National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

LES OPÉRATIONS D'INFORMATION: UN ENJEU SIGNIFICATIF POUR LES FORCES ARMÉES CANADIENNES

Major Michael Janelle

JCSP 45

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

LES OPÉRATIONS D'INFORMATION: UN ENJEU SIGNIFICATIF POUR LES FORCES ARMÉES CANADIENNES

Major Michael Janelle

Word count: 6217

Nombre de mots: 6217

INTRODUCTION

Depuis les attentats du 11 septembre 2001, les États-Unis et la coalition ont été confrontés à un affrontement qui non seulement redéfinit l'avenir du conflit, mais contribue également à redéfinir l'organisation et les méthodes de fonctionnement du gouvernement et des forces armées.[1]1 Les raisons de ce changement dynamique sont nombreuses, mais la raison la plus importante réside dans l'émergence de nos adversaires potentiels qui ont incontestablement utilisé des moyens non conventionnels pour déjouer les forces militaires conventionnelles.

Le paradigme de l'information n'était pas le seul domaine négligé au crépuscule de la mentalité de la guerre froide. De même, les politiques et la doctrine des forces armées en matière de guerre contre-insurrection (COIN) ont été ignorées. Les leaders politiques et les populations touchées ne peuvent plus être considérés comme une simple augmentation des efforts cinétiques plus tangibles des opérations militaires traditionnelles.

Alors que le Canada poursuit ses efforts, il est clair que le rôle des opérations d'information (OI) relativement aux opérations cinétiques a été grandement mal compris. Cette situation est attribuable en grande partie à l'absence d'une compréhension commune du concept des OI au sein de la communauté militaire et à l'absence de directives doctrinales cohérentes sur la façon d'intégrer adéquatement les OI dans les opérations COIN. Compte tenu de ces lacunes doctrinales, les commandants qui sont mal à l'aise avec le concept des OI ont tendances à systématiquement diminuer son importance à des éléments cinétiques plus tangibles des opérations COIN. La nature politiques de celles-ci ainsi que la disponibilité accrue d'information contribuent grandement à la complexité de la situation.

---

[1] Leigh, Annistead, *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, DC: Brassey's Inc. 2004), p. 1.

La doctrine commune des Forces armées canadiennes (FAC) définit les OI comme «des actions entreprises à l'appui d'objectifs politiques et militaires qui influencent les décideurs en influant sur les informations des autres tout en exploitant et en protégeant leurs propres informations».[2]

Depuis la fin de la guerre froide, le Canada et ses alliés de l'OTAN, en particulier les États-Unis, ont réorganisé leurs forces militaires afin de lutter contre les opérations de contre-terrorisme et COIN. Nos adversaires potentiels, principalement la Russie et la Chine, ont continué de développer leurs capacités d'information et de guerre politique. En conséquence, un fossé important entre les connaissances et les capacités en matière d'information existe maintenant entre l'OTAN et ces adversaires potentiels.

Afin de fonctionner efficacement dans l'environnement opérationnel actuel, les FAC doivent mettre à jour leur capacité et leur doctrine en matière d'OI afin de s'aligner sur celles de nos adversaires potentiels. Les FAC doivent également travailler en étroite collaboration avec les autres ministères du gouvernement canadien afin de développer les médias sociaux et la cyber doctrine afin de contrer efficacement les menaces potentielles contre les cibles canadiennes, y compris la population civile.

Les OI prennent de plus en plus d'importance dans tous les domaines des environnements militaire, politique, industriel et social, et plusieurs questions demeurent sans réponse. Ce document tentera de mettre en lumière certains des problèmes actuels et de fournir des recommandations de solutions potentielles pour l'avenir. Ce document prouvera que les FAC doivent adapter leur doctrine et leurs capacités en matière d'OI pour opérer efficacement dans le contexte opérationnel changeant d'aujourd'hui.

---

[2] Department of National Defence, B-GG-005-004/AF-033 *Canadian Forces Information Operations* (Ottawa:1998-04-02), p. I3.

OPÉRATIONS D'INFORMATION ET CYBER

La nature de la guerre change et évolue. Il ne s'agit plus seulement de savoir qui a l'armée la plus importante, mais aussi de savoir qui a la meilleure information sur le champ de bataille; inclure tous les acteurs, qu'ils soient étatiques ou non, combattants ou non, militaires ou civils.[3] À cette fin, les OI sont devenues un élément important de la guerre moderne. Des batailles et des conflits sont parfois entièrement livrés dans le domaine de l'information. Le domaine de l'information et le conflit de l'information ont estompé les frontières entre la paix, le conflit et la guerre.[4] Le domaine de l'information a la capacité de perturber et d'éroder les hiérarchies autour desquelles nos institutions sont formées. Il peut également diffuser et redistribuer le pouvoir, souvent au profit des acteurs les plus faibles et les plus petits.[5] Des États, comme la Russie et la Chine, l'utilisent comme un moyen d'obtenir un avantage asymétrique par rapport au très grand États militaires. Les OI sont devenues un élément fondamental de la guerre moderne, non seulement pour les forces armées dotées de pouvoir informatique comme celles des États-Unis et de la Russie, mais également pour les forces de pointe. Les groupes d'insurgés bénéficient de l'utilisation d'Internet pour recruter des combattants et financer des opérations. Les médias sociaux sont exploités à des fins allant de la transmission d'informations de ciblage à la direction du déploiement des forces, comme ainsi que des campagnes de recrutement et de désinformation.[6]

Les conflits ou activités d'information entre nations et sociétés ont pour but de perturber, de détériorer ou de modifier les connaissances ou les croyances d'une population cible sur elle-même et sur le monde. Les activités d'information couvrent l'ensemble des conflits, qu'ils soient

---

3 Arquilla, John, and David Ronfeldt, *Cyberwar is Coming!*, (Santa Monica: RAND Corporation, 1997), p. 23.
4 Ehrhart, Hans-Georg, *Postmodern warfare and the blurred boundaries between war and peace*, (Defense & Security Analysis 33, No. 3, 2017), p. 264.
5 Arquilla, John, and David Ronfeldt, *Cyberwar is Coming!*, (Santa Monica: RAND Corporation, 1997), p. 23.
6 Schmitt, Michael N, *The Law of Cyber Targeting*, (Naval War College Review 68, Iss. 2, 2015), p. 11.

politique, économique, social ou militaire. Contrairement aux guerres économiques, qui ciblent la production et la distribution de biens, et aux guerres politiques, qui visent le leadership et les institutions d'un gouvernement, les OI peuvent affecter tous ces domaines en ciblant l'information et les communications.

La fusion des moyens civils et militaires est un autre aspect important de l'environnement de l'information. La pertinence des moyens civils en opération augmente. Cela est dû au lien entre la sécurité et le développement qui est devenu la norme dans le contexte des interventions militaires. La combinaison de la sécurité et du développement vise à stabiliser le pays hôte tout en gagnant la population. Les activités d'information jouent un rôle important dans la fusion des efforts civils et militaires en une approche pangouvernementale.[7]

Jusqu'à présent, le conflit d'information ne connaît pas de limites réelles. Le cyber domaine émergent, associé au reste du domaine de l'information, n'est pas réglementé et est exploité dans une nouvelle forme de conflit.[8] La bataille physique peut être gagnée sur le champ de bataille mais perdue devant l'opinion publique, si l'une des parties agi contre la loi, ou semble agir contre le droit des conflits armés. Compte tenu de la nouveauté de l'information et des opérations cyber, toute utilisation abusive présumée au niveau tactique peut même avoir un potentiel de conséquences stratégiques.[9]

Les opérations cyber, gagnent en importance pour les gouvernements occidentaux. Il y a eu une série d'attaques contre des systèmes informatiques gouvernementaux en provenance de Chine et de Russie, notamment un cyber assaut russe contre l'Estonie et des attaques chinoises

---

7 Ehrhart, Hans-Georg, *Postmodern warfare and the blurred boundaries between war and peace*, (Defense & Security Analysis 33, No. 3, 2017), p. 265.

8 *Ibid*. p. 270.

9 Schmitt, Michael N, *The Law of Cyber Targeting*, (Naval War College Review 68, Iss. 2, 2015), p. 12.

contre des cibles militaires et économiques américaines et japonaises.[10] Récemment, le piratage russe d'ordinateurs du comité national démocrate lors des élections présidentielles américaines de 2016 a également fait les gros titres. Nos adversaires potentiels se sont montrés à la fois doués pour les aspects techniques des OI, tels que les opérations cyber, et psychologiques, comme les campagnes de désinformation sur les réseaux sociaux.

Stratégie de guerre de l'information (GI) et opérations d'information (OI)

La théorie militaire moderne, qui remonte à l'époque napoléonienne, divise la guerre en trois niveaux: stratégique, opérationnel et tactique. La stratégie peut être définie comme le processus de planification pour atteindre les objectifs et les buts dans l'intérêt national. Pour les militaires, il s'agit généralement de déterminer la fin, les moyens et la manière d'atteindre les objectifs énoncés. Le dictionnaire du Ministère de la Défense Nationale (MDN) définit le niveau stratégique de la guerre comme le niveau auquel une nation, souvent en tant que membre d'un groupe de nations, détermine les objectifs et les orientations stratégiques de sécurité nationale ou multinationale (alliance ou coalition), puis développe et utilise les ressources nationales pour atteindre ces objectifs.[11] La GI se déroule au niveau stratégique, tandis que les opérations d'information (OI) font appel à diverses capacités liées à l'information pour mettre en œuvre la stratégie. Le niveau opérationnel est celui où les campagnes et les opérations importantes sont planifiées, menées et soutenues pour atteindre les objectifs stratégiques dans les théâtres d'opérations ou d'autres zones opérationnelles.[12] Le niveau tactique de la guerre concerne l'arrangement ordonné et la manœuvre des éléments de combat en relation les uns avec les autres

---

10 Black, Jeremy, *Into the Future*, (Bloomington: Indiana University Press, 2013), p. 253.
11 Defence Terminology Standardization Board; DND/CF Manual of Abbreviations; AAP-15.
12 *Ibid*.

et avec l'ennemi pour atteindre les objectifs de combat.[13] Les OI se produisent au niveau opérationnel, reliant les capacités et les tactiques liées à l'information d'une stratégie plus vaste.

ALLIÉ

Les États-Unis

Les OI sont définies dans la publication conjointe 3-13.1, doctrine commune pour la guerre de commandement et de contrôle comme les «mesures prises pour obtenir la supériorité de l'information en affectant l'information adverse, les processus basés sur l'information, les systèmes d'information et les réseaux informatiques, tout en défendant sa propre information, les processus basés sur l'information, les systèmes d'information et les réseaux informatiques.»[14] Plus concrètement, dans le manuel FM 100-6 Information Operations, l'armée de terre américaine définit les OI comme étant des opérations militaires continues dans le contexte militaire qui permettent, améliorent et protègent la capacité de la force amie de recueillir, de traiter et de communiquer des renseignements personnels, et d'agir sur l'information pour obtenir un avantage dans toute la gamme des opérations militaires. Les OI comprennent l'interaction avec l'environnement mondial de l'information et l'exploitation ou le refus des capacités d'information et de décision d'un adversaire.[15] Le but de ces opérations est la domination de l'information, ou le degré de supériorité de l'information qui permet au possesseur d'utiliser les systèmes et les capacités d'information pour obtenir un avantage opérationnel dans un conflit ou pour contrôler la situation dans des opérations autre que la guerre, tout en refusant ces capacités à l'adversaire.[16]

Fonctionner dans l'environnement de l'information

---

13 *Ibid*.
14 Joint Chiefs of Staff (JCS) Pub 3-13.1, *Joint Command and Control Warfare (C2W) Operations*, (1996), p. I3.
15 Department of the Army Field Manual 100-6, *Information Operations*, (1996), p. 8.
16 *Ibid*, p. 8.

Depuis février 2015, l'armée de terre américaine participe de façon accrue aux exercices interarmées et interalliés visant à démontrer la capacité des États-Unis à respecter leurs obligations en matière de sécurité collective, en envoyant des signaux clairs et visibles au sujet de la puissance de combat crédible et la compétente des États-Unis.

Ces engagements ont permis de dégager un certain nombre de leçons apprises et de pratiques exemplaires en ce qui concerne la synchronisation des capacités liées à l'information dans un environnement d'information contesté mettant en cause un concurrent.[17] Les barrières entre les capacités liées à l'information et la synchronisation efficace de ces capacités ont affaibli la capacité des unités tactiques de se battre et de gagner dans l'environnement de l'information. Ces obstacles découlent d'une combinaison de changements doctrinaux et de la conception de la force.

Changements doctrinaux

En 2014, l'armée de terre américaine a mis fin à l'utilisation de la doctrine promulguée par le manuel FM 3-13, Inform and Influence Activities, qui avait été publiée en janvier 2013.[18] Cette doctrine a souligné le rôle important des capacités liées à l'information pendant les guerres en Irak et en Afghanistan. Et même si elle est fondée sur la doctrine des OI, elle ne fait que mettre l'accent sur les capacités plus axées sur l'humain, comme les engagements clés des leaders, les affaires publiques et les opérations de soutien de l'information militaire (OSIM).

Ainsi, la doctrine de l'armée de terre américaine est revenue à la définition conjointe d'OI, soit «l'emploi intégré, pendant les opérations militaires, de capacités liées à l'information de concert avec d'autres lignes d'opération pour influencer, perturber, corrompre ou usurper la prise

---

17 Joint Chiefs of Staff (JCS) Pub 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office, 2014), GL-3, p. III-2.

18 Department of the Army Field Manual 3-13, *Inform and Influence Activities*, (2013), p. I-3.

de décision des adversaires et des adversaires potentiels tout en protégeant les nôtres.»[19] L'armée de terre américaine a également créé une doctrine distincte pour les activités cyber-électromagnétiques (CEMA) en reconnaissance de l'importance des opérations dans le cyberespace et de la guerre électronique (GE).[20]

Ces changements doctrinaux ont contribué à une meilleure compréhension de la relation entre les OI et les CEMA. L'armée de terre américaine a fait des CEMA une fonction d'intégration semblable à celle des OI et a mis l'accent sur l'importance des opérations dans le cyberespace et des capacités de GE. Cela souligne l'importance de l'utilisation synchronisée des capacités liées à l'information pour créer, dans l'environnement de l'information, les conditions propices à la réalisation de l'état final souhaité par le commandant.

Les adversaires potentiels des États-Unis et de leurs alliés mènent des activités dans tout le domaine de l'information, et non seulement dans le cyberespace, pour atteindre leurs objectifs.[21] Ils n'ont pas créé les mêmes barrières entre les capacités comme les affaires publiques, le contre-espionnage, la tromperie militaire, les opérations dans le cyberespace, la GE et la sécurité des opérations. Ils utilisent agressivement des agents étrangers pour exploiter les faiblesses des opérations en matière de sécurité. Ils utilisent ce qu'ils apprennent de ces efforts de collecte pour créer des produits d'hameçonnage ciblés conçus pour avoir accès à des réseaux d'information conviviaux. Ils exploitent l'information en diffusant de la désinformation et de la propagande en tant qu'activités médiatiques conventionnelles. Ils induisent en erreur et trompent

---

19 Joint Chiefs of Staff (JCS) Pub 3-13, *Information Operations* (Washington, DC: U.S. Government Publishing Office, 2014), GL-3, p.II-1.

20 Joint Chiefs of Staff (JCS) Pub 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office, 2017), p. 1-1.

21 Timothy L, Thomas, *Comparing US, Russian and Chinese Information Operation Concepts*, (Fort Leavenworth, Foreign Military Studies Office, 2004), p. 11.

pour créer de la confusion et des défis d'action collective qui empêchent des réponses cohésives à leurs actions.

Pour surmonter les difficultés liées à l'incidence du domaine de l'information sur l'avantage opérationnel, l'armée de terre américaine a dû changer la culture au sein de son organisation. Pour ce faire, il a fallu mettre l'accent sur le commandement et créer des organisations d'état-major efficaces capables d'exécuter les activités liées à l'information et de synchroniser de multiples activités liées à l'information afin de modifier le domaine de l'information pour en tirer un avantage opérationnel. Les commandants, les officiers d'état-major et les dirigeants à tous les niveaux discutent régulièrement de ces défis, coopèrent avec les médias, et ils utilisent les sites web et les médias sociaux pour mobiliser les auditoires clés. Ainsi, chaque action reliée à l'environnement de l'information envoie un message distinct et démontre la capacité de l'armée de terre américaine de planifier, de préparer et d'exécuter des tâches tactiques qui accomplissent les objectifs stratégiques établis.[22]

De plus, tout individu et toute unité est en partie responsable de protéger les systèmes d'information et de commandement de mission essentiels en synchronisant les capacités liées à l'information, la cyber sécurité, les opérations de défense du cyberespace, et la sécurité des opérations. Les commandants à tous les niveaux doivent s'assurer que leurs formations sont capables de fonctionner dans un environnement d'information contesté.[23]

Au niveau de brigade, le commandant et l'officier des opérations mettent l'accent sur la synchronisation avec l'officier des OI affecté à l'état-major. Au niveau de division, l'officier des OI joue un rôle crucial en fournissant des ressources au commandant de brigade et à son état-major, ainsi que des moyens de synchronisation. L'adoption d'une approche d'exploitation de

---

22 Joint Chiefs of Staff (JCS) Pub 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: U.S. Government Publishing Office, 2017), p. 1-1.

23 *Ibid*. p. 1-1.

l'environnement de l'information tire parti des efforts de l'armée de terre américaine pour renforcer les capacités cyber afin de suivre l'évolution rapide des menaces dans le cyberespace.

De plus, l'armée de terre américaine envisage d'effectuer une évaluation globale axée sur les capacités de ses OI et de ses forces de capacités liées à l'information afin de s'assurer qu'elles disposent de ressources suffisantes pour répondre aux besoins. Si l'armée de terre a l'intention de se battre et de gagner dans un cet environnement contesté, elle devra continuer de développer les capacités liées à l'information. Les capacités CEMA créent à elles seules des conditions nécessaires, mais non suffisantes, au succès. La fonction de synchronisation des OI est essentielle pour traduire les capacités techniques en effets sur le champ de bataille qui créent un avantage opérationnel pour le commandant.[24]

ADVERSAIRES

Les États nations et les organisations terroristes ont recours à la GI pour atteindre leurs objectifs stratégiques. Les exemples suivants mettent en lumière la façon dont les concurrents et les adversaires cherchent à optimiser leur ciblage des réseaux d'information et des concepts opérationnels canadiens, tout en utilisant d'autres domaines de compétition que la guerre ouverte pour atteindre leurs objectifs.

La Russie

La Russie a maintenu sa position de grande puissance, malgré sa faiblesse matérielle relative, grâce à son utilisation supérieure de l'information comme un outil politique asymétrique. Les dirigeants russes considèrent les OI comme un outil décisif du pouvoir de l'État et une façon d'engager dans la concurrence internationale continue dans le domaine de l'information exécuté par des acteurs étatiques et non étatiques. Ces efforts coordonnés pour projeter l'influence en utilisant l'information et la désinformation font partie intégrante la

---

[24] *Ibid*. p. 1-5.

politique étrangère russe. La logique des OI guide souvent les efforts militaires, diplomatiques et économiques coordonnés de la Russie. Alors que les OI des autres états sont généralement guidées par des faits, les décideurs russes créent des faits à diffuser auprès de publics cibles afin d'atteindre les objectifs stratégiques.

Bien que la Russie ait employé l'information comme un outil de l'état depuis 2013, ses penseurs militaires ont adopté une nouvelle approche de l'information qui place de telles considérations au cœur de leur stratégie. Les russes utilisent des termes tels que la guerre de nouvelle génération, guerre de nouveau type, la guerre hybride, et la guerre non linéaire pour décrire le contexte militaire contemporain et leur doctrine.[25] Tout comme les anciens dirigeants soviétiques, les dirigeants militaires russes d'aujourd'hui ont tenté de dissimuler leurs intentions et de malmener leurs concurrents en accusant leurs adversaires de l'utilisation des capacités militaires contre la Russie.[26]

Le chef d'état-major russe, le général Valery Gerasimov, a noté l'efficacité avec laquelle les puissances occidentales utilisaient l'information pour subvertir les États. En outre, le Kremlin affirme que les révolutions de couleur en Géorgie (2012), en Ukraine (2004) et au Kirghizistan (2005), que le printemps arabe au Moyen-Orient et en Afrique du Nord (2010-2011), et même à les protestations à Moscou (2011-2012) ont été le résultat d'interventions de l'Ouest utilisant la guerre hybride.[27] La Russie affirme que seuls les États étrangers mènent des opérations de guerre hybride. Mais la Russie le fait clairement aussi. En tant que secrétaire de presse du président russe Vladimir Poutine, Dmitri Peskov a déclaré en 2017, «Si vous appelez ce qui se passe maintenant une guerre hybride, que ce soit une guerre hybride n'a pas d'importance, c'est la

---

25 Timothy L, Thomas, *The Evolving Nature of Russia's Way of War*, (Military Review 97, No. 4, 2017), p. 35.

26 Timothy L, Thomas, *Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War*, (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), p. 5.

27 Nicolas, Bouchet, *Russia's 'Militarization' of Colour Revolutions*, (CSS Policy Perspectives 4, No. 2, 2016), p. 2.

guerre.»[28] Les OI, un élément clé de la guerre contemporaine de la Russie, englobe toutes les utilisations de l'information et de la désinformation, par des états ou des acteurs non étatiques, en tant qu'outil du pouvoir de l'état et comprend les opérations militaires de soutien de l'information, les opérations cyber, la GE, la guerre psychologique, les affaires publiques, et de la communication stratégique.

Le concept de défense de la Russie définit le futur des OI comme «une capacité de saper les systèmes politiques, économiques et sociaux, et d'effectuer des campagnes contre la population d'un État pour déstabiliser la société et forcer le gouvernement à prendre des décisions dans l'intérêt de leurs adversaires.»[29] La doctrine militaire russe décrit également une conception plus large de «la confrontation dans le domaine de l'information qui incorpore le champ de bataille militaire, le cyberespace et les effets informationnels et psychosociaux conçus pour manipuler la perception et le comportement des publics cibles.»[30] Les OI ont un impact sur la dimension cognitive humaine qui est «composée des attitudes, des croyances et des perceptions de ceux qui transmettent l'information, la reçoivent et y répondent.»[31]

Certains stratèges suggèrent que les organisations militaires effectuent des manœuvres cognitives pour affecter le domaine cognitif, d'une manière similaire à la Russie, mais contrairement aux conceptions occidentales, la Russie considère les OI comme un outil décisif, plutôt que qu'un élément de soutien du pouvoir de l'état.»[32]

---

28 Jim, Rutenberg, *RT, Sputnik and Russia's New Theory of War*, (New York Times Magazine, 2017), p. 3.

29 Timothy L, Thomas, *Russia's 21st Century Information War: Working To Undermine and Destabilize Populations*, (Defence Strategic Communications, No. 1, 2015), p. 12.

30 Defense Intelligence Agency (DIA), *Russia Military Power: Building a Military to Support Great Power Aspirations* (Arlington, VA: DIA, 2017), p. 38.

31 US Department of Defense (DoD), *Strategy for Operations in the Information Environment* (Washington, DC: DoD, 2016), p. 3.

32 Allison, Astorino-Courtois, *A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap*, (2017), p. 12.

Aujourd'hui, la Russie investit dans les capacités d'opérations d'information en raison de leur rentabilité et de leur impact stratégique. Malgré les récentes modernisations, la Russie est peu susceptible de vaincre les États-Unis ou l'OTAN dans un conflit militaire conventionnel. Cependant, la Russie veut réaffirmer son contrôle historique sur les anciens États soviétiques, y compris ceux qui sont membres de l'OTAN. La Russie cherche également à accroître son influence au Moyen-Orient par rapport à celle exercée par les États-Unis dans le but de renforcer le contrôle sans provoquer une guerre qu'elle ne peut pas gagner. La Russie rivalise avec l'Occident en utilisant les OI et en exploitant au maximum la zone grise de conflit sans toutefois passer la barre de la déclaration de la guerre.[33]

Cependant, même si la Russie prétend disposer d'un vaste et complexe arsenal de techniques, offrant des moyens d'influence multiples, évolués et flexibles, elle est confrontée à d'importants défis économiques et sociaux, la corruption est répandue et le ralentissement économique limite la liberté d'action. Sa prétention à être une puissance mondiale repose sur des bases faibles, politiquement, économiquement et militairement, et ses partenaires se méfient de ses intentions. Les tensions politiques internes s'accentuent et l'élite est préoccupée par d'éventuelles manifestations à grande échelle.

La propagande russe ne correspond souvent pas à la réalité et les efforts ne sont souvent pas couronnés de succès, parfois même dans les États baltes. Les tentatives russes de mobiliser leur diaspora ont largement échoué en raison d'une prise de conscience croissante des objectifs réels de la Russie, et parce que les organisations impliquées ont souvent un intérêt personnel et des ressources limitées. L'agression russe a également sensibilisé les sociétés occidentales au problème et, de ce fait, les a rendu plus résistantes. La politique énergétique de l'UE a progressivement réduit la capacité de la Russie d'utiliser l'énergie comme un outil politique.

---

[33] Hal, Brands, *Paradoxes of the Gray Zone*, (Foreign Policy Research Institute, 2016), p. 1.

La Russie est dépeinte comme une menace majeure, mais de nombreux exemples indiquent également que la Russie n'est pas particulièrement réussie. L'influence des organisations pro-russes demeure limitée, la Lituanie est un environnement défavorable pour les journalistes pro-russes et les activités russes dans le domaine de l'information ont eu un impact négligeable sur les attitudes à l'égard de l'OTAN.

La Russie a une longue histoire de coercition, mais son efficacité a été remise en question. Depuis 1990, la Russie a utilisé à plusieurs reprises la menace d'interruption de l'énergie comme une arme politique. L'effet net a été de sensibiliser l'UE à cette question, de diversifier les approvisionnements et de prendre des contre-mesures. Tandis que l'utilisation de méthodes coercitives est particulièrement importante le long de la périphérie de la nation, la Russie utilise de plus en plus l'intimidation contre des entités plus fortes comme l'OTAN, l'UE, et les États-Unis. Cette tendance à recourir à des moyens coercitifs plutôt qu'à la coopération s'est souvent avérée contre-productive, aliénant des alliés, consolidant l'opposition et conduisant à des échecs diplomatiques. L'utilisation de moyens coercitifs est un signe de faiblesse et non de pouvoir.

La Chine

La République populaire de Chine (RPC) a été sensible aux changements continus dans les contextes géopolitiques et géostratégiques, ainsi qu'à la nature changeante de la guerre.[34] Elle a façonné ses réponses en élaborant des doctrines et des stratégies militaires appropriées pour faire face aux menaces et aux défis futurs. Ainsi, la doctrine militaire de la Chine a subi au cours des années une transition de la guerre des peuples à la guerre des

[34] Pillsbury, Michael, *Chinese Views of Future Warfare*, (National Defense University, 2000), p. 414.

peuples dans des conditions modernes, puis de la guerre locale limitée à la guerre limitée dans des conditions de haute technologie.[35]

En raison de la pertinence croissante de la technologie de l'information (TI) dans la vie des gens, les individus qui participent à la GI ne sont pas tous des soldats et que quiconque comprend les ordinateurs peut devenir un combattant. La GI est peu coûteuse car la partie ciblée peut recevoir un coup paralysant à travers le filet et il peut être difficile pour cette dernière de discerner l'origine de l'attaque. Une grande quantité d'information inutile peut être créée pour bloquer ou arrêter le fonctionnement du système d'information d'un adversaire. Ainsi, une guerre populaire dans le contexte de la GI peut être menée par des centaines de millions de personnes, en utilisant des systèmes d'information modernes de type ouvert. Même la mobilisation politique pour la guerre peut être réalisée via Internet, par l'envoi de messages électroniques patriotiques et par la mise en place de bases de données pour l'éducation.[36]

La compréhension chinoise de la GI, qui était initialement basée sur des concepts occidentaux, a de plus en plus évolué vers l'évolution de sa propre orientation. Les experts chinois pensent que l'essence de la GI est la somme des capacités d'information capables de briser la volonté de résister en attaquant la compréhension cognitive et les convictions d'un ennemi, en le forçant à utiliser des moyens cinétiques pour atteindre ses objectifs militaires, la guerre électronique, le secret opérationnel et la guerre psychologique.[37]

Les deux domaines généraux sont la protection de l'information (défense) et l'attaque contre l'information. La défense de l'information consiste à empêcher la destruction de ses propres systèmes d'information et à s'assurer que ces systèmes peuvent remplir leurs

---

35 *Ibid*. p. 412.
36 *Ibid*. p. 412.
37 Timothy L, Thomas, *China's Electronic Strategies*, (Military Review 81, No. 3, 2001), p. 72.

fonctions normales. Dans les guerres futures, les systèmes d'information deviendront des priorités de combat, les cibles principales des attaques ennemies.[38]

Les opérations d'information (OI) sont des opérations spécifiques et sont considérées comme étant au cœur de la GI, de la même manière que la GI est considérée comme étant au cœur de l'informationalisation. En fait, les OI sont une manifestation de la GI sur le champ de bataille. Elle peut être à la fois défensive et offensive et peut être menée aux niveaux stratégique, opérationnel et tactique en temps de paix ou de guerre. Les principes des OI ont été définis par les auteurs militaires chinois de manière à inclure le commandement centralisé, le contrôle décentralisé, l'inspection et les essais multidimensionnels, la prise de décision en temps opportun et l'intégration des actions militaires et civiles en mettant l'accent sur les liens clés. Les OI intégrées et interarmées donnent plus de portée et de but à la guerre des peuples. Il définit les OI comme une série d'opérations dont l'environnement informationnel est la condition de base sur le champ de bataille, les systèmes d'information étant les cibles opérationnelles directes et la GE et les réseaux informatiques étant la forme principale. Selon l'approche traditionnelle chinoise, les stratégies peuvent compenser des équipements et des technologies de qualité inférieure et, dans le cas des OI, elles peuvent également compenser des lacunes dans l'information ou une mauvaise information au sujet de l'ennemi.[39]

La doctrine chinoise a traditionnellement accordé une plus grande attention aux dimensions psychologiques de la GI, y compris la tromperie, même si, ces derniers temps, elle a également accordé une attention égale, sinon plus, aux dimensions technologiques.[40]

---

38 *Ibid*. p. 72.
39 *Ibid*. p. 73.
40 Timothy L, Thomas, *Comparing US, Russian and Chinese Information Operation Concepts*, (Fort Leavenworth, Foreign Military Studies Office, 2004), p. 15.

La cible des opérations psychologiques est toujours les gens et les décideurs, de sorte que leur volonté et leurs perceptions sont attaquées pour modifier leurs croyances, leurs buts et leur comportement. Elles s'adressent aux composantes militaires et civiles de la population adverse. Les opérations psychologiques comprennent la manipulation des médias pour soutenir les efforts militaires ainsi que des méthodes conventionnelles de propagande et d'autres moyens de communication. Comme la plupart des composantes de la GI, les opérations psychologiques sont un continuum d'actions en temps de paix et en temps de guerre.[41]

La Chine considère la guerre intégrée comme un domaine dans lequel des stratégies asymétriques peuvent être utilisées pour affronter ses rivaux, en particulier ceux qui disposent de meilleures capacités technologiques. Elle a appliqué le concept de la guerre du peuple dans le contexte de la GI afin de tirer parti de la disponibilité d'un grand nombre d'experts civils en TI.

La GI est importante à l'échelle nationale, aux niveaux stratégique et opérationnel. Au niveau national, l'objectif est de modifier les perceptions de l'adversaire afin que la victoire puisse être obtenue sans combat ou au moindre coût. Partout dans le monde, les militaires reconnaissent la GI comme un multiplicateur de force et un outil clé pour remporter la bataille.[42] Le spectre électromagnétique, un élément clé du domaine de l'information, est devenu le nouveau haut lieu à saisir pour le succès des opérations, mettant ainsi en évidence les aspects opérationnels de la GI. La montée en puissance militaire de la Chine a suscité des inquiétudes non seulement pour les États-Unis, mais aussi pour le Canada.

---

41 *Ibid*. p. 3.
42 *Ibid*. p. 7.

L'approche de plus en plus affirmée de Pékin face au contrôle de l'information, en Chine comme à l'étranger, pourrait bien fonctionner pour l'administration Xi Jinping. À long terme, il pourrait être en mesure d'utiliser son offensive d'information pour façonner des récits dans les médias mondiaux sur la Chine et les politiques de la Chine. Avec la croissance de l'économie chinoise, la Chine pourrait également être mieux placée pour établir les règles et les normes pour l'Internet dans le monde entier.[43]

Toutefois, la stratégie pourrait également avoir un effet inverse. En dépit de l'énorme marché de consommation de la Chine pour toutes sortes de services Internet, la patience des entreprises étrangères avec la censure de Pékin et les tentatives d'incliner les règles du jeu pour les entreprises chinoises, pourrait éventuellement avoir un impact négatif. Les restrictions imposées aux investisseurs étrangers et la demande de transfert de propriété intellectuelle à des partenaires chinois ont fait hésiter de nombreuses start-ups informatiques de pointe, en Europe et en Amérique du Nord, à tenter de s'étendre sur le marché du géant asiatique. Bien que Facebook et Apple n'aient pas encore abandonné, d'autres grandes entreprises de technologie l'ont fait.

De plus, certaines grandes entreprises de technologie chinoises se sont acharnées contre les restrictions, se plaignant qu'elles étouffent l'innovation et rendent difficile l'attraction des meilleurs talents. Elles se plaignent également du fait que la Chine change souvent, et sans avertissement, ses règles sur Internet. Même les entreprises chinoises ont de la difficulté à s'adapter.

Pendant ce temps, d'autres pays pourraient riposter si la Chine étend sa GI et si le pays s'ingère de plus en plus dans la politique et les sociétés d'autres nations. Déjà, les États-Unis et d'autres pays repoussent l'offensive d'information et le jeu d'influence de la

---

[43] Pillsbury, Michael, *Chinese Views of Future Warfare*, (National Defense University, 2000), p. 412.

Chine. L'administration Trump accroît sa pression commerciale et lance des enquêtes sur les violations de la propriété intellectuelle. Certaines nations, comme l'Australie, ont réagi aux reportages des médias sur l'influence chinoise en adoptant de nouvelles lois sur les dons étrangers et en renforçant la surveillance gouvernementale des investissements chinois dans les projets d'infrastructure nationaux.

En fin de compte, la GI de la Chine pourrait conduire à un tel retour en arrière que Pékin pourrait avoir à repenser sa stratégie globale de l'information.

LES FORCES ARMÉES CANADIENNES

Les commandants intelligents ont naturellement toujours intégré les OI. Notre tâche consiste maintenant à veiller à ce que tous les commandants, les états-majors et les soldats pensent et agissent de manière à exercer une domination sur l'information.

Premièrement, bien qu'il existe une doctrine pour les OI, il faut insister davantage sur ce point. Les commandants doivent comprendre que, à moins d'établir clairement leurs besoins en matière d'information, en se fondant sur l'état final de la bataille tel qu'ils l'envisagent, ils ne pourront jamais tirer pleinement parti des OI. Deuxièmement, les états-majors et les commandants doivent commencer à voir le champ de bataille en termes de décisions amicales et ennemies. Les FAC doivent planifier des opérations pour répondre aux besoins et aux exigences de ces décisions, tout comme elles prévoient détruire et protéger la puissance de combat.

Doctrine

En termes généraux, les problèmes rencontrés par de nombreux professionnels des FAC est de comprendre que les OI peuvent être résolu en limitant le problème en termes de dominance de l'information. Cet état final indique clairement à tous où les FAC se situent actuellement avec le concept des OI et fournit une orientation en donnant aux planificateurs et

aux commandants un objectif à atteindre. À l'avenir, la doctrine des OI doit faire partie intégrante de la façon dont les opérations militaires sont envisagées. Cependant, une doctrine distincte, incluant les tactiques, les techniques et les procédures, devrait être mise en place pour montrer aux états-majors comment intégrer la partie la plus agressive des OI dans leurs plans de bataille. La doctrine actuelle des OI des FAC est la doctrine conjointe des FAC, B-GG-005-004/AF-010 Opérations d'Information, publiée le 15 avril 1998.[44] Au cours des vingt dernières années, la TI ainsi que la manière de communiquer ont grandement évolué. La Doctrine interarmées des FAC, B-GJ-005-313/FP-001 Opérations Psychologiques, est une autre référence à mettre à jour car elle a été publiée le 15 janvier 2004.[45]

La doctrine de l'armée canadienne, B-GL-300-001/FP-001 Opérations Terrestres, publiée le 1er janvier 2008, contient une section consacrée à l'utilisation des OI dans les opérations terrestres. Plus particulièrement, même si les OI sur la doctrine interarmées des FAC ne mentionnent pas les opérations cyber, les opérations terrestres mentionnent que les CNO font partie intégrante des OI.[46]

Le 3 avril 2018, le chef d'état-major de la défense (CEMD) a publié la politique sur les opérations d'information conjointes du MND et des FAC. Le CEMD précise que les adversaires utilisent l'environnement de l'information pour créer la désinformation et la propagande, de sorte que ces adversaires puissent atteindre leurs buts et objectifs au détriment du Canada et de ses

---

[44] Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04.

[45] Canada. Department of National Defence. B-GJ-005-313/FP-001, CFJP 03.10.1 – Psychological Operations. Ottawa, ON: Chief of the Defence Staff, 2004-01.

[46] Canada. Department of National Defence. B-GL-300-001/FP-001, Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-01, p. 5-50.

alliés.[47] Cette politique permet aux FAC de contribuer à la défense du Canada tout en contribuant à l'effort gouvernemental visant à développer et améliorer la capacité OI.

Organisation

Les FAC ont un besoin important d'un leader stratégique, dont le focus serait la dominance de l'information ainsi que la planification et l'exécution des OI. La planification et l'exécution des OI est une entreprise multifonctionnelle dans laquelle de nombreux acteurs jouent un rôle. Chaque fonction sur le champ de bataille aura des exigences en matière d'information, et celles-ci seront satisfaites par les états-majors et les opérateurs du renseignement, et transmises au moyen d'un système d'information planifié par les communicateurs. Pour la plupart, ces aspects du processus de planification des OI font déjà partie intégrante du processus de planification des opérations. Dans les faits, la planification doit s'inscrire dans le contexte du processus de planification opérationnelle (PPO) de manière beaucoup plus intégrée et délibérée.

Changement culturel

Les officiers et les sous-officiers des FAC doivent pouvoir s'adapter et adopter le changement culturel auquel les FAC sont exposées. Les leaders stratégiques, les commandants de formation, de division et de brigade, doivent apprendre à visualiser l'espace de bataille de l'information, à clarifier les besoins en information et à établir des objectifs reliés à l'information. De plus, ils doivent avoir une compréhension de base des outils à leur disposition qu'ils peuvent utiliser pour les aider à accomplir leur mission, et des exigences qu'ils peuvent et doivent placer sur le système d'information qui soutient leurs unités.

---

[47] Canada. Department of National Defence. Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations. Ottawa, ON: Chief of the Defence Staff, 2018-04, p. 41.

Les futurs dirigeants doivent être formés. En établissant un programme de formation qui enseigne la doctrine et les concepts des OI à tous les officiers et sous-officiers, les FAC peuvent favoriser le changement culturel et permettre aux états-majors actuels et aux futurs commandants d'utiliser pleinement les OI.

Formation professionnelle spécifique

Les exigences des OI ne sont pas seulement liées à un changement culturel. Certaines compétences sont requises pour l'exécution. La formation axée sur des compétences particulières a été discutée dans deux domaines: la planification des OI en termes de processus, du personnel, des méthodologies et de la technologie de soutien ainsi que de la modélisation de la décision, qui inclue l'étude du processus décisionnel et des technologies de l'adversaire.

CONCLUSION

L'importance des OI a augmenté dans la guerre moderne en raison des progrès technologiques. Les adversaires potentiels du Canada ont créé un vaste fossé en matière de capacités et de connaissances que le Canada doit maintenant combler. Lors de récents conflits, la Russie s'est montrée habile à utiliser la désinformation et la désinformation, ainsi qu'à combiner les aspects techniques et psychologiques des opérations d'information, pour faire avancer leurs objectifs politiques.

La doctrine russe de la tromperie militaire a évolué avec le temps, elle est devenue une complexité de mesures visant à induire l'ennemi en erreur quant à la présence et à la disposition des forces russes, et comprend des moyens stratégiques, politiques et diplomatiques. Elle est basée sur manipulation des faits et de la perception des médias et de l'opinion publique dans le but d'atteindre des objectifs tactiques, stratégiques, nationaux et internationaux. Les OI russes constituent un système complexe d'activités financières, politiques, économiques et d'espionnage

en dans le but d'influencer les décisions politiques et économiques d'une manière jugée favorable à la Russie.

Le gouvernement russe poursuit activement l'imposition d'une relation dépendante aux États baltes, avec le désir de rester l'acteur dominant et l'arbitre politique de la région, en poursuivant le modèle soviétique de relations hégémoniques avec ces petits États voisins. L'utilisation des instruments et techniques de politique douce tels que le soutien à certains médias indépendants et acteurs de la société civile font partie intégrante de la stratégie. La Russie, étant militairement plus faible que l'OTAN, et économiquement et technologiquement moins développée que les États-Unis et l'UE, doit donc recourir à la GI.

Les OI et la GI en Chine sont basées sur des concepts et des termes similaires à ceux utilisés par les États-Unis, mais les chinois les ont développés pour qu'ils soient plus appropriés et pertinents à la culture chinoise et à la doctrine communiste. Alors que la RPC a adopté l'idée de dominance de l'information, sa méthode pour aller sur la dominance de l'information diffère, en utilisant des méthodes anciennes.

L'intérêt sérieux de la Chine pour les OI et la GI depuis les deux dernières décennies et le succès résultant des TI et de la domination totale dans l'espace de bataille, démontrent le potentiel futur significatif de la RPC. L'idée d'une révolution dans le domaine de l'information a surgi comme une école de pensée dans la guerre chinoise. Les dirigeants de la Chine insistent constamment sur l'utilisation de techniques asymétriques pour contrer les nations plus puissantes, comme les États-Unis.

Les FAC doivent adapter leur doctrine et leurs capacités en matière d'OI pour opérer efficacement dans le contexte opérationnel changeant d'aujourd'hui, afin de protéger

efficacement les intérêts du Canada au pays et à l'étranger.[48] Les opérations cyber et les médias sociaux devraient devenir des aspects importants de la doctrine des OI et des FAC.

Les FAC doivent également être prêtes à aider et à collaborer avec d'autres ministères gouvernementaux dans le but de protéger le Canada.[49] À moins que le Canada ne réduise l'écart en matière de capacités avec ses adversaires potentiels, il demeurera vulnérable en raison du manque de dissuasion efficace.

---

48 *Ibid*. p. 34.
49 *Ibid*. p. 1.

BIBLIOGRAPHIE

Astorino-Courtois, Allison. *A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap.* National Security Innovations (2017).

Armistead, Leigh, United States. National Security Agency/Central Security Service, and Joint Forces Staff College (U.S.). *Information Operations: Warfare and the Hard Reality of Soft Power*. 1st ed. Washington, D.C: Brassey's, 2004.

Arquilla, John and David Ronfeldt. *Cyberwar is Coming*. In . 1st ed., 23: RAND Corporation, 1997.

Black, Jeremy. *War and Technology*. Bloomington and Indianapolis: Indiana University Press, 2013.

Bouchet, Nicolas. *Russia's "Militarization" of Colour Revolutions.* CSS Policy Perspective 4, no. 2 (2016).

Brands, Hal. *Paradoxes of the Gray Zone*: Foreign Policy Research Institute, 2016.

Canada. Department of National Defence. B-GG-005-004/AF-010, CFJP 03.10 – Information Operations. Ottawa, ON: Chief of the Defence Staff, 1998-04.

Canada. Department of National Defence. B-GJ-005-313/FP-001, CFJP 03.10.1 – Psychological Operations. Ottawa, ON: Chief of the Defence Staff, 2004-01.

Canada. Department of National Defence. B-GL-300-001/FP-001, Land Operations. Ottawa, ON: Chief of the Defence Staff, 2008-01.

Canada. Department of National Defence. Department of National Defence and Canadian Armed Forces Policy on Joint Information Operations. Ottawa, ON: Chief of the Defence Staff, 2018-04.

Canada. Department of National Defence. Terminology Standardization Board. DND/CF Manual of Abbreviations: AAP-15.

Ehrhart, Hans-Georg. "Postmodern Warfare and the Blurred Boundaries between War and Peace." *Defense & Security Analysis* 33, no. 3 (2017).

Pillsbury, Michael and National Defense University. Institute for National Strategic Studies. *Chinese Views of Future Warfare*. Washington, DC: National Defense University, Institute for National Strategic Studies, 2000.

Rutenberg, Jim. *RT, Sputnik and Russia's New Theory of War*. New York: New York Times Company, 2017.

Schmitt, Michael N. "The Law of Cyber Targeting." *Naval War College Review* 68, no. 2 (2015).

Thomas, Timothy L. "China's Electronic Strategies." *Military Review* 81, no. 3 (2001).

Thomas, Timothy L. "Comparing US, Russian and Chinese Information Operation Concepts" Fort Leavenworth, KS: Foreign Military Studies Office, (2004).

Thomas, Timothy L. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations" *Defence Strategic Communications 1,* no. 4 (2015).

Thomas, Timothy L. "The Evolving Nature of Russia's Way of War." *Military Review* 97, no. 4 (2017).

Thomas, Timothy L. "Thinking like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War." Fort Leavenworth, KS: Foreign Military Studies Office, (2017).

United States. Defense Intelligence Agency. *Russia Military Power: Building a Military to Support Great Power Aspirations*. Washington, D.C: Defense Intelligence Agency, 2017.

United States. Department of the Army. *Inform and Influence Activities*. Washington, DC: Headquarters, Department of the Army, 2013.

United States. Department of the Army. *Information Operations*. Washington, DC: Headquarters, Department of the Army, 1996.

United States. Joint Chiefs of Staff. *Cyberspace and Electronic Warfare Operations*. Vol. 3-12. Washington, D.C: The Joint Chiefs of Staff, 2017.

United States. Joint Chiefs of Staff. *Joint Doctrine for Command and Control Warfare (C2W)*. Vol. 3-13.1. Washington, D.C: The Joint Chiefs of Staff, 1996.

United States. Joint Chiefs of Staff. *Information Operations*. Vol. 3-13. Washington, D.C: The Joint Chiefs of Staff, 2014.

United States. Department of Defense (DoD). *Strategy for Operations in the Information Environment*. Washington, D.C: Department of Defense, 2016.