National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# LE PROCESSUS DE CIBLAGE, UN LEVER DE VOILE VERS UN AVENIR CYBERNÉTIQUE AUTOMATISÉ

**Major Mathieu Deshaies**

## JCSP 49

## 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.

© His Majesty the King in Right of Canada, as represented by the Minister of National Defence, 2023.

## PCEMI n° 49

## 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.

© Sa Majesté le Roi du chef du Canada, représenté par le ministre de la Défense nationale, 2023.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 - PCEMI n° 49
2022 - 2023

Exercise Solo Flight – Exercice Solo Flight

# LE PROCESSUS DE CIBLAGE, UN LEVER DE VOILE VERS UN AVENIR CYBERNÉTIQUE AUTOMATISÉ

**Major Mathieu Deshaies**

*"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."*

*« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de difuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »*

# LE PROCESSUS DE CIBLAGE, UN LEVER DE VOILE VERS UN AVENIR CYBERNÉTIQUE AUTOMATISÉ

## Introduction

Le ciblage militaire est une pratique qui a évolué dans les derniers siècles. La simple application de la force brute évolua au fil des avancées technologiques en des techniques plus précises et sophistiquées de prise de décision basée sur les renseignements qui bénéficie soudainement de la surveillance aérienne, des satellites et de la reconnaissance électronique. Au cours des guerres modernes, le ciblage est devenu un processus très complexe impliquant une analyse minutieuse des données de renseignement, de l'information de terrain et des capacités d'armement disponibles pour déterminer la meilleure stratégie de frappe. La précision et l'efficacité du ciblage sont essentielles pour minimiser les pertes civiles et maximiser les dommages infligés à l'ennemi.[1] Il en dans l'intérêt singulier de n'importe quel acteur ou état de savoir comment tirer son épingle du jeu avec le ciblage et saisir ou maintenir l'avantage sur la scène internationale. L'inaction ou l'inefficacité dans le domaine du ciblage entraîne inévitablement une perte en opportunités non saisie. Pour être efficace avec le ciblage, il faut enchaîner les cycles décisionnels le plus rapidement et il faut savoir comment agir le plus près possible de la ligne séparant la légitimité des actions et les actions condamnables sans toutefois traverser du côté de l'espace d'opérations des actions condamnables. Cependant, l'espace de manoeuvre qui est considéré légalement acceptable est jugé sur les principes de la dissuasion, car lorsqu'il vient le temps de mesurer la légitimité des actions posées, la capacité de dissuader est le facteur vital. Posséder la capacité d'imposer par la force sa perspective sur l'emploi des effets est un concept qui échappe partiellement au Canada. La dissuasion est un effet en soi et s'obtient en possédant suffisamment de capacités. Les alliances, l'économie, les chaînes industrielles nationales et la puissance militaire sont principalement ce qui permet de mesurer la capacité d'un état à dissuader. Ainsi, une marge de manœuvre existe dans la zone grise d'application des effets. La loi est faite et appliquée par les plus dissuasifs, et c'est encore plus évident au niveau de la scène internationale. Dans un monde où l'instabilité ne fait qu'augmenter constamment, il serait judicieux d'augmenter notre capacité canadienne de poser des effets légitimes et avantageux pour les alliances qui nous font tant bénéficier pour, au minimum, maintenir notre position dans ses alliances. Augmenter l'ampleur canadienne des effets posés, par le processus de ciblage et pour le bien de la communauté en réorganisant notre méthodologie nous permettant autant d'agir que de dissuader, maintiendra la pertinence et le bien-fondé canadien sur la scène internationale dans cette époque de lutte géopolitique globale pour le pouvoir. Le processus de ciblage est donc une clé pour les Forces armées canadiennes (FAC). En réorganisant sa structure et en raffinant le processus, les FAC pourraient augmenter leur pertinence sur la scène internationale en contribuant aux efforts de sécurité mondiale sans toutefois nécessiter de plus amples ressources. Ce papier s'intéressera à l'intégration pangouvernementale des opérations de renseignement, et de ciblage cybernétiques supporter par l'Intelligence Artificielle (IA) dans le processus de ciblage tout en considérant les fondements légaux.

[1] Paul A.L. Ducheine, Michael N. Schmitt & Frans P.B. Osinga 2016, Targeting: The Challenges of Modern Warfare, T.M.C. Asser Press, The Hagu

**Développement**

Para 1. Le lien entre le ciblage et la loi. Loi sur le droit des conflits armés et le fondement légal canadien.

Le processus de ciblage canadien est strictement militaire. Les principes légaux fondamentaux de notre monarchie constitutionnelle empêchent l'intégration d'une approche pangouvernementale du ciblage militaire. Il est primordial de comprendre qu'au Canada les décisions importantes sont prises par les élus et les gouvernements en place, et les citoyens ont également des droits constitutionnels tels que la liberté d'expression, la liberté de religion, la liberté de presse et la liberté d'association. Le Canada est également régi par un ensemble de lois et de règles qui régissent le fonctionnement de l'État et protègent les droits et les libertés des citoyens. Il existe également des institutions telles que le système judiciaire indépendant et la Charte canadienne des droits et libertés qui servent de garants de la démocratie canadienne. Comme tout pays, le Canada n'est pas parfait et il peut y avoir des défis et des controverses en matière de gouvernance et de protection des droits. Néanmoins, dans l'ensemble, le Canada est considéré comme un pays démocratique où les citoyens ont des droits et une voix dans le processus politique. Cette situation est forte avantageuse, car il n'est pas nécessairement souhaitable que les actions civiles deviennent dictées par des militaires. Cependant le ciblage canadien est très limité aux horizons militaires.

Le contexte légal canadien permet de comprendre la nature des différences entre le ciblage appliqué par le Canada et les États-Unis d'Amérique. En effet, le président américain est à la fois le chef de l'État et le chef du gouvernement. Le président américain dirige donc une certaine partie de l'exécutif et du législatif permettant une décentralisation du commandement et contrôle du ciblage tout en ouvrant les portes aux approches pangouvernementales. Le pouvoir gouvernemental canadien est centralisé sans être délégué et ne permet toutefois pas l'approche pangouvernementale du ciblage en raison du système bureaucratique gouvernemental qui est grotesquement départementalisé. Le principal allié du Canada applique donc un processus de ciblage pangouvernementale et est prêt à accepter du risque afin de soulever les opportunités tandis que le ciblage canadien se limite aux opérations militaires, et ce sans accepter de risque au niveau du respect de la vie, de la dignité humaine et des lois applicables.

**Le droit des conflits armés et le concept de légitimité.**

La légitimité du droit des conflits armés découle des documents écrits de la convention de Genève.[2] L'article 1 et l'article 2 de la convention de Genève de 1949 incluent la définition d'un objectif militaire. Cette définition fut ajoutée en 1977 par le biais de documents supplémentaires dans le cadre du protocole additionnel. La définition inclut donc deux éléments clés qui doivent être satisfaits pour légalement préparer et appliquer des effets sur un objectif.[3] Le premier élément est que l'objectif doit contribuer aux actions militaires et le deuxième élément est que l'action sur l'objectif contribuera réellement aux efforts de guerre.[4]

Au tout début des hostilités en Afghanistan, le choix des objectifs était concentré vers des objectifs militaires du régime non démocratique taliban. Alors que les nations de l'ouest étaient de plus en plus impliquées au Moyen-Orient incluant l'Irak, l'application des effets sur des cibles évolua pour désormais s'appliquer sur des objectifs militaires d'opportunités. Très rapidement, l'effort de guerre fut réaligné pour principalement poursuivre ses objectifs militaires d'opportunités. Étant exécutées d'une manière plus expéditive et avec moins de précautions, les actions sur les objectifs militaires d'opportunités ont généré un plus haut taux de situation controversée et litigieuse.[5] L'implication soudaine des technologies de communication avec l'apparition des médias sociaux et la présence d'organisme non gouvernemental sur le terrain à révéler que la légitimité des effets portés envers des objectifs militaires n'est plus toujours aussi apparente et que l'interprétation contextuelle des effets portés dépend du point de vue.[6] De plus, les pressions provenant des militaires peuvent faire varier l'interprétation des deux éléments de la définition d'objectif militaire avant, pendant et après l'effet posé sur l'objectif.

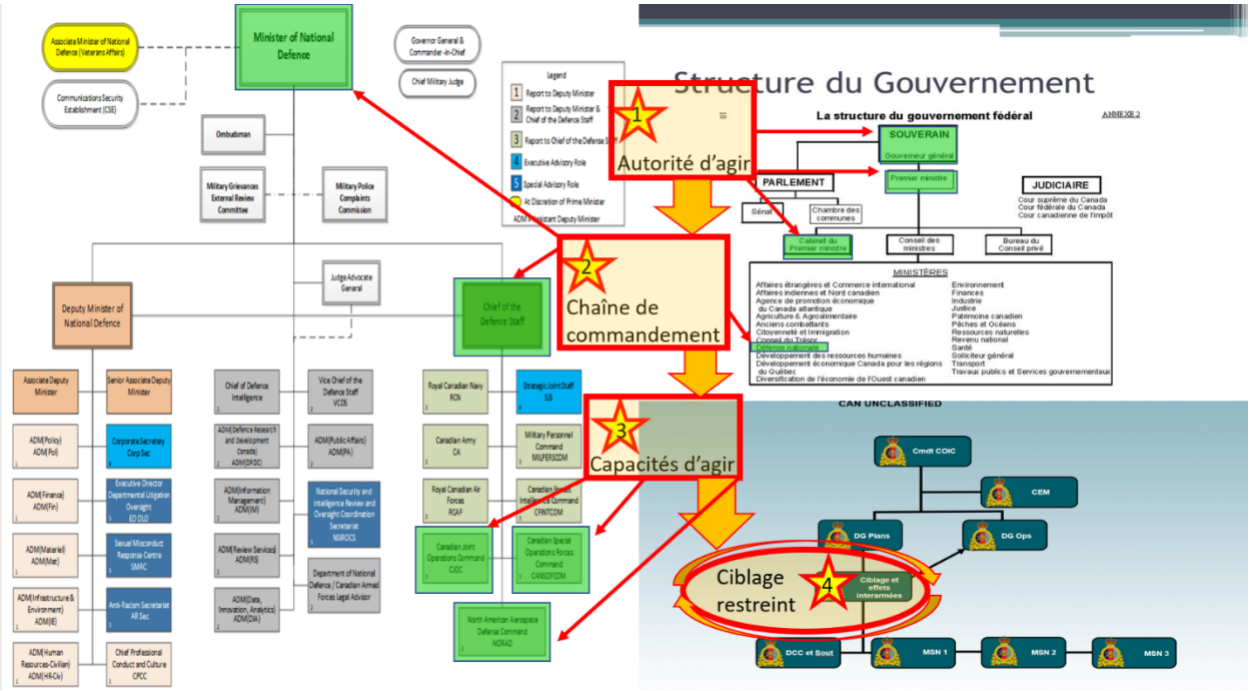
En somme, d'un point de vue légal, le ciblage est un système de système au travers duquel un cibleur s'en prend à un ciblé et après l'action, débattrons devant la scène internationale sur la légalité de l'action posée défendant leur point de vue et leur perception de la légalité face à l'action posée à savoir si l'action était légitime ou devrait être condamnée.[7] Lors du débat de sémantique sur la question entre-le cibleur et le ciblé, les secrets d'État sont toujours évoqués afin de ne pas mentionner le pourquoi de l'action sur l'objectif afin d'éviter de dévoiler trop amplement les intentions stratégiques profonde ou simplement par nécessité de niveau tactique.[8] Maîtriser le système de système qu'est le processus de ciblage permet aux États de flirter le plus proche possible de la ligne entre l'action légitime et la condamnation afin de maintenir le conflit dans la zone grise. La capacité de cibler plus efficacement offre l'avantage à ceux qui savent comment agir le plus près de la ligne vers la transgression d'une action condamnable sur un objectif sans jamais la traverser.

---

[2] Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.
[3] Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.
[4] Nations Unis Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I)
[5] Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.
[6] Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.
[7] Paul A.L. Ducheine, Michael N. Schmitt & Frans P.B. Osinga 2016, Targeting: The Challenges of Modern Warfare, T.M.C. Asser Press, The Hagu
[8]Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.

**Loi sur la défense nationale.**

La loi sur la défense nationale illustre bien les fondements politiques qui dirige le Canada depuis le cabinet incluant notre fonctionnement militaire, particulièrement dans la délégation légale de l'autorité d'agir selon les positions.




Le ministre de la Défense est responsable des FAC. Son rôle se limite au maintien des forces, à l'entretien des établissements et au perfectionnement du matériel.[9] Il est considéré comme un aviseur ou un conseiller. Le chef d'état-major des forces canadiennes assure la direction et la gestion administrative des FAC. Le simple titre de chef d'état-major en dit long sur l'emplacement de l'autorité légale d'agir et d'appliquer la force. Ce titre n'est pas un titre de commandant. Le commandant des FAC est théoriquement royal et est représenté par le gouverneur général. En principe, la monarchie constitutionnelle canadienne dicte au gouverneur général l'agenda à suivre, et ce par le biais du gouvernement canadien voir sous l'avis du conseil privé. En résumé, le ministre de la Défense nationale et le chef d'état-major de la défense sont des aviseurs et des administrateurs, mais ils ne commandent pas. C'est seulement lorsque des missions claires sont ordonnées depuis le conseil privé, par le biais du pouvoir honorifique du gouverneur général, incluant des limitations d'actions et des règles d'engagements que les FAC peuvent agir. Il est évident que ceci constitue en soi en une restriction majeure qui délimite le rayon d'action des FAC dans son processus de ciblage.

**La doctrine canadienne de ciblage et la politique canadienne de défense.**

Les actions étatiques militaires lors de conflits armés sont façonnées en partie par la doctrine militaire et en partie par le droit. La doctrine de ciblage canadienne offre plusieurs définitions importantes et comporte les règles à suivre aux commandants en place dans le cadre du

[9] Loi sur la défense nationale.

processus de ciblage. En fait la doctrine de ciblage canadien ne fait que réitérer la prudence canadienne en obligeant les commandants à s'assurer que les objectifs ciblés sont légitimes, a utilisé le moyen possédant le moins haut taux de chance de dommages collatéraux et de ne pas appliquer d'effet sur un objectif si les dommages collatéraux potentiels surpassaient hors de proportion l'avantage militaire attendu.[10] Présentement, la doctrine de ciblage canadienne est donc très limitative à l'interne des paramètres de mission donnée préalablement par le gouvernement incluant les règles d'engagement, car en résumé cette doctrine ne fait qu'encadrer d'obligations les commandants avec les définitions déjà mentionnées dans la loi sur le droit des conflits armés.

La politique canadienne de la défense Protection Sécurité Engagement (PSE) est prometteuse en ce qu'elle maintien toujours un contrôle afin de négliger le risque, tout en ouvrant la porte aux actions dans la zone grise de la légalité. En effet, PSE présente une nouvelle initiative qui est d'améliorer la capacité de ciblage des FAC supporté par une croissance de la force régulière de 3500 personnes, ce qui rendra possible une modernisation délibérée des capacités de ciblage et du renseignement en impliquant les possibilités offensives du cyberespace.[11] L'intention est de maintenir les capacités cybernétiques défensives toute en ajoutant un volet actif et en support aux missions militaires autorisées à l'extérieur des frontières canadiennes, et ce sous approbation du gouvernement.[12] Cette nouvelle capacité de ciblage cybernétique sera soumise aux mêmes limitations de nos lois nationales ainsi que d'estimation des dommages collatéraux.[13] PSE inclus aussi des investissements fortement susceptibles d'augmenter les effets dans l'aviation canadienne notamment avec le remplacement des CF-18 par 88 F-35, mais aussi avec l'annonce d'investissement dans les systèmes télépilotés non seulement pour acquérir de l'information, mais aussi pour conduire des frappes précises augmentant ainsi les possibilités pour le cycle de ciblage canadien.

Le Canada est donc très respectueux du droit des conflits armés et exerce un contrôle étouffant afin de s'assurer que les intentions du cabinet sont respectées au cours de chaque mission. Il est cependant évident de constater qu'il existe une zone grise sur les perspectives de légitimité des actions et que cette zone grise est exploitable. PSE ouvre la porte aux FAC d'agir un peu plus près de la ligne délimitant le légitime de l'illégitime, et ce dans la zone grise autant avec le cybernétique que les frappes furtives sans pilotes.

<u>Para 2. Le ciblage et la zone grise légale.</u> Les opportunités offertes par les opérations cybernétiques offensives.

Pour paraphraser Clausewitz, baser le ciblage sur les effets est la quintessence de la poursuite de la politique par d'autres moyens.[14] Le ciblage militaire moderne inclut désormais des cibles non tangibles telles que des logiciels. Certes les logiciels pris pour cible comportent toujours des éléments physiques, fonctionnels, cognitifs, temporels et environnementaux. Chacun de ces éléments présente une ou des vulnérabilités cybernétiques exploitables.[15] Les systèmes de

---

[10] Doctrine Canadienne de ciblage. Canada. Ministre de la défense nationale. PIFC 3-9, Ciblage. Ottawa: l'état-major interarmées stratégique, 2014
[11] Protection Sécurité Engagement, La politique de défense du Canada. 2017.
[12] Protection Sécurité Engagement, La politique de défense du Canada. 2017.
[13] Protection Sécurité Engagement, La politique de défense du Canada. 2017.
[14] Paul A.L. Ducheine, Michael N. Schmitt & Frans P.B. Osinga 2016, Targeting: The Challenges of Modern Warfare, T.M.C. Asser Press, The Hagu
[15] Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic.

technologie de l'information permettent l'atteinte d'objectif militaire par le biais d'action cybernétique.[16] En s'infiltrant rapidement dans le cycle de commandement et contrôle, il est possible de créer un ou des effets, parfois cybernétiques, pouvant faire bénéficier les commandants de mission vers l'atteinte de leurs objectifs militaires. L'espionnage, la neutralisation de système antiaérien ennemi et le sabotage ne sont que de simple exemple de ce qui est désormais beaucoup plus accessible. Les FAC sont donc devant l'opportunité. L'opportunité d'appliquer des effets. Les lois internationales s'appliquant aux cyberespaces sont présentement soumises à des dissensions sur la scène internationale. Certains s'entendent pour dire que le '*'Tallin Manual on the International Law Applicable to Cyber Warfare*'' (TM) est un guide à suivre, comme dans la majorité des démocraties libérales de l'Ouest.[17] D'autres préfèreraient l'établissement de document officiel plus clair, comme chez les régimes plus conservateurs de l'Est. D'ici la fin des dissensions, la zone grise légale sera toujours assujettie aux débats et spéculations. Cette zone grise existera dans le temps jusqu'à ce qu'un consensus ne soit atteint sur la scène internationale au sujet de la définition de cybercriminalité internationale et qu'une expérience suffisante vécue des deuxièmes et troisièmes ordres d'effets n'ait été expérimentée. Seulement lorsque ces conditions ne seront remplies que les définitions d'opérations cybernétiques offensives évolueront vers un consensus global légal et constituera en soit en la fin de la zone grise légale. Présentement, les opérations cybernétiques offensives consistent en ce qui pourrait provoquer des effets physiques de premier ordre tel que des morts, blessés et dommages matériels.[18] Les effets de deuxième et troisième ordre ne sont toujours pas pris en considération et les interprétations favorise généralement les états le plus puissants ou faisant partie d'un regroupement d'états puissants. Si une action cybernétique offensive est posée et ne présente aucun effet physique direct, les effets de deuxième et troisième ordre sont difficilement définissables. L'incompréhension militaire et surtout civile du monde cybernétique est quintuplée lorsqu'arrive le temps de discuter d'action militaire cybernétique offensive avec la population globale civile afin de définir une action cybernétique qui affecte négativement l'état. Les conséquences des effets cybernétiques posés dans le temps finiront par caractériser l'emplacement de la limite légale.

La cybersécurité est désormais un principe central de la posture de l'OTAN. Par le biais des opérations cybernétiques offensives, le processus de ciblage canadien exploitant la zone grise de la légalité cybernétique se définissant présentement comme action non létale, d'information, économique, des forces de l'ordre, de renseignement ou de tous autres moyens spéciaux de contraindre, présente une opportunité pour le Canada d'augmenter sa contribution en effort de guerre au sein de son alliance.

Para 3 Définition de la capacité cybernétique.

L'espace cybernétique contient des cibles nôtres, neutres ou ennemies. Les capacités de renseignement des transmissions de tous les acteurs autant privés qu'étatiques explorent en continu les failles sur la toile. Des failles qui ne sont seulement détectables qu'avec des organisations bien entraînées et éduquées. Il n'est donc question de capacité cybernétique que lorsqu'une faille est détectée et qu'il est décidé qu'un effet doit être posé afin d'intervenir

[16] Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic.
[17] Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict.
[18] Giampiero Giacomello. 2014. Security in Cyberspace : Targeting Nations, Infrastructures, Individuals. London: Bloomsbury Academic.

défensivement ou offensivement. Il m'apparaît opportun de souligner l'importance de la capacité à détecter de nos renseignements des transmissions et de la capacité de décider des objectifs par le biais du processus de ciblage.

Il existe des différentiations parmi les cibles cybernétiques. Les cibles cybernétiques peuvent être fondamentalement un État souverain ou une nation, des réseaux d'ordinateurs autant public que privé ou des individus seuls.[19] En supplément de leur fondement, les cibles cybernétiques consistent en l'aspect physique des ordinateurs et du filage, en programme informatique contrôlant l'information ou en l'information elle-même ainsi que ses définitions.[20] L'appréhension et la compréhension de ce type de cible cybernétique et des opportunités que ces cibles représentent sont tout autant nécessaires que récentes créant de l'incertitude. Créé une confiance institutionnelle en la capacité cybernétique afin d'enlever les incertitudes seraient un bon premier pas. Cette incertitude est justement due à la complexité même de la compréhension des capacités cybernétiques. L'éducation sur ce qu'est la capacité cybernétique devient importante autant nationalement qu'internationalement. Nationalement, afin de définir sa propre définition et doctrine des opérations cybernétiques, et, internationalement, pour participer aux discussions sur la légalité de l'emploi des effets cybernétique autant afin de se renseigner que de l'influencer. Cette participation aux efforts d'éducation et de conscientisation des opérations cybernétiques qui porte l'espoir d'établir la confiance est en soi une preuve qu'au fil du temps l'opportunité de ce type de cible est bel et bien éphémère.

Les opérations cybernétiques ouvrent donc la porte aux opportunités existantes de l'application des lois internationales et plus particulièrement en l'absence de consensus ou d'une gouvernance acceptée.[21] Une capacité cybernétique opérationnelle offre des opportunités qui conviennent parfaitement comme outil pour le ciblage stratégique. Mais les opportunités ne sont pas toujours si simples à décerner. Dans cet infini d'information, un support aux commandements et contrôle est nécessaire.

<u>Paragraphe 4 L'Intelligence Artificiel (IA) et le commandement et contrôle.</u> Automatisation et autonomie des systèmes de système.

La quantité de produits détectée à analyser des renseignements des transmissions devient en constante expansion et ne permet pas une couverture humaine complète.[22] Il est inconcevable de consommer et diriger toute cette information d'une manière efficiente. De plus, les opportunités d'action cachées parmi la masse d'information peuvent s'avérer très éphémères par nature d'où l'importance d'un commandement et le contrôle capable de comprendre l'ensemble de l'information et réagir adéquatement. Les réactions peuvent être défensives ou offensives.

Il existe une conception fausse au sujet de l'intelligence artificielle en ce que l'intelligence artificielle contiendrait elle-même le potentiel de devenir mal intentionné. Cette conception est fondamentalement erronée. Il n'y a pas de bénévolence ou de malévolence avec l'intelligence artificielle seulement des objectifs à atteindre. Si l'humanité se retrouve entre l'intelligence artificielle et son objectif, l'humanité, qu'il s'agisse de l'humanité dans son ensemble ou d'une

---

[19] Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic.
[20] Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic.
[21] Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic.
[22] Ekelhof, Merel A. C. "LIFTING THE FOG OF TARGETING: "Autonomous Weapons" and Human Control through the Lens of Military Targeting." Naval War College Review 71

partie de l'humanité, elle sera détruite. Des limites d'exploitation peuvent bien être implantées électroniquement afin d'empêcher que les décisions automatiques incluent des crimes contre l'humanité, mais l'humanité même se retrouverait retirée du processus décisionnel.

Les opérations de ciblage automatisé soulèvent, avec raison, des débats chauds. L'automatisation du ciblage dans un processus de ciblage simpliste ou une bombe est délivrée sur un objectif qui présente un risque qui est gérable de par sa nature cinétique simpliste. L'automatisation du ciblage dans un processus de ciblage moderne alors que les objectifs sont déjà des logiciels implique qu'une plus grande difficulté a intégré des limites d'exploitation qui maintiendraient la légitimité des effets. Le concept d'un système d'arme, qu'est le processus de ciblage, qui se déshumanise en s'automatisant, impose un dilemme éthique.[23] Présentement, aucun consensus n'existe afin de déterminer le niveau de jugement humain et la méthodologie technique appropriée a intégré au sein du processus de ciblage afin de respecter l'éthique militaire et les DDCA.[24] L'autonomie décisionnelle devient donc une capacité possible d'acquérir afin de prioriser les actions des acteurs. Cette autonomie devra simultanément ne jamais surpasser les acteurs humains tout en libérant, lesdits acteurs humains, d'une certaine lourdeur informationnelle leur laissant plus d'espace pour prioriser leurs responsabilités.

Il est facile d'imaginer le Canada devenir la pointe de la lance dans le domaine du processus de ciblage automatiser afin d'augmenter son support à l'OTAN. Ce type de modernisation d'automatisation du système devrait se faire en temps de paix, car les réglementations auto-imposées sont plus lourdes qu'en temps de guerre. Effectuer la bascule vers le ciblage autonome en temps de guerre implique un risque beaucoup plus grand qu'en temps de paix. Les règlementations auto-imposées se voient rapidement mises de côté sous prétexte que le contrôle humain équivaut une perte d'efficacité en opportunité d'objectif non poursuivi. Ceci peut potentiellement se traduire en une perte du contrôle humain sur des étapes décisionnelles critiques du processus de ciblage. Pour que les acteurs humains conservent un certain contrôle des décisions critiques du processus de ciblage, un cadre décisionnel dans lequel le contrôle humain ne peut être contourné doit être instauré afin de permettre une juste balance entre rapidité des décisions automatisées et légitimité des effets posés.

Selon les notes de doctrines interarmées sur le commandement et contrôle des opérations interarmées, les forces armées canadiennes possèdent six principes de commandement.[25] L'unité de commandement qui implique que le but, l'intention, les objectifs, les effets et l'état finals soient tous cohérents et harmonieusement synchronisés.[26] La portée du commandement qui implique que les commandants reçoivent des capacités adéquates pour les tâches confiées et vice versa.[27] La chaîne de commandement qui limite clairement la structure hiérarchique décisionnelle.[28] La délégation des pouvoirs qui implique que les commandants sont suffisamment habiliter capable de délégué adéquatement leur propre pouvoir.[29] La liberté

---

[23] Ekelhof, Merel A. C. "LIFTING THE FOG OF TARGETING: "Autonomous Weapons" and Human Control through the Lens of Military Targeting." Naval War College Review 71

[24] Ekelhof, Merel A. C. "LIFTING THE FOG OF TARGETING: "Autonomous Weapons" and Human Control through the Lens of Military Targeting." Naval War College Review 71

[25] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[26] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[27] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[28] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[29] NDI 02-2014 Commandement et contrôle des opérations interarmées.

d'action qui confère suffisamment d'espace décisionnel pour que les commandants soient efficaces et efficients dans la réussite de leur mission.[30] Pour finir, la continuité du commandement en ce que les projets entrepris doivent être exploitée au travers du temps et des niveaux de commandement stratégique, opérationnel et tactique.[31]

C'est au sein des trois premiers principes de commandement, soit; l'unité de commandement, la portée du commandement et la chaîne de commandement qu'une opportunité d'introduire une structure décisionnelle restrictive existe afin de permettre un minimum de contrôle humain sur les décisions automatisées. Ceci permettrait de maintenir les mesures adéquates sur les missions dans leur ensemble, les capacités délégués pour accomplir la mission et d'identifier adéquatement les niveaux de commandements. Les autres principes devraient se voir complètement automatisés afin de maximiser cette liberté décisionnelle et obtenir la fluidité et la rapidité d'action tant recherchées.

En introduisant la technologie utilisant l'algorithme, l'intelligence artificielle va venir augmenter la capacité humaine de surveiller, prédire, cibler et répondre adéquatement aux actions de nos adversaires.[32] Cette automatisation du ciblage ouvre la porte à des cibles dans l'ensemble du spectre de nos opérations. Les renseignements et les opérations deviendront synchronisés et les opérations seraient mieux gérées. Des tâches logistiques répétitives seront prédites et planifiées automatiquement d'avance en libérant beaucoup de personnel qui pourront s'attaquer à d'autres priorités. Des décisions, plus rapide et mieux ficeler, guider par le renseignement et basé sur de l'information automatiquement trouvée et trié seront plus souvent posés.

Paragraphe 5 Discussion

Les FAC présentent l'opportunité par le biais du ciblage cybernétique automatisé d'augmenter la pertinence et le bien-fondé canadien sur la scène internationale et le tout sans publiquement entacher sa réputation. Les avenues potentielles que le Canada et les FAC peuvent emprunter afin d'accomplir un tel rehaussement du niveau de la qualité et de la rentabilité des opportunités saisies des opérations de ciblage cybernétiques son multiple et jumelable. Concrètement, sur le plan national, le Canada peut investir dans la technologie de pointe au service des opérations nationales. Plateformes aériennes et cybersécurité augmenter afin de maintenir un contrôle cybernétique territorial Canadien. Ceci viendrait au coût d'une augmentation des dépenses en défenses qui est déjà présentement prévue dans PSE. Sur le plan international, croître la participation canadienne aux opérations cybernétiques internationales permettrait au Canada d'obtenir de l'expertise, car l'univers cybernétique est un univers qui se développe en le pratiquant opérationnellement.

Avec notre présent format gouvernemental, un brouillard de guerre existe entre le Premier Ministre (PM) et le Chef d'État-Major de la Défense (CEMD) en matière de ciblage. Le CEMD ne peut saisir l'intention en raison de sa nature civile et le PM ne comprend pas les capacités, le risque et les options dont il dispose, même s'il est très bien conseillé. De plus, le CEMD doit également composer avec la nature élective de l'autorité civile du PM. Le conseil privé du PM

---

[30] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[31] NDI 02-2014 Commandement et contrôle des opérations interarmées.

[32] THE DEPARTMENT OF NATIONAL DEFENCE AND CANADIAN ARMED FORCES ARTIFICIAL INTELLIGENCE STRATEGY.

peut conduire à un engagement militaire qui risque d'être rapatrié avant d'avoir potentiellement porté ses fruits en raison de la nature démocratique de la gouvernance qui peut s'avérer une entreprise fort couteuse. Il est plus avantageux pour le CEMD dans plusieurs cas d'aviser d'agir sans être engagé définitivement ou jusqu'à un point non désirable.

Actuellement, la chine et la Russie agissent toutes deux dans une zone grise où le gouvernement et la défense est assujettie aux tentatives de mettre à profit des failles dans notre système, comme l'environnement cybernétique. Des adversaires profitent des failles de nos systèmes pour agir. Une articulation automatisée de nos intérêts nationaux s'exprimant harmonieusement par le biais du ciblage cybernétique gouverner par un commandement des renseignements au sein d'une agence pan gouvernemental permettra non seulement en une défense constante, mais aussi en un puissant moyen de dissuasion. Les temps turbulents nous mènent aujourd'hui plus que jamais vers le conflit et la bascule du pouvoir décisionnel devra tanguer du côté militaire jusqu'à un certain degré prochainement si nous voulons survivre aux compétitions des grandes puissances. Il ne faut pas attendre qu'une catastrophe se produise pour positionner avantageusement les FAC dans un effort de transformation vers une approche militaire du ciblage automatisé dirigée par le renseignement et vers une stratégie de défense plus pangouvernementale.

Paragraphe 6 Plan d'action

L'histoire politique nous démontre qu'une catastrophe doit arriver pour justifier le changement. Il existe des options afin de parvenir a instauré une stratégie de défense autonome et pangouvernementale guider par une agence de renseignement opérationnelle et en constant processus de ciblage cybernétique. Les options favorisées se concentreraient autour de trois lignes d'efforts, soit l'éducation, l'acquisition de technologie et la collaboration.

L'éducation incluant, la sensibilisation et la formation sont essentielles pour améliorer la capacité de la main-d'œuvre à faire face aux menaces cybernétiques et être consciencieux du processus de ciblage et de l'impact de l'IA sur l'environnement opérationnel. L'acquisition des technologies de pointe est essentielle pour détecter, prévenir et répondre aux attaques et cyberattaques. Cela inclut des systèmes de logiciel de détection des menaces en temps réel et d'intelligence artificielle pour l'autonomisation. La collaboration avec des partenaires pour partager des renseignements sur les menaces, les vulnérabilités et les meilleures pratiques en matière de cybersécurité et renforcer la sécurité des réseaux nationaux. Le dernier ingrédient incertain serait l'aspect pangouvernemental qui ne peut présentement être atteint qu'avec une bonne relation entre le CEMD et l'adjoint du ministre.

## Conclusion

Aujourd'hui, le ciblage représente harmonieusement le pont entre les fins et les moyens de la guerre.[33] La prochaine étape est que le ciblage canadien doit évoluer pour servir de mécanisme de coordination et d'aide à la décision synchronisant l'application des mesures militaires et non militaires ce qui signifie produire à la fois des effets physiques et non physiques. La doctrine de ciblage au Canada est très limitée aux opérations militaires, ce qui restreint les actions sur les objectifs et la contribution à l'effort de guerre. De plus, l'approche pangouvernementale est pratiquement inexistante. Les commandants de mission sont encadrés d'obligations par les règles d'engagement et les définitions déjà mentionnées dans la loi sur le droit des conflits armés, ce qui restreint considérablement la maîtrise du système de ciblage canadien aux limites d'exploitation imposées aux missions. Cependant, cette approche respectueuse des lois internationales et du droit des conflits armés permet de maintenir le conflit dans une zone grise, tout en évitant les actions illégitimes. Actuellement, les opérations cybernétiques offensives ne prennent pas en compte les effets de deuxième et troisième ordre, ce qui avantage généralement les états les plus puissants. Il n'existe pas de consensus sur la légitimité des actions cybernétique et ni sur le niveau de jugement humain et la méthodologie technique appropriée à intégrer au sein du processus de ciblage afin de respecter l'éthique militaire et les DDCA. Par conséquent, l'autonomie décisionnelle du ciblage cybernétique devient une capacité possible à acquérir afin de prioriser les actions des acteurs. Pour les FAC, la capacité à digérer l'information et à appliquer rapidement l'effet ouvre de grandes possibilités. L'autonomisation du ciblage doit être intégrée dans les FAC et encadrée sur les trois premiers principes de commandement : l'unité de commandement, la chaîne de commandement et la portée de commandement. En réorganisant sa méthodologie de ciblage, le Canada peut augmenter l'ampleur de ses effets en agissant et en dissuadant. Cela permettra de maintenir la pertinence et le bien-fondé canadien sur la scène internationale dans cette époque de lutte géopolitique globale pour le pouvoir.

[33] Paul A.L. Ducheine, Michael N. Schmitt & Frans P.B. Osinga 2016, Targeting: The Challenges of Modern Warfare, T.M.C. Asser Press, The Hagu

**Bibliographie**


Paul A.L. Ducheine, Michael N. Schmitt & Frans P.B. Osinga 2016, Targeting: The Challenges of Modern Warfare, T.M.C. Asser Press, The Hagu, viewed 26 February 2023, https://www.proquest.com/docview/2135836609/6AF9A10B755B42E6PQ/1

Giampiero Giacomello. 2014. *Security in Cyberspace : Targeting Nations, Infrastructures, Individuals*. London: Bloomsbury Academic. https://journals.sagepub.com/doi/abs/10.1177/0267323115600603a?journalCode=ejca

Agnieszka Jachec-Neale. 2014. The Concept of Military Objectives in International Law and Targeting Practice. Routledge Research in the Law of Armed Conflict. Hoboken: Routledge. https://www.routledge.com/The-Concept-of-Military-Objectives-in-International-Law-and-Targeting-Practice/Jachec-Neale/p/book/9781138242708

Ekelhof, Merel A. C. "LIFTING THE FOG OF TARGETING: "Autonomous Weapons" and Human Control through the Lens of Military Targeting." Naval War College Review 71, no. 3 (Summer, 2018): 61-94. https://digital-commons.usnwc.edu/nwc-review/vol71/iss3/6/

NDI 02-2014 Commandement et contrôle des opérations interarmées. https://mars.cfc.forces.gc.ca/CFCLearn/mod/folder/view.php?id=15919

Protection Sécurité Engagement, La politique de défense du Canada. 2017. https://www.canada.ca/fr/ministere-defense-nationale/organisation/rapports-publications/politique-defense-canada/nouvelle-approche-defense.html#6.2

The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy. No.: D2-633/2022E-PDF (Electronic PDF) ISBN: 978-0-660-45122-0

Leveraging Artificial Intelligence for Canada's Army: Current Possibilities and Future ChallengesMay 2, 2022 - Major Geoffrey Priems and Peter Gizewski https://www.canada.ca/en/army/services/line-sight/articles/2022/05/leveraging-artificial-intelligence-for-canadas-army.html

Andrew S. Erickson, and Ryan D. Martinson. 2019. China’s Maritime Gray Zone Operations. Studies in Chinese Maritime Development. Annapolis, Maryland: Naval Institute Press. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8072&context=nwc-review

- Nations Unis Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) https://www.ohchr.org/fr/instruments-mechanisms/instruments/protocol-additional-geneva-conventions-12-august-1949-and

Loi sur la défense nationale. https://laws-lois.justice.gc.ca/PDF/N-5.pdf

Doctrine Canadienne de ciblage. Canada. Ministre de la défense nationale. PIFC 3-9, Ciblage. Ottawa: l'état-major interarmées stratégique, 2014 https://mars.cfc.forces.gc.ca/CFCLearn/mod/folder/view.php?id=7150

NATO. AJP-3.9, Allied Joint Doctrine for Joint Targeting. Brussels: NATO Standardization Office, April 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1033306/AJP-3.9_EDB_V1_E.pdf