Guerre cognitive : conquérir les cœurs et les esprits

DANIEL NIKOULA, DAVE MCMAHON | Juillet 2024

uOttawa

Laboratoire sur l'intégrité de l'information

Information Integrity Lab

« Dans la guerre cognitive, l'arme c'est vous ! »

— Zack Rogers, PhD

SOMMAIRE

Le présent article explore le terrain complexe de la guerre cognitive qui englobe des tactiques comme la manipulation de l'information, les cyberattaques et le façonnement du discours pour influencer l'opinion publique et miner la confiance. Avec la montée des technologies numériques, des adversaires comme la Russie et la Chine ont cherché à exploiter les médias sociaux et les plateformes en ligne pour pratiquer la désinformation et semer la discorde. L'escalade de la guerre cognitive a exercé des pressions sur le Canada et ses alliés afin qu'ils comprennent mieux la menace et élaborent des contre-mesures, notamment le renforcement des moyens de cyberdéfense, la promotion de la médiatique et l'accroissement de la résilience face à la manipulation de l'information. Il est essentiel de comprendre la dynamique entre l'information et la perception afin de se protéger contre les menaces évolutives émanant de la guerre cognitive. La collaboration entre les gouvernements, les entreprises de technologie et la société civile est indispensable à la lutte contre les stratégies cognitives antagonistes — principalement la désinformation — et à la protection des institutions démocratiques.

Daniel Nikoula est analyste au Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa.
Dave McMahon est associé au Laboratoire sur l'intégrité de l'information de l'Université d'Ottawa.

INTRODUCTION

La guerre cognitive est un concept multidimensionnel englobant les opérations d'information, les cybercapacités et la communication stratégique. Elle est généralement définie comme [traduction] « l'utilisation des moyens d'action que fait un État ou un groupe influent pour manipuler les mécanismes spontanés de la cognition d'un ennemi ou des citoyens afin de les affaiblir, de les infiltrer, de les influencer, voire de les maîtriser ou de les détruire[1] ». Cela comprend l'utilisation de tactiques psychologiques, la manipulation de l'information et les stratégies cognitives (les exposés, la sémiotique, l'iconographie[i]) pour influencer les émotions, les croyances, les perceptions et les comportements des personnes, des groupes ou des populations entières. Essentiellement, la guerre cognitive représente une combinaison de [traduction] « guerre psychologique, sociale et technique » et de « guerre d'influence » par des cybermoyens[2].

Les opérations psychologiques et les tactiques d'influence et de déception existent depuis les débuts des guerres humaines. Le général chinois Sun Tzu, éminent stratège militaire de son époque, a écrit dans L'Art de la guerre que « La guerre, c'est l'art de leurrer ». Il fait remarquer qu'un grand chef militaire n'est pas nécessairement celui qui remporte de nombreuses victoires sur le champ de bataille, mais bien celui qui atteint ses objectifs sans recourir à la violence comme première mesure. Les moyens de remporter une victoire sans effusion de sang — la subversion, la furtivité et le subterfuge — ont évolué au fil du temps et ont principalement été utilisés dans des conflits asymétriques où des forces plus faibles s'opposaient aux forces classiques plus fortes.

Aujourd'hui, les populations mondiales sont assaillies de quantités massives d'informations, dont une grande partie est fausse ou trompeuse. Bien que l'utilisation d'informations fausses ou déformées pour gagner un avantage sur son adversaire ne date pas d'hier, le poids relatif et la présence de telles méthodes ont considérablement augmenté ces dernières années, la guerre de l'information atteignant des niveaux sans précédent[3]. L'essor des médias de masse a rendu l'esprit humain plus sensible aux influences malveillantes tout en érodant la capacité des gens à choisir en connaissance de cause.

Dans la guerre cognitive, l'esprit humain représente le champ de bataille. Celle-ci cible principalement la cognition, qui est [traduction] « le processus mental d'acquisition et de compréhension des connaissances ainsi que l'interprétation et la perception de l'information[4] ». Prenant appui sur la guerre psychologique du passé, qui avait recours à la propagande pour cibler les émotions, la guerre cognitive mobilise la technologie moderne pour [traduction] « exploiter les préjugés ou les automatismes mentaux, [provoquant] des distorsions dans les représentations, l'altération du processus décisionnel ou même l'inhibition de l'action, et entraîner des conséquences désastreuses, tant au niveau individuel que collectif[5] ». Contrairement à la guerre classique (ou cinétique) qui repose sur la violence physique, la destruction et la conquête territoriale, la guerre cognitive opère dans le domaine des idées, des émotions et des perceptions.

Rappelant Sun Tzu, la guerre cognitive vise à exploiter les vulnérabilités de l'esprit humain pour tenter de [traduction] « gagner la guerre avant qu'elle soit déclenchée[6] ». Bien que les capacités classiques — qui permettent de saisir et d'occuper le territoire par une force écrasante — puissent déterminer les résultats tactiques ou opérationnels, la conquête du domaine cognitif (l'esprit humain) est essentielle pour remporter une victoire durable. De récents conflits cinétiques ont souligné l'importance de ce principe.

Rôle de la désinformation dans la guerre cognitive

On a de plus en plus recours à la désinformation, c'est-à-dire de fausses informations vérifiables qui sont créées et diffusées intentionnellement dans le but de confondre, de manipuler ou d'induire en erreur, dans le cadre des stratégies de guerre cognitive, ce qui représente une menace grave pour la sécurité nationale du Canada et de ses alliés[7]. La création et la diffusion de la désinformation sont l'une des méthodes principales de la guerre cognitive, car elle implique la construction de réalités parallèles et la déformation de la vérité à titre de concept référentiel. Cela a pour effet de confondre les gens, les rendant plus susceptibles d'adhérer aux théories de conspiration et de croire des faussetés. L'exploitation des préjugés cognitifs des gens, un objectif majeur de la guerre cognitive, peut les inciter à s'identifier fortement à un groupe de pensée particulier et à susciter chez eux une hostilité envers d'autres personnes, groupes ou institutions qui ne s'alignent pas sur leur vision conformiste du monde. S'il n'est pas réprimé, le cloisonnement cognitif peut conduire à la discorde, à la polarisation et à l'instabilité sociale. Au cours des dernières années, un nombre incalculable d'acteurs étatiques et non étatiques utilisant la désinformation se sont ingérés dans les élections, ont porté atteinte au consensus scientifique et médical, ont fomenté la division sociale et déstabilisé les économies, ce qui a obligé les pays démocratiques à reconnaître que la désinformation posait une menace sérieuse et permanente à la sécurité nationale. Jens Easterly, directeur de la Cybersecurity and Infrastructure Security Agency des États-Unis, a déclaré que [traduction] « l'infrastructure la plus essentielle est notre infrastructure cognitive. Il est donc extrêmement important de renforcer la résilience face à la mésinformation et à la désinformation[8] ». Son assertion repose sur la reconnaissance croissante que la guerre cognitive, dans les milieux de politique publique et les pays membres de l'OTAN, constitue un domaine distinct qui mérite qu'on lui porte une attention assidue.

La désinformation amplifie la fréquence et la couverture médiatique des faussetés. L'objectif est de former un public prêt à gober d'abord un mensonge, puis à le répéter. Les attaques contre le domaine cognitif font usage des capacités cybernétiques, psychologiques, de désinformation et d'ingénierie sociale. La guerre cognitive positionne l'esprit comme un espace de combat et un domaine contesté. Son objectif est d'introduire la dissonance, de susciter des récits contradictoires, de polariser l'opinion et de radicaliser les groupes. La guerre cognitive peut inciter les gens à agir d'une manière qui peut perturber ou fragmenter une société par ailleurs cohésive. Le désordre qui en résulte peut influencer la prise de décisions, modifier les idéologies et susciter la méfiance chez les alliés.

Les opérations de désinformation de prochaine génération peuvent causer de graves dommages cognitifs. Il s'agit notamment de la diffusion rapide d'« hypertrucages » : des vidéos qui cherchent à créer l'illusion d'un individu qui fait ou dit quelque chose au moyen de la technologie de transplantation faciale. Même si la technologie en est à ses débuts, les vidéos peuvent être convaincantes. De plus, d'autres perfectionnements sont apportés aux versions audio seulement de cette technologie de trucage, comme les soi-disant applications d'intelligence artificielle. Les réseaux sociaux comme Facebook et TikTok ont déjà lancé des campagnes pour interdire les contenus truqués[9]. Les préjudices potentiels associés aux contenus truqués soulèvent des préoccupations profondes chez les défenseurs de la vérité. Même si un contenu fallacieux peut être révoqué ou supprimé d'une plateforme en ligne, les corrections et les rectifications parviennent rarement à ceux qui ont consulté le contenu original.

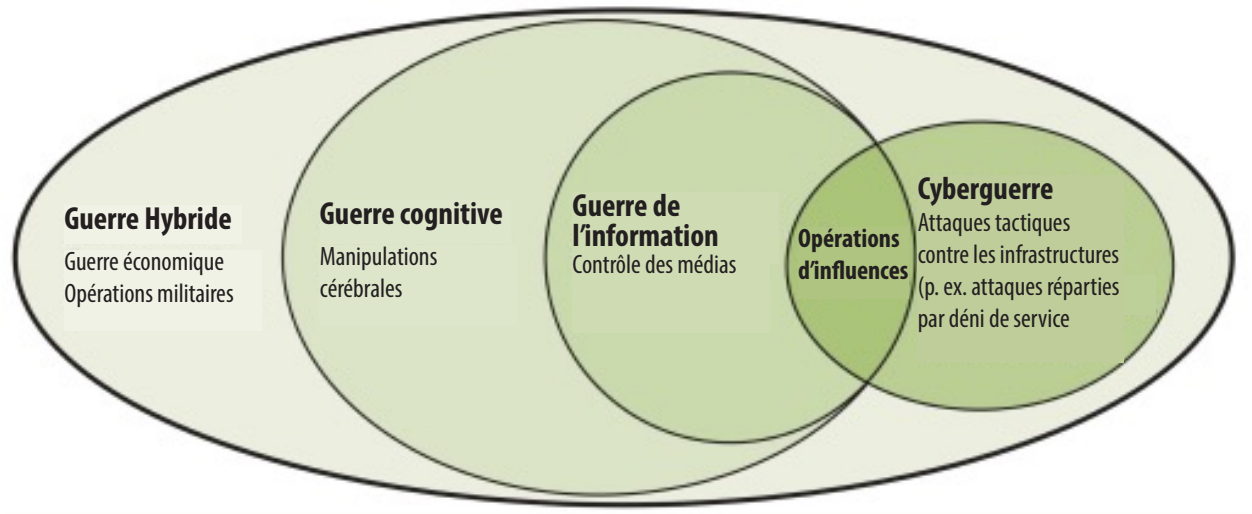

Figure 1. Relations conceptuelles de la guerre cognitive

Défendre le Canada à l'ère de la guerre cognitive

Bien que les groupes d'influence secrets (comme les organisations extrémistes) utilisent les techniques de la guerre cognitive comme moyens de gagner en influence, d'atteindre leurs objectifs stratégiques et de pallier leur puissance militaire classique limitée, les acteurs étatiques continuent de mobiliser les ressources les plus productives pour élaborer et déployer de telles stratégies, en particulier dans les domaines des opérations d'ingérence étrangère et de la guerre hybride. Le Canada et ses alliés sont devenus le centre de l'attention malveillante de deux acteurs étatiques de premier plan : la Russie et la Chine.

L'ours (la Russie)

La Russie a appris à appliquer systématiquement les principes des démocraties libérales contre elles en transformant l'information en arme. Cela fait maintenant partie intégrante du concept de la guerre « non linéaire » du Kremlin, qui englobe de nombreux éléments de la guerre cognitive[10]. Par le passé, la Russie a mené des activités non cinétiques, comme des campagnes ciblées de propagande et de désinformation, pour propager ses discours à l'étranger. Russia Today, la chaîne multilingue russe 24 heures sur 24, est présente dans plus de 100 pays, y compris jusqu'à récemment au Canada. Ses effets sont considérables, car [traduction] « les destinataires de la désinformation alignée sur la Russie subissent une détérioration de leur capacité à distinguer les faits et la fiction, une diminution de leur résilience mentale ainsi des répercussions potentielles à long terme, comme une perte de confiance dans les médias[11] ».

Comme le révèle le récent rapport du Service canadien du renseignement de sécurité, Menaces d'ingérence étrangère visant les processus démocratiques du Canada, le but des activités de la guerre cognitive russe est de déstabiliser la démocratie par la polarisation[12], notamment en exploitant les failles existantes dans la société. Quant à la cote d'écoute de Russia Today, on estime que plus de 100 000 Canadiens regardaient la chaîne chaque jour avant que le Conseil de la radiodiffusion et des télécommunications canadiennes ne révoque, en 2022, l'autorisation de sa diffusion au pays[13] [14]. Au début de 2022, Russia Today a suivi avec attention l'évolution des manifestations dans le cadre du convoi de la liberté en mettant l'accent sur les récits incendiaires — une tactique éprouvée de la guerre de l'information et cognitive, surnommée [traduction] « tout ce qui cause le chaos[15] ». De plus, la recherche de l'ONG canadienne Disinfowatch a révélé que les activités d'information russes dévalorisaient les Canadiens de différentes communautés, tout en exploitant [traduction] « les réactions émotionnelles négatives à des enjeux délicats comme les pensionnats, l'environnement et les questions anti-LGBTQ[16] ». Les propagandistes russes prêtent une attention particulière aux sensibilités locales en cherchant à utiliser, contre le Canada, son soutien du multiculturalisme. La stratégie de la Russie, qui consiste à cerner et à exploiter les points de clivage entre les communautés ou contre le gouvernement, constitue une menace particulièrement grave pour un pays aussi diversifié que le Canada.

Après que l'Occident l'a isolée à l'échelle internationale après son invasion de l'Ukraine, la Russie s'est repliée sur elle-même. Confrontée à des contraintes imposées à son matériel et à sa capacité d'opérer au-delà de son espace géographique, elle a de plus en plus eu recours à des campagnes de désinformation à l'appui d'une stratégie visant à favoriser la désunion de ses adversaires. S'appuyant sur un vaste réseau d'usines à trolls, de zombies et de pirates informatiques, la Russie assaille activement de désinformation les personnes et les communautés pour attiser la division et paralyser l'Occident dans sa détermination à soutenir l'Ukraine.

Le dragon (la Chine)

Alors que la Russie cherche à rétablir son rôle d'important acteur mondial dans un monde multipolaire, la Chine exerce son influence croissante pour tirer un avantage économique et politique et saper la détermination de ses adversaires à résoudre les conflits[17]. La « stratégie des trois guerres » de la Chine est une forme de guerre cognitive qui intègre la guerre sur les plans médiatique, juridique et psychologique. Cette stratégie ne se résume pas à imiter le plan stratégique de la Russie en matière de propagande et de désinformation. Plutôt, la Chine continue de préciser sa propre approche en tirant parti des technologies de pointe et de ses ressources humaines. Par exemple, le ministère du Travail du Front uni, supervisé directement par le Comité central du Parti communiste chinois, cible activement les publics étrangers. La diaspora chinoise au Canada a résisté à des opérations d'influence et à l'intimidation des autorités chinoises et de leurs mandataires. Des organisations comme l'Association des étudiants et universitaires chinois exercent leurs activités au sein des universités canadiennes et s'efforcent de faire progresser leurs objectifs politiques. De plus, la Force de soutien stratégique de l'Armée de libération populaire est chargée d'exécuter des opérations psychologiques et d'influence.

Les médias étatiques chinois représentent le modèle de « cuisine centrale » de la diffusion de contenu dans les médias et les plateformes de médias sociaux. Leur contenu est amplifié par un vaste réseau de partenariats public-privé. Des entreprises comme Spamouflage, Onesight, Nothing Technologies, Urun Big Data Services, Chinaii et d'autres prennent part aux campagnes de censure et de propagande du gouvernement qui visent à propager la propagande et la désinformation à l'étranger au moyen de réseaux de zombies sémantiques[ii]. Le Canadian Centre for International Governance Innovation fait écho à une analyse du secteur privé, qui a souligné que [traduction] « la sécurité nationale du Canada est directement touchée par des éléments des politiques chinoises actuelles, y compris la pratique de l'espionnage, l'utilisation offensive de la cyberpuissance, la volonté d'user de la diplomatie des otages et les efforts d'ingérence dans notre démocratie et notre société[18] ».

Dans un récent rapport d'enquête, Disinfowatch a émis une vigoureuse mise en garde contre les tactiques inquiétantes qu'utilise le gouvernement chinois pour promouvoir ses intérêts au Canada. Selon le rapport, en plus des tactiques comme la diplomatie des otages et l'ingérence dans les processus démocratiques, des efforts concertés sont déployés pour manipuler l'opinion publique par le biais de vastes campagnes de désinformation[19].

La révélation à propos de la campagne de Huawei pour influencer l'opinion publique canadienne est particulièrement préoccupante. Selon le rapport, Huawei Canada a constitué un dossier de personnes, dont des politiciens, des professeurs d'université, des avocats et des dirigeants du milieu des affaires, qu'elle identifie comme des personnalités influentes clés. On croit que ces personnes sont prises pour cible en raison de leur soutien potentiel du programme de Huawei et de leur participation aux campagnes

d'influence visant à insérer la technologie chinoise dans l'infrastructure d'information essentielle du Canada.

Ces activités représentent non seulement une menace importante pour l'intégrité de la démocratie canadienne, mais minent également la confiance du public dans les processus et les institutions démocratiques. L'utilisation de ces tactiques souligne le besoin urgent d'une vigilance accrue et de contre-mesures robustes pour protéger la souveraineté et les intérêts nationaux du Canada contre l'ingérence étrangère.

Près de ses frontières, la Chine a recours à la guerre cognitive comme moyen pour créer des conditions favorables à l'unification de Taïwan. La guerre cognitive chinoise utilise des activités de zone grise dans le but de légitimer, auprès des publics chinois, les contestations de l'ordre international existant et des systèmes axés sur les règles. La Chine fait la promotion de discours sur les soi-disant provocations américaines et l'incitation au conflit dans le détroit de Taïwan, conjointement avec les représentations du gouvernement de Taïwan comme un acteur agressif. Ces tactiques visent à créer des conditions propices à l'unification de Taïwan, potentiellement par des moyens cinétiques. De plus, elles exploitent les vulnérabilités inhérentes aux démocraties libérales, y compris l'absence de consensus sur une définition de la guerre et de seuils clairs relatifs aux comportements inacceptables parmi les pays aux vues similaires comme Taïwan et les membres du G7.

L'alliance (l'OTAN)

En tant que principale alliance militaire mondiale, l'OTAN s'est intéressée à l'étude de la guerre cognitive et a commencé à élaborer des contre-stratégies d'action collective. L'OTAN reconnaît que ses adversaires sont de plus en plus habiles dans leur recours à la guerre hybride et non conventionnelle, qui conjugue des éléments cinétiques, cybernétiques et cognitifs, pour atteindre leurs objectifs. Sur le plan de la désinformation, l'alliance surveille activement les médias traditionnels et les plateformes en ligne pour comprendre le contexte narratif et répondre efficacement aux défis émergents. Le lieutenant-colonel François du Cluzel, gestionnaire du Centre d'innovation de l'OTAN, a lancé l'avertissement suivant : [traduction] « la guerre cognitive [est] utilisée par les adversaires pour miner la confiance et affaiblir, perturber et déstabiliser les populations, les institutions et les États cibles afin d'influencer leurs choix[20] ». Les conflits futurs se produiront probablement entre les peuples connectés numériquement plutôt qu'entre ceux qui sont situés à proximité géographique des pôles de pouvoir politique, militaire et économique.

Dans le contexte des défis militaires, l'OTAN décrit la guerre cognitive comme une « menace invisible » et met en garde contre les [traduction] « tentatives antagonistes de manipuler les membres de l'alliance ». Le rapport de l'OTAN précise que [traduction] « la guerre cognitive a comme but qu'un adversaire détruise sa cible de l'intérieur, de sorte que celle-ci soit incapable de résister, de dissuader ou d'esquiver – ce qui permet à l'agresseur de donner suite à son propre programme » (citation). Les discussions de l'OTAN donnent à

penser que l'objectif principal est de conforter la confiance, tout en reconnaissant que les adversaires utilisent des stratégies de guerre cognitive visant à affaiblir les institutions publiques et à façonner les politiques publiques ou gouvernementales. Ces tactiques facilitent l'accroissement du mécontentement au sein d'une société afin de favoriser des idéologies et des comportements particuliers. Malgré son influence, l'OTAN a beaucoup de travail à faire pour acquérir une supériorité cognitive par rapport à ses adversaires.

L'alliance élabore actuellement un concept spécifique lié à la guerre cognitive, dont la publication est prévue plus tard cette année (2024). Il s'agit notamment de favoriser une compréhension collective et des capacités individuelles et de faire progresser les opérations cognitives au sein de l'alliance de sécurité de 32 États — une tâche qui nécessitera [traduction] « la coopération soutenue entre les alliés afin d'assurer la cohérence générale, de renforcer la crédibilité et de permettre une défense concertée[21] ». De plus, l'Organisation de science et de technologie de l'OTAN a approuvé une variété d'équipes d'examen et de groupes opérationnels de recherche sur le sujet[22].

Selon l'alliance, la supériorité cognitive par rapport aux adversaires repose sur trois principaux piliers : la conscience, la compréhension et l'avantage. Le premier pilier, la conscience, consiste à [traduction] « acquérir, stocker et exploiter l'information, les données et les renseignements par de nombreux moyens[23] ». Elle va au-delà de la prise de conscience des capacités stratégiques des alliés et des adversaires pour évaluer et comprendre l'état cognitif des personnes en temps réel. La compréhension suppose [traduction] « la vision et la stratégie à long terme; la culture stratégique, le comportement et l'art opérationnel; la trajectoire de développement de la conduite de la guerre et l'orientation technologique à long terme; les dispositifs de commandement et de contrôle, etc. » (ibid.). Bref, il s'agit de comprendre les intentions des différents acteurs.

Compte tenu de l'importance des technologies émergentes et des défis et opportunités qu'elles présentent, l'Agence d'information et de communication de l'OTAN a lancé des initiatives stratégiques axées sur l'intelligence artificielle et l'analyse prospective de la cybersécurité. De plus, l'OTAN a créé des groupes de recherche et de technologie pour étudier cet enjeu et comprendre comment la manipulation de l'information influence les populations des alliés[24].

Au pays (le Canada)

Les Forces armées canadiennes (FAC) considèrent la guerre cognitive comme une menace distincte et émergente, reconnaissant que « l'ère numérique [...] dans laquelle nous vivons a redéfini les règles des conflits et a rendu les frontières autrefois défendables vulnérables aux incursions d'une toute autre sorte[25] », reconnaissant qu'« un adversaire peut attaquer sous le seuil du conflit armé en faisant passer le « champ de bataille » d'une guerre conventionnelle à une guerre narrative qui se passe dans les esprits de la population[26] ». La plus récente mise à jour de la politique de défense publiée en avril cette année souligne

que : « La concurrence stratégique entre les États ouvre la voie à des conflits entre grandes puissances. L'intensification des crises environnementales, provoquée ou renforcée par le changement climatique, et les menaces posées par [...] la désinformation [...][27] ». Toutefois, l'approche du Canada relative aux opérations cognitives a longtemps été considérée comme une extension des affaires publiques des FAC au lieu d'une exigence conjointe et intégrée. « Les menaces posées par des activités malveillantes sous le seuil, y compris les cyberattaques, la désinformation et l'ingérence étrangère, exigent de nouvelles approches en matière de défense nationale.[28] »

D'après les renseignements accessibles au public, l'infrastructure cognitive des FAC s'appuie sur 10 « entreprises » exerçant des activités d'influence qui soutiennent 10 groupes-brigades canadiens au sein d'une structure comptant 4 divisions. De plus, il existe une Force opérationnelle des activités d'influence au sein de la 5e Division du Canada (Boudreau). La mise en place du Centre canadien pour la cybersécurité, rattaché au Centre de la sécurité des télécommunications, a marqué une évolution positive sur la voie de la lutte contre les activités préjudiciables de la guerre cognitive. Puisque de nombreux mauvais acteurs utilisent les cybercapacités pour influencer les décisions politiques, le Centre vise à protéger les systèmes et les actifs d'information du Canada. En 2021, le Centre a coorganisé le Défi de l'innovation de l'OTAN, intitulé « La menace invisible : Contrer la guerre cognitive ». De plus, le programme Innovation pour la défense, l'excellence et la sécurité du ministère de la Défense nationale du Canada a été mis sur pied en 2023. Il vise à rassembler les innovateurs et à trouver des solutions aux défis technologiques de l'avenir, dont ceux qui peuvent affecter les perceptions sur le champ de bataille et au-delà[29].

Enfin, le gouvernement a annoncé un investissement de 5,5 millions de dollars dans le cadre de l'Initiative de citoyenneté numérique de Patrimoine canadien pour créer le Réseau canadien de recherche sur les médias numériques. Le Réseau « renforcera encore davantage la résilience de la population canadienne en matière d'information en menant des recherches sur la manière dont la qualité de l'information, y compris les récits de désinformation, se répercute sur les attitudes et les comportements des gens et en appuyant des stratégies qui améliorent la littératie numérique des Canadiens[30] ». Voilà les étapes nécessaires pour commencer à contrer les activités liées à la guerre cognitive au pays, tout en jetant les bases sur lesquelles bâtir au cours des prochaines années.

L'avenir de la guerre cognitive

Les nouvelles technologies de pointe accélèrent les stratégies traditionnelles en matière de guerre cognitive sur les plans de la rapidité, de la portée et de l'envergure. Toute activité d'influence nécessite une compréhension approfondie du public cible. Les réseaux sociaux, l'intelligence artificielle et les mégadonnées représentent un terrain vital pour la guerre cognitive. Plus précisément, les mauvais acteurs tirent parti du comportement numérique des populations en recueillant de grandes quantités de données personnelles sur les réseaux personnels, leurs préférences et leurs vulnérabilités. Les programmes modernes

d'intelligence artificielle ont facilité les processus de collecte et d'analyse des données à une échelle sans précédent. De plus, les adversaires se livrent à des cyberattaques contre les systèmes d'information afin d'obtenir des renseignements étatiques sensibles. Ces attaques servent un autre objectif, à savoir mieux comprendre les connaissances et les capacités de l'État cible tout en minant la confiance dans les services publics qu'il offre et sa capacité à se protéger et à protéger ses citoyens.

L'influence cognitive facilitée par l'information exploite également les réseaux sociaux et la psychologie humaine. Plusieurs théories sociocognitives expliquent comment cette information se propage et influence les utilisateurs des médias sociaux. Parmi celles-ci, mentionnons la théorie des utilisations et de la gratification, la théorie du capital social et la théorie cognitive sociale. En d'autres mots, le bouche-à-oreille électronique — appuyé par les algorithmes — peut joindre rapidement un grand nombre de personnes[31] [32]. Les médias sociaux facilitent les interactions et les réponses instantanées, offrant une plateforme accessible aux personnes qui cherchent à gagner en influence. En raison d'une telle mobilisation et de l'aspiration à assurer leur pertinence et leur visibilité, les médias sociaux incitent les utilisateurs à partager du contenu, souvent sans évaluer sa crédibilité.

Les acteurs de la guerre cognitive ont maintenant commencé à utiliser les médias synthétiques créés par l'intelligence artificielle, y compris ceux générés dans des contextes liés à la guerre en Ukraine et à Gaza. Ceux-ci peuvent prendre la forme de fichiers visuels ou audio falsifiés qui représentent faussement les dirigeants militaires et étatiques semant le chaos parmi les populations. Sur le plan cognitif, la tromperie visuelle a beaucoup plus d'impact en raison du concept appelé le « réalisme heuristique ». Les expériences menées par Doris Graber, professeure à l'Université d'Ottawa, dans les années 1990, ont démontré comment les éléments visuels influencent la formation des souvenirs et leur remémoration — effectivement, « voir, c'est se souvenir ». Les personnes ont tendance à se rappeler plus facilement les images visuelles, même si elles ne se souviennent pas de leur source. Cela souligne un autre risque cognitif posé par la technologie. Même s'ils sont rapidement réfutés, les hypertrucages peuvent encore se propager rapidement sur les médias sociaux et, à long terme, [traduction] « contribuer à un état d'indétermination généralisée[33] ». Le matériel peut susciter de fortes émotions négatives dans le but d'encourager des actions précises, de recueillir de grandes quantités de données biométriques pour calibrer les attaques cognitives et de créer de faux souvenirs (ibid.).

Des campagnes de guerre cognitive plus efficaces sont issues de l'optimisation des interactions personne-machine. L'intelligence artificielle peut facilement combler les lacunes en recourant à l'information accessible au public, renforçant ainsi sa capacité à comprendre le comportement humain et à adapter les réponses.

Enfin, les méthodes de la guerre cognitive de l'ère nouvelle intègrent la neuroscience et la psychologie pour en améliorer l'efficacité. Ces techniques pourraient comporter de profondes répercussions sur la prise de

décisions, la confiance et la performance en fournissant aux acteurs de la guerre cognitive un avantage pour neutraliser leurs adversaires. De telles tactiques tombent sous le seuil de la guerre classique sans activité cinétique. De plus, les méthodes liées aux neurosciences dépassent le champ d'application du droit international en vigueur, ce qui complique les efforts pour en réglementer l'utilisation.

Observations et recommandations

Il est évident que dans la guerre moderne, le rôle du pouvoir de convaincre et de l'influence, surtout dans le domaine cognitif, prend de plus en plus d'importance. Les progrès technologiques continus exigent une meilleure compréhension des méthodes, des techniques et des effets de la guerre cognitive. La lutte contre les opérations de guerre cognitive sera un aspect fondamental des stratégies de sécurité et de défense nationales du Canada et de ses alliés. La prolifération de la guerre cognitive souligne la nécessité pour le Canada et ses partenaires de l'OTAN d'adopter une posture de défense assurée qui intègre de nouvelles contre-stratégies et mesures de sécurité. De telles mesures sont particulièrement nécessaires compte tenu des nombreux préjudices causés par la guerre cognitive à la société, à l'industrie et aux personnes visées par les attaques cognitives qui contournent les défenses militaires traditionnelles.

Un défi persistant réside dans l'établissement de liens entre les domaines cognitif (sémantique), cybernétique et physique d'une manière cohérente qui procure une défense en profondeur et réduit les menaces. Il est difficile de trouver un compromis cognitif, car ce type de compromis émane du subconscient. Les acteurs malveillants prennent des précautions extraordinaires pour dissimuler leurs activités, leur identité et leurs méthodes, conduisant souvent la guerre cognitive à l'aide de techniques telles que les pseudonymes en arrière-plan, les réseaux non attribuables (non traçables), les réseaux à double flux rapide, la désinformation populaire et les réseaux de zombies sémantiques. La doctrine, les plans et les normes classiques en matière de sécurité ne traitent pas des tactiques utilisées dans la guerre cognitive. Les attaques cognitives peuvent également [traduction] « contourner les couches d'air » dans tous les réseaux sécurisés. Cela signifie que les mesures de sécurité classiques comme les jardins fermés et les pare-feux deviennent inefficaces. En ce sens, la guerre cognitive n'a pas de frontières géographiques ni de limites temporelles.

Les approches classiques en matière de guerre cognitive perçoivent cette situation comme un problème social unique, alors qu'en fait, la solution nécessite une expertise et des capacités dans de nombreux domaines. Comme le signale le rapport Reimagining a Canadian National Security Strategy : [traduction] « En fin de compte, nous ne pouvons pas légiférer pour venir à bout d'un problème de mésinformation et de désinformation.[34] » Pour élucider les activités malveillantes de la guerre cognitive, il faut disposer de renseignements provenant de sources multiples et d'analyses approfondies appuyés par les talents, les technologies, le savoir-faire et la capacité d'opérer clandestinement dans l'ensemble des réseaux et des domaines humains. Pour contrecarrer les adversaires, il faut une sécurité opérationnelle et une infrastructure

auxiliaire furtive et sophistiquée. Par conséquent, [traduction] « les armées occidentales doivent travailler plus étroitement avec [le secteur privé] et le secteur des sciences sociales et humaines [pour] aider l'alliance à développer ses capacités en matière de guerre cognitive [défense]. »

L'analyse du renseignement, comme méthode de collecte et d'analyse de l'information et sa transformation en renseignements exploitables, sera essentielle pour prévenir et combattre la guerre cognitive. Ces objectifs peuvent être atteints par les moyens suivants :

- Créer une base de données sur les tactiques de guerre cognitive les plus courantes et les catégoriser selon les différents acteurs malveillants.
- Surveiller les sources d'information et leur authenticité.
- Utiliser des technologies pour analyser et vérifier l'authenticité des données.
- Collaborer avec d'autres organismes pour échanger des renseignements essentiels.

Toutefois, à l'ère moderne, il est impossible de détecter, de contrer ou de dissuader efficacement les attaques cognitives sans un solide programme de renseignement de sources ouvertes et des capacités d'évaluation robustes. La recherche de menaces, l'attribution des entités ultimes et le recensement des réseaux techniques à l'origine des campagnes d'information sont également nécessaires avant de présenter un contre-discours. La réponse à la guerre cognitive sera ancrée dans la planification spécialisée d'analyses dirigées par l'humain et accélérées par la technologie et comportant des composantes clés[iii]. La création de programmes de sources ouvertes dans les cultures cloisonnées de la communauté du renseignement comporte ses propres difficultés, en particulier lorsqu'une industrie mature de renseignement de sources ouvertes (OSINT) est déjà en place. À bien des égards, le secteur privé a joué un rôle important dans la lutte à grande échelle contre la radicalisation, l'influence et le filtrage de la mésinformation et de la désinformation sur la scène mondiale pendant des décennies. Les adversaires de l'OTAN externalisent leurs opérations de désinformation et de guerre cognitive.

Cette solution nécessitera une plateforme unifiée et un environnement collaboratif d'analyse capable de traiter les mégadonnées ainsi qu'une formation commune. La création de programmes de sources ouvertes dans les cultures cloisonnées de la communauté du renseignement comporte ses propres difficultés, en particulier lorsqu'une industrie mature de renseignement de sources ouvertes (OSINT) est déjà en place. À bien des égards, le secteur privé a joué un rôle important dans la lutte à grande échelle contre la radicalisation, l'influence et le filtrage de la mésinformation et de la désinformation sur la scène mondiale pendant des décennies. Les adversaires de l'OTAN externalisent leurs opérations de désinformation et de guerre cognitive. Par conséquent, les solutions doivent être fondées sur des partenariats public-privé solides.

L'alliance doit reconnaître la dynamique interreliée des conflits contemporains. Pour contrer l'empiètement dans le domaine cognitif et se prémunir contre des tactiques comme les opérations psychologiques, la tromperie et la guerre électronique, l'OTAN doit intégrer des cybercapacités pour perturber ou contrôler les systèmes d'information, les réseaux et les données.

La sécurité nationale et la résilience sociale peuvent être renforcées en adoptant une approche à l'échelle de la société, qui combine les secteurs civil, économique, commercial et militaire. Cette approche doit favoriser la collecte planifiée des données, l'échange sécurisé des données et leur gestion efficace. La division du pouvoir, les technologies perturbatrices et les manœuvres d'adversaires sophistiqués et de plus en plus belligérants produiront de nouveaux effets plus rapidement que les organisations traditionnelles peuvent s'y adapter. Les solutions nécessiteront une orchestration centralisée puisque les enjeux touchent l'ensemble des domaines, des mandats et des missions.

Les réponses politiques et juridiques à la désinformation et à la mésinformation doivent être adoptées de façon proportionnelle et après mûre réflexion. La lutte contre la désinformation doit tenir compte de valeurs concurrentes, y compris la protection de la vie privée et les libertés fondamentales. Dans certains cas, le blocage et l'élimination numériques peuvent être justifiés.

En fin de compte, le Canada et ses alliés de l'OTAN doivent contrer la guerre cognitive, notamment au moyen de cyberopérations, en identifiant et en perturbant les réseaux de désinformation. Toutefois, les alliés doivent éviter de pratiquer la propagande noire ou la désinformation publique afin de préserver la confiance et de respecter les valeurs démocratiques.

La réalisation d'une enquête exhaustive et de la déconstruction d'une campagne de guerre cognitive menée par des adversaires contre les pays de l'OTAN comporte divers éléments essentiels, notamment l'appréciation renseignement, l'analyse tactique graphique, l'analyse tactique de l'environnement opérationnel et l'analyse de systèmes d'objectifs reliés aux réseaux pertinents d'influence hostile. De plus, l'exécution d'évaluations exhaustives contre les membres militaires de l'OTAN comporte l'analyse des surfaces d'attaque, l'évaluation de la résilience et la détermination de la vulnérabilité à la gamme complète des attaques de la guerre cognitive, aboutissant à l'identification des lacunes en matière de capacités.

Renforcer les défenses alliées contre les menaces de la guerre cognitive suppose la conception, la mise à l'essai et la sélection de contre-mesures efficaces, telles que les tactiques de contre influence, les stratégies de cyberdéception, les méthodes de recherche de menaces, les techniques de poursuite antagoniste, les approches de ciblage, les activités de réduction des menaces et les mécanismes de cyberdéfense active.

Conclusion

Au milieu des années 2000, le major-général Robert H. Scales, ancien commandant de l'École supérieure de guerre des États-Unis, s'est prononcé comme suit sur l'avenir de la guerre : [traduction] « la victoire sera définie davantage en termes de capture du contexte psychoculturel plutôt que du terrain géographique[35]». L'évocation de cette prédiction en 2024 démontre le caractère prémonitoire de sa déclaration, soulignée par le chef d'état-major des armées canadiennes sortant, M. Eyre, le 18 juillet 2024 : [traduction] « Outre la menace de guerre, l'autre menace la plus importante pour notre nation est la désinformation. La nature de la guerre reste, pour reprendre les termes de Clausewitz, un concours de volonté humaine. Mais si cette volonté peut être influencée avant le premier coup de feu, il est possible de gagner sans combattre. Nos institutions de démocratie libérale sont assaillies par un bombardement constant de théories du complot et de mensonges qui façonnent un récit de méfiance et de déclin. Ces théories et ces mensonges sont créés à la fois à l'intérieur et à l'extérieur du pays. Dans l'approche stratégique des trois guerres de la Chine communiste, cela s'appelle la guerre cognitive. Notre propre institution est prise pour cible tous les jours, car nous voyons des trolls pro-Kremlin adapter leur propagande insidieuse pour causer un maximum de dégâts - dans de nombreux cas, avec des attaques personnelles fabriquées de toutes pièces. » La désinformation exerce une emprise croissante dans le cadre des efforts déployés par des acteurs malveillants pour promouvoir leurs intérêts nationaux. Les valeurs qui font la force des sociétés occidentales, à savoir l'ouverture, le multiculturalisme, la liberté d'expression et la libre circulation de l'information, les rendent également vulnérables aux attaques cognitives, qui emploient la désinformation comme un cheval de Troie mental pour pénétrer le périmètre de l'esprit et le corrompre de l'intérieur. Autrement dit, ces valeurs représentent le « centre de gravité » clausewitzien que les adversaires attaquent sans relâche. Les techniques sophistiquées de manipulation de l'information peuvent miner les facultés essentielles des citoyens. La désinformation dans le cadre de la guerre cognitive mobilise directement les craintes, les préjugés et la haine des gens. Face à la polarisation sociale croissante, au mécontentement et à la discorde causés par la désinformation ciblée, la population des sociétés démocratiques doit consacrer des ressources importantes à la sensibilisation et à la formation d'un public informé, résilient et capable de discerner les faits de la fiction grâce à une analyse critique et sceptique de l'information véhiculée par les médias.

Comme l'a fait remarquer Vasily Gatov, analyste des médias, [traduction] « si le XXe siècle a été défini par la lutte pour la liberté de l'information et contre la censure, le XXIe siècle sera défini par des entreprises, des acteurs ou des États malveillants qui portent atteinte au droit à la liberté de l'information[36] ». La gouvernance pose également des défis importants. Dans l'avenir émergent, les gouvernements doivent faire face à la réalité actuelle dans laquelle les acteurs à la fois étatiques et non étatiques se partagent le pouvoir. Pour préserver l'intégrité de l'information et consolider les défenses cognitives, le Canada et ses alliés devraient prendre des mesures proactives qui renforcent la résilience collective. Quant au Laboratoire sur l'intégrité de l'information, il joue un rôle important en servant de centre d'analyse rigoureuse et en facilitant un dialogue constructif entre d'éminents spécialistes. Les multiples complexités du contexte

moderne de l'information exigent la collaboration, l'innovation et, surtout, un discours éclairé. Le Canada et ses partenaires doivent s'efforcer de relever les défis posés par la prolifération des activités liées à la guerre cognitive et s'assurer de préserver les valeurs démocratiques dans un monde libre.

Il n'y a pas de rempart unique ni de mur extérieur que l'État peut construire pour se prémunir contre la guerre cognitive. Les murs défensifs devront être de nature psychologique. Les gouvernements ont intérêt à offrir aux citoyens une formation numérique poussée qui développe et affine leur pensée critique, en les outillant pour reconnaître et combattre la désinformation au moment où elle se présente. Les stratégies proactives accroissent non seulement la résilience personnelle, mais renforcent également les mesures de protection sociales contre la manipulation et la mystification. Des mesures rigoureuses, y compris celles décrites dans le rapport, sont essentielles pour immuniser les populations contre les intrusions mentales et préserver la prospérité, la stabilité et la liberté des sociétés démocratiques.

Remerciements

Nous tenons à exprimer notre gratitude à M. Anvesh Jain et à Mme Mariana Savka pour leur précieuse contribution et leurs commentaires sur le rapport.

Notes en fin d'ouvrage

[i] Dans ce contexte, la sémiotique s'entend des signes et des symboles et de leur utilisation ou interprétation, tandis que l'iconographie désigne les images et leur signification.

[ii] Les réseaux de zombies sémantiques sont des réseaux automatisés qui utilisent l'intelligence artificielle pour créer et diffuser la désinformation.

[iii] Y compris les renseignements mondiaux sur les cybermenaces, les OSINT, les renseignements sur les médias sociaux, les experts humains, la cyberdéfense active, l'attribution, la recherche de menaces, le ciblage et la génération d'effets avec des résultats mesurables.

Endnotes

1 Kimberly Underwood, « Cognitive Warfare Will Be Deciding Factor in Battle », SIGNAL Magazine, août 2017.
2 Shay, Shaul. « Between Kiev and Venice the cognitive warfare and the Biennale of Venice. » Security Science Journal, vol. 3, no 2, 31 décembre 2022, p. 101 à 117.
3 Kuperwasser, Y., et Siman-Tov, D. The cognitive campaign: Strategic and intelligence perspectives. Tel-Aviv : Institute of National Security Studies, 2019.
4 Ottewell, Paul. « The Disinformation Age: Towards a Net Assessment of the United Kingdom's Cognitive Domain. » Expeditions with MCUP, 2022.
5 du Cluzel, François, « NATO Cognitive Warfare, a Battle for the Brain », Commandement allié Transformation de l'OTAN, 2020.
6 Pappalardo, David. « Win the War Before the War?: A French Perspective on Cognitive Warfare. » War on the Rocks, juillet 2022.
7 Rutheford, Nicholas. About mis-disinformation, its potential impacts, and the challenges to finding effective Countermeasures. Laboratoire sur l'intégrité de l'information, février 2023.
8 Ken Klippenstein et Lee Fang. « Leaked Documents Outline DHS's Plans to Police Disinformation. » The Intercept, juillet 2023.
9 Chan, Kelvin. « TikTok Bans Deepfakes of Young People as It Updates Guidelines », Associated Press News, 22 mars 2023, apnews.com/article/tiktok-china-cybersecurity-data-privacy-595f9ae7c0a1fc22f0b285 cede6bd67c.
10 Pomarantsev, Peter. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. Institute of Modern Russia, 2014.
11 « Cognitive Warfare: Strengthening and Defending the Mind », Commandement allié Transformation de l'OTAN, 2023.
12 Service canadien du renseignement de sécurité, Menaces d'ingérence étrangère visant les processus démocratiques du Canada, 2021.
13 Gouvernement du Canada, « RT et RT France ne peuvent plus être distribuées par les fournisseurs de services de télévision canadiens », mars 2022.
14 Russia Today, « Distribution », https://www.rt.com/about-us/distribution/.
15 Orr Bueno, Caroline. « Russia's role in the far-right truck convoy. » The Journal of Intelligence, Conflict, and Warfare, vol. 5, no 3, 31 janvier 2023.
16 Kolga, Marcus. Russia's threat to Canadian democracy and the Arctic. MacDonald-Laurier Institute, avril 2022.
17 Orinx, K., Tanguy Struyede Swielande. « China and Cognitive Warfare: Why Is the West Losing? »; Bernard Claverie, Baptiste Prébot, Norbou Beuchler et François du Cluzel. Cognitive Warfare: The Future of Cognitive Dominance, Collaboration Support Office de l'OTAN, p. 1 à 6 et 8, 2022.
18 Momani, Besma. « International Security: Canada's Role in Meeting Global Threat ». Canadian Centre for International Governance Innovation, 2021.
19 « Chinese State Interference in Canada's 2021 Election ». DisinfoWatch, septembre 2021, disinfowatch.org/chinese-state-interference-in-canadas-2021-election/.
20 du Cluzel, François, « Cognitive Warfare », Centre d'innovation de l'OTAN, 2020.
21 Ibid., du Cluzel.
22 Marsili, Marco. « Guerre à la carte : Cyber, information, cognitive warfare and the metaverse. » Applied Cybersecurity & Internet Governance, vol. 2, no 1, 28 décembre 2023.
23 Shay, Shaul. « Between Kiev and Venice the cognitive warfare and the Biennale of Venice. » Security Science Journal, vol. 3, no 2, 31, p. 101 à 117, décembre 2022.
24 Claverie B., B. Prébot, N. Buchler et F. Du Cluzel. Cognitive Warfare: The Future of Cognitive Dominance. Première rencontre scientifique de l'OTAN sur la guerre cognitive (France) – juin 2021 et mars 2022.
25 Gouvernement du Canada, « Défendre le Canada contre la guerre cognitive », novembre 2021.
26 Ibid. Gouvernement du Canada.
27 Gouvernement du Canada, « Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada », avril 2023.
28 Ibid., « Notre Nord, fort et libre : Une vision renouvelée pour la défense du Canada ».
29 Gouvernement du Canada, Cyberattribution pour la défense du Canada, 2023.
30 Chambre des communes du Canada, Comité permanent de la défense nationale, février 2024.
31 Faiswal, Kasirye, « The Importance of Needs in Uses and Gratification Theory ». Avance. Mai 2022.
32 Baker, Eva et coll. International Encyclopedia of Education. 3e éd., Elsevier Science, 2010.
33 Vaccari, C. et Chadwick, A. « Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News ». Social Media + Society, 6(1), 2022.
34 Shull, Aaron et Wark, Wesley, « Reimagining a Canadian National Security Strategy », Center for Internation Governance Innovation, décembre 2021.
35 « The 21st Century Game-Changer: Cognitive Warfare », Centre de combat interarmées de l'OTAN, 2023.
36 Ibid., Pomarantsev.

Infolab.uOttawa.ca
Labinfo.uOttawa.ca