cbc.ca/news/politics/cost-of-covid-19-misinformation-study-1.6726356

29 https://theconversation.com/russian-propaganda-is-making-inroads-with-right-wing-canadians-186952

30 La Russie a utilisé les moyens de propagande financés par l'État pour mobiliser le soutien au « Convoi de la liberté » et miner le gouvernement Trudeau Par Caroline Orr | Analyse | 10 février 2023, https://www.nationalobserver.com/2023/02/10/analysis/russian-propaganda-freedom-convoy-disinformation

31 Canadian professor's website helps Russia spread disinformation, says U.S. State Department, Oct 2020, https://www.cbc.ca/news/science/russian-disinformation-global-research-website-1.5767208

32 Centre for Artificial Intelligence, Data, and Conflict (CAIDAC), by the University of Maryland College of Information Studies and Digital Public Square March 2023 - Enemy of my enemy – investigated Russian weaponization of Canada's far right and far left to undermine support to Ukraine https://www.tracesofconflict.com/_files/ugd/17ec87_c9aa91bdc83f4f0498b4b0123ed33d5e.pdf

33 Ibid. CAIDAC

34 Marcus Kolga, « Confusion, Destabilization and Chaos: Russia's Hybrid Warfare Against Canada and Its Allies », Institut canadien des affaires mondiales, octobre 2021.

35 Ibid. CAIDAC

36 https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and

37 https://cskacanada.ca/wp-content/uploads/2023/03/CSKA-CyberBarnRaising-FIN-digital.pdf

38 https://globalnews.ca/news/5433257/canada-investigating-china-certificates-pork-ban/

39 https://www.cbc.ca/news/canada/calgary/china-canola-pests-bibeau-calgary-chamber-1.5053283

40 https://www.canada.ca/fr/services/defense/securitenationale/consultation-registre-influence-etrangere.html

AUTEURS

Dave McMahon

Dave McMahon est chef du renseignement de Sapper Labs Group et ancien coprésident du comité interministériel sur la guerre de l'information et les opérations psychologiques. Cet article a été commandé et publié par le Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa.