National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

LE CYBERESPACE ET LES FORCES ARMÉES CANADIENNES

LCol J.M.F. Robichaud

JCSP 40

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 40

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 40 – PCEMI 40

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

LE CYBERESPACE ET LES FORCES ARMÉES CANADIENNES

LCol J.M.F. Robichaud

Word Count: 3864

Compte de mots: 3864

LE CYBERESPACE ET LES FORCES ARMÉES CANADIENNES

« The next war will begin in cyberspace. »

Lieutenant-Général K.B. Alexander, USCYBERCOM[1]

Au cours des dernières décennies, les technologies de l'information ont subit une croissance exponentielle. L'apparition d'Internet à la fin du dernier siècle a révolutionné le monde des communications et depuis, son étendu et notre dépendance envers ces systèmes ne cesse d'augmenter. Que ce soit dans les activités commerciales, financières, industrielles, militaires ou gouvernementales, les technologies de l'information sont omniprésentes dans la société d'aujourd'hui. Au Canada en 2008, il était estimé que plus de 74% des foyers possédaient un abonnement à Internet et près de 80% des entreprises utilisaient ce moyen de communication pour supporter leurs opérations internes ainsi que pour rejoindre leur clientèle. A lui seul, le gouvernement fédéral offrait plus de 130 services en ligne à la population canadienne.[2] Notre dépendance envers les technologies de l'information est telle qu'il est aujourd'hui difficile d'imaginer un retour en arrière avant l'apparition d'Internet, des téléphones intelligents et des tablettes numériques.

L'environnement cybernétique se définit comme étant un « Réseau interdépendant de structure de technologies de l'information, incluant Internet, les réseaux de télécommunication, les systèmes informatiques et les contrôleurs intégrés ainsi que les logiciels et les renseignements qu'ils contiennent. »[3] On estime que le cyberespace relie maintenant plus de 1,7 milliards de personnes dans le monde entier.

---

[1] Rex Hughes, « A Treaty for Cyberspace », International Affairs, page 523.

[2] Ministère de la Sécurité Publique. *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, Ottawa : Groupe Communication Canada, 2010, page 2.

[3] Ministère de la Défense Nationale, *Introduction aux cyberopérations des FAC*, Chef du développement des forces, Février 2014.

Malheureusement, cet espace virtuel fait aussi l'objet d'un nombre grandissant de menaces qui viennent mettre à risque son utilisation sécuritaire et sa fiabilité. Des états à la recherche de pouvoir et d'influence, des organisations terroristes désirant semer le doute dans la confiance des citoyens, des groupes criminels voulant étendre leurs activités dans cet environnement, ou simplement des individus mal intentionnés, multiplient les efforts pour tirer avantages des vulnérabilités du cyberespace. Les rapports annuels publiés par les grandes firmes de sécurité informatique comme McAfee[4] et Symantec[5] démontrent bien l'ampleur de cette réalité. Afin de freiner cette menace, de nombreux pays ont publié des stratégies afin de sécuriser le cyberespace. Le Canada ne fait pas exception à cette tendance et, en 2010, il a publié la « Stratégie de cybersécurité du Canada »[6] qui vient énoncer les grandes lignes qui permettront au pays d'être prêt à contrer cette menace efficacement.

La dépendance aux technologies de l'information touche aussi les forces armées modernes et pousse ces dernières à développer des stratégies afin de préserver la sécurité de leurs opérations dans le cyberespace. Le présent essai fera l'analyse de la stratégie mise sur pied par le Ministère de la Défense Nationale (MDN) et les Forces Armées Canadiennes (FAC) pour ce qui a trait au cyberespace. L'intention étant de déterminer si celle-ci répond à leurs besoins opérationnels. Pour ce faire, l'emploi du cyberespace ainsi que les menaces spécifiques aux opérations militaires seront brièvement décrits. Par la

[4] McAfee Labs, *Threats Report – November 2014*, McAfee Labs. Accédé le 14 avril 2015, http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q3-2014.pdf

[5] Symantec, *Internet Security Threat Report 2015*. Accédé le 14 avril 2015, http://know.symantec.com/LP=1123.

[6] Ministère de la Sécurité Publique. *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, Ottawa : Groupe Communication Canada, 2010.

suite, une révision des stratégies canadiennes en matière de cyber-sécurité et de cyber-opérations sera complétée afin d'en faire une évaluation adéquate.

LE CYBERESPACE ET LES FAC

Bien qu'au niveau organisationnel, le MDN et les FAC conservent toujours la vision traditionnelle des trois environnements principaux (Air, Terre, Mer), le domaine cybernétique n'est pas une nouveauté dans les opérations militaires. En effet, bien qu'ils puissent être considérés archaïques, les systèmes de communication employés lors des différents conflits au début du 20^{e} siècle étaient les technologies de l'information de l'époque. Le code Morse, les postes de transmission radio et les téléphones de campagne sont les systèmes qui constituaient le cyberespace de jadis, et des unités de guerre électronique menaient des opérations spécifiques dans cet environnement. Bien que ces technologies représentaient un avantage à quiconque pouvait en faire une utilisation efficace, le succès des opérations ne dépendaient pas du cyberespace.

Ce qui diffère aujourd'hui, c'est la dépendance que les FAC, comme toutes les autres forces armées modernes, ont face au cyberespace. Les technologies de l'information sont maintenant omniprésentes dans les opérations militaires. Les postes de commandement d'une brigade ou d'un groupement tactique canadien ne se déploient plus sans une infrastructure informatique complexe. Les radars et les appareils automatisés servant à la surveillance, la détection et la protection de la force sont de plus en plus sophistiqués. La chaîne logistique repose sur le Réseau Étendu de la Défense (RÉD) et des applications comme PeopleSoft et DRMIS, qui sont désormais essentielles au soutien des opérations. Qui plus est, l'ensemble est interconnecté par des systèmes de communication perfectionnés afin d'offrir aux commandants à tous les niveaux (du

tactique au stratégique) une connaissance de la situation et un commandement efficace. Un ennemi qui serait en mesure de dégrader ou empêcher l'utilisation du RÉD ou d'un système de commandement et contrôle par les FAC, pourrait grandement affecter le succès de nos opérations. Le cyberespace est aussi essentiel pour assurer l'interopérabilité avec nos alliés dans le cadre d'opérations expéditionnaires. La nécessité d'avoir nos systèmes nationaux interconnectés avec ceux de la coalition augmente notre dépendance au cyberespace et représente une vulnérabilité supplémentaire.

De nombreuses nations ont compris que les conflits du futur ne se gagneraient pas seulement par des troupes déployées au sol, des campagnes aériennes et des affrontements navals. Le cyberespace devient un enjeu qui gagne en importance. Tout comme les concepts de supériorité et de suprématie aérienne, quiconque est en mesure de dominer dans le cyberespace possède un avantage certain face à son adversaire. Des pays comme la Chine, la Russie, l'Iran et la Corée du Nord ont ainsi créé des unités spécialisées pour faire la guerre dans le cyberespace.[7] Ailleurs, des groupes terroristes et des factions armées non-étatiques exploitent aussi le cyberespace. Par exemple, l'État Islamique en Iraq et au Levant (EIIL) l'utilise pour mener des campagnes de recrutement ainsi que pour la distribution de propagande. Certains de ces combattants ont même ouvertement déclaré avoir l'intention d'acquérir des capacités offensives dans le cyberespace afin de nuire aux forces de la coalition.[8] Sachant qu'il est relativement simple, efficace et peu couteux de se procurer ce type de capacité, on ne peut négliger

[7] Department of Defense, *The DoD Cyber Strategy*, April 2015, Page 9
[8] *Idem.*

cette menace. Il est possible d'obtenir des réseaux zombies, en mesures de mener des attaques importante via Internet, pour aussi peu que 250$.[9]

Au cours de la dernière décennie, des attaques concrètes ont été menées par diverses organisations afin d'acquérir des avantages militaires. Par exemples, les drones américains, qui ont fait leurs preuves au cours des conflits en Afghanistan et en Iraq dans les deux dernières décennies, ont été pris pour cible à diverses reprises. En 2009, des troupes américaines ont découvert que des insurgés Iraquiens avaient réussi à accéder à une quantité impressionnante de vidéo provenant de ces drones. Des recherches ont démontré que de simples logiciels disponibles à faible coût permettaient aux insurgés d'intercepter les transmissions et de capturer les données précieuses.[10] En 2011, grâce à une attaque cybernétique, l'Iran a réussi à prendre le contrôle d'un drone américain (RQ-170 Sentinel), de le faire atterrir, pour ensuite récupérer du renseignement et de la technologie militaire.[11] En 2013, la Corée du Nord aurait mené une attaque contre les institutions financières et les médias sud-coréens en guise de répercussion aux tensions militaires entre les deux pays. Il existe de nombreux autres exemples et les alliés n'y font pas exception, ces derniers exploitent aussi le cyberespace à leur avantage. Stuxnet, découvert en 2010 pour contrer le programme nucléaire iranien, n'est qu'un exemple bien connu de son utilisation par les Américains.[12]

---

[9] Ministère de la Défense Nationale, *Introduction aux cyberopérations des FAC*, Chef du développement des forces, Février 2014, page 4, note.

[10] Wired, *Exclusive: Computer Virus Hits U.S. Drone Fleet*, http://www.wired.com/2011/10/virus-hits-drone-fleet/ , Accédé le 25 mai 2015.

[11] Global Research, *Israeli Intelligence Report: US Drone Downed by Iran Cyber Attack*, http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114, Accédé le 25 mai 2015.

[12] NATO, *Cyber Timeline*, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. Accédé le 25 mai 2015.

Ainsi, les risques que représente l'utilisation du cyberespace ne se limitent pas au gouvernement, à l'industrie privé et aux groupes criminels. Les FAC en ont besoin pour conduire leurs opérations militaires et doivent en comprendre les menaces et les vulnérabilités. Le Canada doit donc adopter une stratégie afin de sécuriser l'emploi du cyberespace par ses forces armées, se défendre contre une attaque éventuelle et être prêt à opérer dans un environnement cybernétique dégradé. Alors que nous sommes toujours dans les débuts de l'ère de la guerre cybernétique, le Canada doit dès maintenant faire son choix à savoir s'il désire être un joueur actif dans se domaine en développant une capacité offensive, ou bien s'il se contentera de sécuriser ces systèmes.

LA STRATÉGIE CANADIENNE

Tel que déjà mentionné, en réponse à la menace grandissante sur le Canada, le gouvernement a publié la « Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité » en 2010. Cette dernière propose un approche pangouvernemental à la sécurité dans le cyberespace afin d'atteindre trois principaux objectifs : 1 – Protéger les systèmes gouvernementaux; 2 – Nouer des partenariats pour protéger les cyber-systèmes essentiels à l'extérieur du gouvernement fédéral; 3 – Aider les Canadiens à se protéger. Le gardien de cette stratégie est Sécurité Publique Canada, mais chaque ministère y retrouve son rôle. Ainsi, le mandat suivant est attribué au MDN et aux FAC :

> « Le MDN et les FAC renforceront leur capacité de défendre leurs propres réseaux et travailleront avec d'autres ministères fédéraux afin de cerner les menaces et de déterminer les interventions possibles. Ils continueront en outre d'échanger avec les forces militaires de nos alliés de l'information sur les pratiques exemplaires […] Le MDN et les FAC collaboreront avec nos alliés pour établir des cadres stratégiques et juridiques régissant les aspects militaires de la cybersécurité [...] »[13]

[13] *Idem*, page 11.

Bien que cette stratégie donne un mandat clair au MDN et aux FAC, ce dernier est limité à la sécurité de ses propres réseaux. Il n'est aucunement mention d'avoir une posture ou une capacité offensive. De plus, Sécurité Publique Canada étant le ministère avec la responsabilité globale de la cyber-sécurité auprès du gouvernement fédéral, le mandat lui revient d'assurer la coordination en vue de la protection des infrastructures essentielles, le MDN n'y jouant qu'un rôle secondaire.

D'un autre coté, le MDN et les FAC n'ont pas attendu d'avoir des directives du gouvernement fédéral avant d'orienter certains efforts dans le domaine du cyberespace, ni se sont-ils limités à la protection de leurs systèmes. Ainsi, dans une grande quantité de documents publiés par le MDN et les FAC depuis 2008, il est question de cyberespace. Premièrement, dans la publication qui constitue le pilier de la stratégie canadienne pour la défense, soit la « Stratégie de défense – Le Canada d'abord », on retrouve une mention explicite quant aux opérations dans le cyberespace.

> « Étant donné le caractère complexe et imprévisible du contexte actuel en matière de sécurité, le Canada doit pouvoir compter sur des forces armées modernes, bien entraînées, bien équipées et dotées de la flexibilité et des capacités essentielles requises pour contrer les menaces traditionnelles et asymétriques, y compris le terrorisme, les mouvements insurrectionnels et les cyberattaques. »[14]

Bien qu'il ne s'agisse pas ici d'une stratégie formelle en matière de cyberespace, il est tout de même question de la nécessité pour les FAC de contrer les menaces liées aux cyber-attaques. Dans cette même lignée, le bureau du Chef du Développement des Forces publie en 2009 un document intitulé « Concept Cadre Intégré » dans lequel il introduit des concepts émergents et suggère la création de trois nouveaux environnements stratégiques, soient l'Espace, le Cyberespace et l'environnement Humain. On y indique

[14] Ministère de la Défense Nationale, *Stratégie de Défense – Le Canada d'abord*, 2008, page 7.

que ces environnements auront des répercussions stratégiques dans les conflits du futur et que les forces armées modernes doivent être prêtes à gérer les répercussions d'une attaque dans n'importe quel des six environnements. Elles doivent aussi être capables d'y générer des impacts opérationnels et de les exploiter avantageusement et ce, d'une façon intégrée.[15]

En 2010, alors que le gouvernement canadien publiait sa stratégie sur la cyber-sécurité, le Vice-chef d'état-major de la Défense (VCEMD) créait le premier groupe de travail sur la cybernétique. Opérant sous le SMA(GI), son mandat était d'examiner les capacités existantes et futures du MDN et des FAC en matière de cyberespace et de développer les concepts et les structures organisationnelles entourant ce domaine.[16] C'est deux ans plus tard, soit en 2012, que ce groupe de travail deviendra le Directorat du Développement de la Force Cybernétique.[17]

Dans son guide à l'intention des FAC de 2013, le Chef d'état-major de la Défense (CEMD) confirme son intention de développer une force cybernétique afin de conduire des opérations dans ce domaine en coopérations avec les environnements traditionnels. Cependant, aucun détail sur l'ampleur d'une capacité potentielle n'est énoncé.[18] Ainsi, malgré cette variété de documents officiels et d'intentions nobles identifiant le cyberespace comme un domaine dans lequel les FAC se doivent d'investir, le MDN et les FAC n'avaient toujours pas de politique ou de stratégie formelle qui encadraient le développement d'une force cybernétique.

---

[15] Ministère de la Défense National, *Concept Cadre Intégré*, 23 octobre 2009, page 29-40.

[16] Ministère de la Défense Nationale, *Directive du VCEMD concernant la création du groupe de travail sur la cybernétique*, Vice-chef d'état-major de la Défense, 1 Septembre 2010.

[17] Ministère de la Défense Nationale, *Canadian Armed Forces Cyber Force Development Program*, Chief of Force Development, 22 May 2014, page 1

[18] Ministère de la Défense Nationale, *CDS – Guidance to the Canadian Armed Forces*, Ottawa : Groupe Communication Canada, 2013, page 13

C'est finalement en 2014 que le bureau du Chef de Développement des Forces publie deux documents qui forment l'embryon de ce qui devrait devenir la stratégie du MDN et des FAC quant au cyberespace, soit :

- Introduction aux cyber-opérations des FAC[19]
- Programme des FAC pour le développement de la force cybernétique[20]

N'étant pas des politiques en soit, ces publications trace le chemin pour le développement d'une stratégie pour le Canada. Le programme de développement des capacités cybernétiques pour les FAC introduit cinq effets désirés à long terme. Ces objectifs représentent ce qui pourrait se retrouver dans une politique future pour les MDN et les FAC.

- Un MDN et des FAC conscients de la réalité cybernétique;
- Un environnement cybernétique sécuritaire, résilient, réactif et fiable;
- Une liberté d'action dans l'environnement cybernétique;
- Les cyber-opérations intégrées dans les opérations des FAC; et
- Un partenaire crédible au sein du Gouvernement du Canada et de la coalition.

Le plan de campagne est divisé en quatre lignes d'opérations distinctes et devrait atteindre une capacité opérationnelle finale en 2021. La première ligne d'opérations s'intitule : « Politique, Gouvernance et Engagement ». Celle-ci vise d'ailleurs directement l'établissement d'une politique et d'une gouvernance pour encadrer les opérations du MDN et des FAC dans le cyberespace d'ici 2016. Les autres lignes d'opérations de ce plan sont le développement des capacités, l'élaboration d'une doctrine propre aux cyber-opérations, ainsi que les aspects liés aux ressources humaines.[21]

---

[19] Ministère de la Défense Nationale, *Introduction aux cyberopérations des FAC*, Chef du développement des forces, Février 2014.

[20] Ministère de la Défense Nationale, *Canadian Armed Forces Cyber Force Development Program*, Chief of Force Development, 22 May 2014.

[21] *Idem*, page 16-21 et Annexe A.

ÉVALUATION DE LA POLITIQUE DU MDN ET DES FAC

Premièrement, avant même de faire une analyse approfondie, la première critique qu'il est possible d'énoncer au sujet de la stratégie du MDN et des FAC face aux cyber-opérations est tout simplement l'absence d'une politique formelle. Comme il a été mentionné précédemment, depuis 2008 le concept de cyberespace est présent dans une variété de documents stratégiques. Dans certains, il est même question du besoin de créer un environnement spécifique pour le cyberespace. Cependant, plus de sept ans plus tard, une politique se fait toujours attendre. L'un des rôles du programme de développement de la force cybernétique est spécifiquement d'élaborer cette politique. En 2013, le Brigadier-Général Greg Loos, alors assumant le leadership de cette initiative, accordait une entrevue au Vanguard Magazine et affirmait : « … we don't necessarily have a strategy but we have a plan and that is what we have been working on for the past couple of years. »[22]

Le Canada accuse donc un certain retard face à ces principaux alliés dans le domaine. Par exemple, les États-Unis ont récemment publié la seconde mouture de leur stratégie[23] qui leur a permis de renforcer certains aspects de leur politique, la première ayant été publiée en 2011.[24]

Cependant, une des tendances positives que l'on peut tirer de l'ensemble des publications canadiennes citées ci-haut est l'intention claire du MDN et des FAC d'investir dans le développement de capacités cybernétiques. Cette intention n'est pas de seulement assurer la protection et la sécurité de ses propres réseaux, comme le dicte la

---

[22] Thatcher, Chris, « Operationalizing the Cyber Domain, *Vanguard magazine*, June/July 2013.
[23] Department of Defense, *The DoD Cyber Strategy*, April 2015.
[24] Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.

stratégie gouvernementale, mais bien d'intégrer les cyber-opérations aux opérations militaires et d'être un partenaire crédible auprès de nos alliés. Le tout est appuyé par un programme ambitieux de développement de la force cybernétique, dont la vision se résume par : « Une force cybernétique intégrée, cohérente et entièrement institutionnalisée, capable d'assurer la liberté d'action dans l'environnement cybernétique, tout en niant la même chose pour nos adversaires. [Traduction]»[25]

L'un des aspects que l'on retrouve dans cette politique est la nécessité d'avoir une force consciente du cyberespace, connaissant les avantages ainsi que les risques militaires liés à son exploitation et surtout, du besoin de protéger nos systèmes contre les menaces potentielles. Pour y parvenir, on a clairement identifié la nécessité de l'intégration de tous les environnements des FAC, la coopération avec nos principaux alliés, ainsi que la participation des autres ministères fédéraux et de l'industrie.

En comparant cette politique embryonnaire à celle des États-Unis, on peut faire de nombreux rapprochements avec les cinq objectifs stratégiques américains. Cependant, la politique de notre allié reflète un caractère plus offensif et démontre une vision davantage axée sur l'exploitation du cyberespace en tant qu'environnement. Les États-Unis ont d'ailleurs créé le « United-States Cyber Command » en 2009, dont l'un des principaux mandats est d'être prêt à conduire des opérations dans le cyberespace et ce, dans tout le spectre des conflits.[26] Ceci ne démontre pas nécessairement une faiblesse ou une lacune de la politique canadienne, mais démontre quand même que les États-Unis n'ont pas

[25] Ministère de la Défense Nationale, *Canadian Armed Forces Cyber Force Development Program*, Chief of Force Development, 22 May 2014, p. 2.

[26] U.S. Cyber Command, http://www.stratcom.mil/factsheets/2/Cyber_Command/, accédé le 25 mai 2015.

l'intention de prendre du recul face aux autres nations comme la Chine, la Russie, l'Iran et la Corée du Nord.

Toujours en comparaison avec la politique américaine, cette dernière fait explicitement mention du besoin pour le Département de la Défense d'avoir des plans de contingence, et de les exercer, afin de permettre la poursuite des opérations dans un environnement cybernétique dégradé. Dans l'éventualité où une cyber-attaque contre leurs infrastructures essentielles est réussie, le Département de la Défense doit être en mesure de réagir rapidement et de continuer ses opérations. Dans les publications canadiennes, il n'est aucunement mention du besoin d'avoir un plan de poursuite des activités en cas de cyber-attaques ou d'opérations dans un environnement dégradé. Alors que la technologie est souvent considérée comme « acquise et essentielle» aux opérations, la stratégie canadienne devrait au minimum couvrir la nécessité d'avoir des processus en place pour faire face à ce type de situation.

Une différence supplémentaire se situe dans le mandat attribué au Département de la Défense américain, selon lequel il doit être prêt à défendre les intérêts nationaux contre toutes cyber-attaques.[27] Ce dernier joue donc un rôle de première importance dans la protection cybernétique des infrastructures essentielles dans le pays. Comme il a été mentionné précédemment, la stratégie de cyber-sécurité canadienne n'octroie pas ce mandat spécifique au MDN et aux FAC, son rôle de protection se limitant à ses propres infrastructures.

Que la politique canadienne soit plus ou moins agressive que celle de nos alliés n'est pas nécessairement représentative de la capacité disponible ou de celle qui sera développée dans les prochaines années par le MDN et les FAC. Un aspect qui ne doit pas

[27] Department of Defense, *The DoD Cyber Strategy*, April 2015, p. 14.

être négligé est la capacité des FAC de mettre les conditions en place pour supporter cette politique. Le programme du développement de la force cybernétique prévoit que pour permettre l'exécution du plan actuel, il y a un besoin de 381 personnes supplémentaires d'ici 2021 (militaires et civils). Ces dernières viendraient s'ajouter aux organisations déjà en place comme le Centre d'Opérations des Réseaux des Forces Canadiennes (CORFC) ou autres unités liées à ce domaine. Divers projets capitaux ont aussi été identifiés pour fournir des capacités commençant par l'entraînement, la connaissance de la situation cybernétique, et allant jusqu'aux cyber-opérations défensives et offensives, le tout totalisant au-delà de $500M.[28] Ce qui n'inclut pas les autres projets d'importance liés au cyberespace et non gérer par ce programme, comme ceux relatifs à la sécurité des réseaux informatiques, à la guerre électronique ou autres, et qui sont déjà identifiés dans le Guide d'Acquisition de la Défense.[29] Avec la période de restriction budgétaire des dernières années, les projets capitaux importants à venir, le Plan d'action pour la réduction du déficit (PARD) et l'Examen stratégique (ES), le programme de développement de la force cybernétique demeure un plan optimiste et très ambitieux. Il demeure quand même bien adapté aux réalités canadiennes. Il reste à démontrer que le MDN et les FAC seront en mesure de rencontrer les objectifs fixés, spécialement pour ce qui a trait aux capacités offensives.

CONCLUSION

En résumé, les technologies de l'information et le cyberespace font maintenant parti du quotidien de toute société moderne. Avec cette dépendance croissante de la

[28] Ministère de la Défense Nationale, *Canadian Armed Forces Cyber Force Development Program*, Chief of Force Development, 22 May 2014, p. 27-28.

[29] Guide d'Acquisition de la Défense, http://www.forces.gc.ca/fr/guide-acquisition-de-la-defense/index.page, accédé le 25 mai 2015.

société, les menaces se sont multipliées et la criminalité a trouvé son chemin vers le cyberespace. L'environnement militaire ne fait pas exception à cette règle. De nombreux systèmes militaires exploitent et dépendent de technologies sophistiqués et interconnectés.

Le présent essai a débuté par faire l'introduction de l'impact du cyberespace sur le MDN et les FAC et la dépendance des forces armées modernes envers les technologies de l'information pour assurer le succès de leurs opérations. Alors que le Canada est toujours dans ses premières expériences dans le domaine, plusieurs nations, alliées ou non, ont déjà commencé à exploiter le cyberespace pour obtenir des avantages sur le plan militaire. Des exemples concrets ont été présentés dans lesquels des attaques cybernétiques commanditées par des états ont réussi à atteindre des objectifs militaires.

Une révision de l'ensemble des publications du MDN et des FAC au sujet de la politique canadienne en matière d'opérations dans le cyberespace publiées au cours des sept dernières années a été complétée. Cette dernière a permis d'évaluer la stratégie du MDN et des FAC pour exploiter ce nouvel environnement à son avantage et répondre aux menaces émergentes.

Le premier aspect qui a été soulevé est que le Canada ne possède présentement aucune politique ni stratégie officielle quant au cyberespace. La principale publication dans laquelle il est possible retrouver l'embryon de ce que pourrait être la politique est le programme de développement de la force cybernétique des FAC. L'analyse des éléments de ce programme a cependant permis de démontrer que la stratégie prônée par le MDN et les FAC semble être moins agressive que celle des États-Unis, mais bien adapté aux réalités canadiennes. De plus, bien qu'un plan de développement ambitieux soit en place

pour développer une force cybernétique, il reste à démontrer si le Canada sera en mesure d'investir les ressources (humaines et monétaires) nécessaires pour rencontrer les objectifs fixés.

En guise de conclusion, le plan est en place pour assurer le développement de capacités cybernétiques pour les FAC. Avec l'importance mise sur la sensibilisation, la sécurité et la protection, cette stratégie modeste devrait tout de même être en mesure de contribuer à protéger nos systèmes militaires d'une manière efficace. Il est cependant encore trop tôt afin de déterminer si elle sera suffisante pour mener des opérations cybernétiques offensives, bien intégrés avec les opérations militaires des autres environnements (Air, Terre, Mer), bien que ceci fasse parti de la vision à plus long terme.

Un des aspects qui n'a pas été abordé dans le présent document, et qui semble aussi être omis dans les différentes politiques et stratégies révisées dans le cadre de ce travail, est celui du Droit International, du Droit des Conflits Armés et leurs applications dans le cyberespace. Est-ce qu'une cyber-attaque peut être considérée comme un acte de guerre? Comment fait-on du cyber-ciblage? Comment peut-on juger des dommages collatéraux d'une cyber-attaque? Est-ce que l'attaque de la Corée du Nord contre le système financier sud-coréen peut mener à une réponse militaire? Il serait opportun qu'une politique militaire liée au cyberespace ait une composante juridique. Les réponses aux questions précédentes devraient être identifiées avant qu'un conflit ne survienne à plus grande échelle, et que l'arme nucléaire soit remplacée par l'arme cybernétique ultime.

BIBLIOGRAPHIE

Canada. Bureau du vérificateur général du Canada. *Rapport du vérificateur général du Canada à la Chambre des Communes – Chapitre 3: Protéger l'infrastructure canadienne essentielle contre les cybermenaces*, Ottawa : Groupe Communication Canada, 2012.

Canada, Director General Cyber, DWAN Sharepoint Website, http://collaboration-vcds.forces.mil.ca/sites/DG_Cyber/D_Cyber_FD, Accédé le 23 avril 2015.

Canada, Guide d'Acquisition de la Défense, http://www.forces.gc.ca/fr/guide-acquisition-de-la-defense/index.page, accédé le 25 mai 2015.

Canada, Le Comité sénatorial permanent de la sécurité nationale et de la défense, *Témoignage du 5 novembre 2012*, http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-f.HTM, Accédé le 25 mai 2015.

Canada, Ministère de la Défense Nationale, *Canadian Armed Forces Cyber Force Development Program*, Chief of Force Development, 22 May 2014.

Canada, Ministère de la Défense Nationale, *Directive du VCEMD concernant la création du groupe de travail sur la cybernétique*, Vice-chef d'état-major de la Défense, 1 Septembre 2010.

Canada, Ministère de la Défense Nationale, *No Man's Land : Tech Consideration for Canada's Future Army*, Kingston : Army Publishing Office, 2014.

Canada, Ministère de la Défense Nationale, *Introduction aux cyberopérations des FAC*, Chef du développement des forces, Février 2014.

Canada, Ministère de la Défense Nationale, *Stratégie de Défense – Le Canada d'abord*, 2008.

Canada, Ministère de la Défense National, *Concept Cadre Intégré*, 23 octobre 2009.

Canada, Ministère de la Défense Nationale, *CDS – Guidance to the Canadian Armed Forces*, Ottawa : Groupe Communication Canada, 2013.

Canada, Ministère de la Sécurité Publique. *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, Ottawa : Groupe Communication Canada, 2010.

Canada, Ministère de la Sécurité Publique. *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada*, Ottawa : Groupe Communication Canada, 2013.

Canada, Sécurité Publique Canada, « Cybersécurité : Une responsabilité partagée », Accédé le 14 avril 2015, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/index-fra.aspx

Deibert, Ron. *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*, Calgary: Canadian Defense and Foreign Affairs Institute, 2012.

Global Research, *Israeli Intelligence Report: US Drone Downed by Iran Cyber Attack*, http://www.globalresearch.ca/israeli-intelligence-report-us-drone-downed-by-iran-cyber-attack/28114, Accédé le 25 mai 2015.

Hughes, Rex, « A Treaty for Cyberspace », *International Affairs*, 86, Vol 2 (2010), page 423-541.

Levin, Avner, *Securing Cyberspace: A comparative Review of Strategies Worldwide*, Privacy and Cyber Crime Institute: Ryerson University, http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf, Accédé le 14 avril 2015.

McAfee Labs, *Threats Report – November 2014*, McAfee Labs, http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q3-2014.pdf, Accédé le 14 avril 2015.

Meyer, Paul, « A cyber foreign policy – time for Canada to get one », *Policy Options*, December 2010.

Moens, A., Cushing, S., Dowd A.W., « Cybersecurity Challenges for Canada and the United States », Fraser Institute, Mars 2015.

NATO, *Cyber Timeline*, http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm, Accédé le 25 mai 2015.

Netherlands, Ministry of Defence, *The Defence Cyber Strategy*, September 2012.

Racicot, J., « The Past, Present and Future of Chinese Cyber Operations », *Canadian Military Journal* 14, no 3, Summer 2014, page 26-37.

Schmitt, M.N., « Internation Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed », *Harvard International Law Journal* 54, December 2012.

Symantec, *Internet Security Threat Report 2015*, http://know.symantec.com/LP=1123, Accédé le 14 avril 2015.

Thatcher, Chris, « Operationalizing the Cyber Domain, *Vanguard magazine*, June/July 2013.

United-States, Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011.

United-States, Department of Defense, *The DoD Cyber Strategy*, April 2015.

United-States, U.S. Cyber Command, http://www.stratcom.mil/factsheets/2/Cyber_Command/, Accédé le 25 mai 2015.

Wired, *Exclusice: Computer Virus Hits U.S. Drone Fleet*, http://www.wired.com/2011/10/virus-hits-drone-fleet/, Accédé le 25 mai 2015.