National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

MATÉRIALISER LE VIRTUEL: MODÉLISATION D'UN COMMANDEMENT CYBERNÉTIQUE

Major M.D.F. Boivin

JCSP 40

Master of Defence Studies

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

Maîtrise en études de la défense

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
2013 – 2014

RESEARCH PAPER / MASTER OF DEFENCE STUDIES –
MÉMOIRE DE RECHERCHE / MAÎTRISE EN ÉTUDES DE LA DÉFENSE

MATÉRIALISER LE VIRTUEL: MODÉLISATION D'UN COMMANDEMENT CYBERNÉTIQUE

By Major M.D.F. Boivin
Par le major M.D.F. Boivin

Word Count: 19 896

Compte de mots : 19 896

TABLE DES MATIÈRES

LISTE DES FIGURES

SOMMAIRE

La prospérité ainsi que la sécurité de la population sont à la base de toutes grandes stratégies gouvernementales des pays développés. L'émergence d'internet, bien que favorable à la prospérité et au bien-être de la majorité des visiteurs de ce monde virtuel, a donné naissance à la cybermenace, une nouvelle force ennemie qui exige une vision et une approche différente pour y faire face. Les principaux alliés du Canada ont élevé au rang de priorité la cyberdéfense avec l'annonce de stratégie et de mesures concrètes telles que la mise en place d'un commandement cybernétique au sein de leur institution militaire et qui permet d'unifier les efforts.

Le contexte politique, les usagers, les infrastructures essentielles du Canada et de ses alliés ainsi que les diverses formes de cyberagressions interagissent dans un environnement qui est loin d'être stable. Puisque ces éléments sont considérés comme faisant partie intégrante du cybermonde, il devient dès lors essentiel de comprendre que tous ces acteurs forment la matière même sur laquelle les politiciens et chefs militaires doivent agir afin d'exercer leur leadership de façon efficace.

Le présent travail de recherche propose la création d'un Commandement cybernétique, sous la gouverne du chef d'état-major de la Défense, afin de fusionner les ressources et les initiatives de l'espace virtuel des FAC. Ce changement institutionnel implique une nouvelle vision quant au rôle et aux responsabilités des FAC en matière de cyberdéfense du Canada, et ce, tant auprès du gouvernement canadien que de ses alliés.

MATÉRIALISER LE VIRTUEL:

MODÉLISATION D'UN COMMANDEMENT CYBERNÉTIQUE

> « Certains aspects de la situation réclament une attention particulière, et si nécessaire, une action rapide de la part de l'Administration. Je pense donc qu'il est de mon devoir d'attirer votre attention sur les faits et recommandations suivants […] » [Traduction]
>
> Albert Einstein, Lettre au président Roosevelt le 29 août 1939

CHAPITRE 1 – INTRODUCTION

En 2013, pas moins de 97% des entreprises de la revue Fortune 500 ont été la cible d'attaques cybernétiques. Quant aux autres, ils n'ont tout simplement pas détecté l'agression. Le *Petit Larousse* définit le cybermonde, qu'on appelle aussi monde cybernétique, espace cybernétique, cyberespace et monde virtuel, comme « [L'] espace virtuel rassemblant la communauté des internautes et les ressources d'informations numériques accessibles à travers les réseaux d'ordinateurs »1. Cette nouvelle réalité mondiale est irréfutablement une source de scandale majeure ces derniers temps avec entre autres le site WikiLeaks, la prise de contrôle de la NASA et la conception d'armes cybernétiques ingénieuses de style Stuxnet, qui permettent le contrôle de réseaux informatiques à distance tout en demeurant pratiquement indétectables. Le président américain Barack Obama a même déclaré récemment que [Traduction] « […] les risques reliés à la cybersécurité se classent parmi les plus grands défis de la sécurité nationale de ce jour et la prospérité américaine du XXIe siècle en est totalement dépendante »2. Par

---

1 Isabelle Jeuge-Maynart , *Le Petit Larousse Illustré* (Paris : Larousse, 2007), p. 278.

conséquent, le président a demandé une révision complète de l'effort gouvernemental américain afin de défendre les infrastructures d'information et de communication. Le « Cyberspace Policy Review » découle de cette révision et constitue maintenant une priorité pour Washington. Howard Schmidt, un expert de plus de 40 ans d'expérience dans le domaine de la défense et de la sécurité informatique, et qui a occupé notamment des postes de chef de la sécurité chez Microsoft Corp et eBay, est devenu tout récemment conseiller spécial du président Obama et coordonnateur de la cybersécurité américaine3.

Le gouvernement du Canada (GC), quant à lui, a nouvellement publié Canada numérique 150, un plan audacieux qui vise à ce que la population canadienne se retrouve parmi les chefs de file de la révolution numérique4. En conséquence, la politique du cybermonde semble être devenue une priorité pour notre pays. Tout comme pour les États-Unis, la prospérité économique canadienne est fondamentalement liée à un réseau de communication global, mais sécuritaire. En 2011, le Canada a obtenu des revenus évalués à 49 milliards de dollars à travers internet, soit la plus forte croissance des 20 pays membres de l'Organisation de coopération et de développement économique (OCDE). Il s'agit d'ailleurs d'un montant plus important que la contribution du secteur de l'agriculture5.

---

2 The White House, « Foreign Policy / Cybersecurity », consulté le 28 janvier 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

3 The White House, « The White House Blog », consulté le 28 janvier 2014, http://www.whitehouse.gov/blog/author/Howard%20A.%20Schmidt

4 Industrie Canada, *Canada numérique 150* (Ottawa : Groupe Communication Canada, 2014), p. 3. Consulté le 28 avril 2014, https://www.ic.gc.ca/eic/site/028.nsf/vwapj/CN150-FR.pdf/$FILE/CN150-FR.pdf

5 Tavis Grant, « Canada urged to pull up its socks in Internet economy », *Globe and Mail*, 19 mars 2012.

De plus, les Canadiens utilisent internet deux fois plus que la moyenne mondiale6. Or une forte utilisation d'internet entraîne inévitablement des problèmes de sécurité. En effet, une récente étude dévoilée par le *Globe and Mail* classe le Canada au sixième rang des pays qui hébergent le plus de logiciels malveillants sur leurs serveurs7. Récemment, une nouvelle étonnante a été dévoilée concernant la débâcle financière de la compagnie Nortel. Siobhan Gorman, un journaliste spécialiste du terrorisme, contreterrorisme et des services de renseignement fédéraux pour *The Wall Street Journal*, a révélé l'ampleur des vols d'identités par internet dont celui du président-directeur général (PDG) de Nortel qui aurait permis à des pirates informatiques d'origine chinoise de naviguer allègrement sur le réseau informatique de Nortel pendant plus d'une décennie, leur donnant accès aux diverses propriétés intellectuelles de la firme8.

Pour les Forces armées canadiennes (FAC), qui tentent de définir son rôle et ses responsabilités dans un environnement de conflits modernes, l'espace cybernétique ne fait que brouiller davantage la détermination des frontières. En effet, peu de stratèges comprennent l'amplitude des interactions à l'intérieur de cette nouvelle dimension, ne facilitant en rien la formulation de la doctrine de cyberdéfense. De même, les multiples organisations des FAC impliquées avec le cybermonde dévouent beaucoup de temps et d'énergie à développer des

---

6 comScore, « 2013 Canada digital future in focus », consulté le 28 janvier 2014, http://www.comscore.com/fre/Insights/Presentations_and_Whitepapers/2013/2013_Canada_Digital_Future_in_Focus2

7 Misha Glenny, « Canada's weakling web defenses », *Globe and Mail*, 18 mai 2011.

8 Siobhan Gorman, « Chinese hackers suspected in long-term Nortel breach », *The Wall Street Journal*, 14 février 2012.

initiatives, trop souvent en parallèle les unes des autres, ce qui, au final, n'apporte aucun résultat stratégique tangible.

L'urgence d'agir au niveau de la cybersécurité et le besoin de concentrer les efforts des organisations cybernétiques des FAC est au cœur de ce mémoire. Sur les traces de Canada numérique 150, de la Stratégie de cybersécurité du Canada, des diverses initiatives de nos alliés et en utilisant comme levier certains travaux de recherche publiés par de précédents étudiants du Collège des Forces canadiennes (CFC), cette étude propose la création d'un Commandement cybernétique sous la gouverne du chef d'état-major de la Défense (CEMD).

Afin de paver la route vers une description d'une telle structure organisationnelle et de ses fonctions, ce travail définira tout d'abord le cybermonde de manière générale à partir de quatre éléments essentiels, soit l'émergence d'internet, les infrastructures essentielles, les acteurs du domaine et enfin, la menace.

Puisque de toute évidence, la dimension cybernétique constitue une puissante menace, elle se retrouvera de plus en plus au cœur des conflits modernes comme ce fut le cas en Estonie en 2007 avec l'attaque par déni de services. Par conséquent, la chaîne de commandement des FAC se doit d'intégrer la cybersécurité à l'intérieur de ses priorités. Trop souvent, le personnel des transmissions est mis sur la sellette pour donner des recommandations de dernières minutes aux commandants qui n'ont pas considéré le monde virtuel parmi leurs facteurs de planification. Ainsi, ce travail propose en deuxième lieu d'analyser la position des FAC et du gouvernement fédéral face à l'environnement cybernétique. Ce deuxième chapitre poursuivra avec la prise de position de certains des alliés du Canada afin d'établir des comparaisons.

Dans ce même ordre d'idée, ce projet de recherche propose comme troisième sujet une façon de percevoir la dimension cybernétique tout en mettant l'emphase sur les actions concrètes prises par les États-Unis et l'OTAN, permettant du coup de visualiser les avantages favorables à la création d'un commandement cybernétique. En plus de permettre au GC de projeter la force cybernétique comme un instrument de pouvoir et de puissance de sa politique étrangère, ce nouveau commandement permettrait entre autres de concentrer l'expertise pour une meilleure économie d'effort ainsi que d'optimiser la génération, l'emploi et le développement des ressources cybernétiques. Au final, le Commandement cybernétique obtiendrait le niveau de crédibilité nécessaire pour collaborer décemment avec le Centre de la sécurité des télécommunications du Canada (CSTC), nos alliés et le secteur privé.

La conception de la structure organisationnelle du Commandement cybernétique doit répondre aux besoins des FAC, du gouvernement fédéral et de la population en général. À cette fin, ce travail propose comme dernier thème d'utiliser la méthode « Design Thinking » pour modéliser ce nouveau commandement. Cette méthode a largement été étudiée à l'école d'études militaires et stratégiques avancées de Fort Lavenworth (School of Advanced Military Studies – SAMS) en plus d'avoir été utilisée par des généraux américains reconnus tels que le général Petraeus au cours de la guerre en Iraq.

Afin d'établir de façon cohérente les bases de la nouvelle structure proposée, nous présenterons tout d'abord les éléments pertinents reliés au cybermonde.

CHAPITRE 2 – LE CYBERMONDE

« Ce n'est pas un camion, c'est une série de tubes »9 [Traduction], voilà comment Ted Stevens, sénateur de l'Alaska en 2006, expliquait le cybermonde dans une allocution au Congrès des États-Unis. Il est clair que peu de gens comprennent la complexité de tous les vecteurs impliqués avec le cybermonde et encore moins le mode d'opération pour le sécuriser. Une équipe d'experts réunie par le Pentagone a mis plus d'un an de travail pour arriver à définir le monde virtuel. En 2008, ils ont proposé la définition suivante [Traduction] :

> Le domaine global au sein de l'environnement de l'information constitué par le réseau interdépendant des infrastructures des technologies de l'information, y compris l'internet, les réseaux de télécommunications, des systèmes informatiques et de ses processeurs et contrôleurs10.

Bien que très complète, plusieurs souhaiteraient quand même utiliser la définition simpliste du sénateur Stevens, car ils sont tout simplement dépassés par ce monde virtuel qui leur échappe. Tel que précisé par John Adams, ancien chef du CSTC [Traduction] « L'espace cybernétique est conventionnellement utilisé pour décrire tout ce qui est relié avec internet »11. La complexité dans la définition et de la compréhension du cybermonde provient particulièrement de l'interdépendance entre tous les acteurs, qu'il s'agisse des usagers, des infrastructures gouvernementales ou du secteur privé, leur chemin se croise librement sur internet. En effet, le monde virtuel en est un qui n'a pas de frontière et qui est très peu légiféré,

---

9 Common Dreams, « Internet "Tubes" Speech Turns Spotlight, Ridicule onto Sen. Stevens », consulté le 4 février 2014, http://www.commondreams.org/headlines06/0715-06.htm

10 Scott W. Beidleman, « Defining and Deterring Cyber War » (travail rédigé dans le cadre du Programme de maîtrise en études stratégique,US Army War College, 2009), p. 9.

ce qui rend les acteurs vulnérables dans leurs échanges non protégés d'information. Contrairement au monde physique, l'espace cybernétique se développe à très grande vitesse et les divers paliers de gouvernement n'ont pas été en mesure de suivre l'évolution et d'imposer des mesures de contrôle en parallèle à son développement.

Tara Murphy, assistante spéciale du Secrétaire adjoint à la Défense des États-Unis pour les affaires stratégiques globales (Global Strategic Affairs - GSA), une organisation attachée au bureau du sous-secrétaire à la Défense pour la politique, précise [Traduction] :

> [que] dans la communauté mondiale d'aujourd'hui, la sécurité nationale n'est pas assurée par le contrôle d'un simple espace à l'intérieur des frontières reconnues, mais dépend de l'habilité à naviguer à travers les communes globales qui sont la mer, l'air, l'espace et l'espace cybernétique, tous contributeurs de l'économie mondiale12.

Les FAC doivent donc bien comprendre l'ensemble des acteurs du cybermonde pour être mieux en mesure de définir leur rôle et leurs responsabilités à l'intérieur de cette dimension. Dans sa récente publication intitulée *Directives du chef d'état-major de la Défense à l'intention des Forces armées canadiennes*, le général Lawson aborde sommairement l'utilisation des ressources cybernétiques en vue d'accroître l'efficacité des effets intégrés là où elles sont nécessaires. Ainsi, il indique :

> Les FAC, en collaboration avec des partenaires gouvernementaux, amorceront l'élaboration de la cyberforce requise pour mener des cyberopérations de la même manière dont elles mènent leurs opérations en milieu terrestre, maritime, aérien ou

---

11 John Adams, « The Government of Canada and Cyber Security : Security Begins at Home » *Journal of Military and Strategic Studies* Volume 14, Issue 2 (2012), p. 1.

12 Tara Murphy, « Security Challenges in the 21st Century Global Commons » *Yale Journal of International Affairs* Volume 5, Issue 2 (2010), p. 2, consulté le 4 février 2014, http://yalejournal.org/wp-content/uploads/2010/09/105205murphy.pdf

> spatial. Cette cyberforce vise à mieux appuyer toutes les missions énoncées dans la [Stratégie de défense *Le Canada d'abord*] (SDCA)13.

Avec l'objectif de mieux circonscrire le monde virtuel et d'améliorer la définition des responsabilités des FAC, ce chapitre se penche sur quatre composantes importantes du cybermonde. Tout d'abord, un regard sur l'émergence d'internet, qui est à la base de l'espace virtuel, permettra une meilleure compréhension de son utilisation hétéroclite. Ensuite, une définition des infrastructures essentielles mettra en contexte la portée de ce qui est partagé entre le Canada et les États-Unis et l'importance de la cybersécurité pour assurer la prospérité et le bien-être des citoyens. Un troisième élément du chapitre portera sur les acteurs du cybermonde. L'accent est mis sur les politiciens et les usagers, soit ceux qui ont le pouvoir de changer la législation et ceux qui utilisent allègrement internet. La diversité des menaces viendra compléter cette introduction au cybermonde. L'exemple d'une brèche importante subi par le Canada et une mise en situation historique de l'ère cybernétique avec l'ère nucléaire endossera l'urgence d'agir immédiatement.

Cette analyse va conduire à la conclusion que le GC et les FAC doivent être grandement concernées face à la menace cybernétique et que des décisions à court terme sont nécessaires pour défendre un Canada numérique prospère et sécuritaire.

Émergence d'internet

L'évolution d'internet est indubitablement un des phénomènes marquant de la fin du XXe siècle et de nos jours, le moteur de notre modernisation et de la globalisation. Tout a commencé avec le réseau de l'Agence des projets de recherche avancés (Advanced Research Project

---

13 Ministère de la Défense nationale, *Directives du chef d'état-major de la Défense à l'Intention des Forces armées canadiennes* (Ottawa : Groupe Communication Canada, 2013), p.14.

Agency network - ARPANET) en 1966 où les deux premiers nœuds qui forment ce réseau ont relié deux universités californiennes, soit l'Université de Californie à Los Angeles (UCLA) et l'institut de recherche de Stanford. Le premier courrier électronique a été envoyé en 1971, mais ce n'est que dans les années 1980 que des progressions technologiques majeures ont défini l'internet tel qu'on le connait aujourd'hui. Ainsi, le protocole de transport (Transmission Control Protocol – TCP) et les protocoles de communication de réseau informatique conçus pour être utilisés par internet (Internet Protocol – IP) ont vu le jour, suivi par le système de noms de domaine (Domain Name System – DNS). En 1985, ce réseau procurait déjà des services à une communauté de chercheurs et commençait à s'exporter vers une utilisation pour les communications quotidiennes. Un premier site est publié sur la toile en 1991 et deux ans plus tard, soit en 1993, le premier navigateur web supportant des textes et des images voit le jour. En 1995, internet a été formellement institutionnalisé par le Conseil de réseautage fédéral américain (Federal Networking Council – FNC) qui regroupait, entre autres, des membres du département de la Défense des États-Unis (Department of Defense – DoD), de l'Administration nationale de l'aéronautique et de l'espace (National Aeronautics and Space Administration – NASA) et de la Fondation nationale pour la science (National Science Fondation – NSF)14. De nos jours, environ 40 trillions de courriels sont envoyés annuellement et la toile contient plus de 30 trillions de sites15. La compagnie Cisco, qui produit la majorité des éléments générant l'infrastructure internet, estime qu'en 2012, il y a eu 8,7 milliards de composantes connectées à

---

14 Internet Society, « Brief History of the Internet », consulté le 4 février 2014, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

internet et qu'il y en aurait 40 milliards d'ici 2020, incluant les voitures, les réfrigérateurs, des composantes médicales et autres gadgets qui ne sont pas encore inventés16. En préambule à la Stratégie de cybersécurité du Canada, le cyberespace est défini comme « […] un bien commun reliant plus de 1,7 milliard de personnes qui échangent des idées et des services et qui tissent des liens d'amitié »17. Parallèlement, l'éditeur du magazine *Wired* Ben Hammersley, établit une définition forte et bien réelle de l'espace cybernétique [Traduction] « […] C'est la plateforme centrale des affaires, de la culture et des relations personnelles. Il ne reste plus beaucoup de place pour le reste […]. Internet n'est pas un luxe additionnel à notre existence, pour la majorité des gens aujourd'hui, internet c'est leur vie »18.

Internet se situe plus en plus au sein des infrastructures essentielles et contribue fortement à notre prospérité et notre bien-être quotidien.

Infrastructures essentielles

Le gouvernement canadien définit les infrastructures essentielles comme :

> […] l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la

---

15 30 trillion individual web pages, « How Search Works », consulté le 4 février 2014, http://www.google.com/intl/fr/insidesearch/howsearchworks/thestory

16 Forbes, « How Many Things Are Currently Connected To The "Internet Of Things" (OIT)? », consulté le 4 février 2014, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/

17 Sécurité publique Canada, *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité* (Ottawa : Groupe Communication Canada, 2010), p.1, consulté le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fra.pdf

18 Ben Hammerseley, « My speech to the IAAC », (discours, Information Assurance Advisory Council, Londres, GB, septembre 2011), consulté le 4 février 2014, http://benhammersley.com/2011/09/my-speech-to-the-iaac/

> sécurité ou le bien-être économique des Canadiens et des Canadiennes ainsi que l'efficacité du gouvernement19.

De plus, il classe les infrastructures critiques parmi les dix catégories suivantes : énergie et services publics, finance, alimentation, transport, gouvernement, technologies de l'information et de la communication, santé, eau, sécurité, secteur manufacturier20. L'envergure des interrelations entre tous ces réseaux et systèmes connectés crée un environnement de dépendance mutuelle où, par exemple, le système d'alimentation et d'énergie dépend de l'efficacité du réseau de transport. Ensuite, presque tous les secteurs croisent les frontières publiques-privées et atteignent plusieurs couches gouvernementales, c'est-à-dire, fédérales, provinciales et municipales, soulevant la juridiction à son niveau le plus complexe. De plus, plusieurs de ces secteurs sont virtuellement connectés à l'infrastructure américaine. Implicitement, cette interdépendance apporte une obligation de collaborer avec nos voisins du sud21. La panne de courant nord-américaine de 2003 est représentative de cette corrélation où 50 millions d'abonnés ont été privés d'électricité. D'origine américaine, cette panne a eu un impact substantiel sur l'économie de l'Ontario qui a vu son produit intérieur brut chuter de 0,7% en août 200322.

---

19 Sécurité publique Canada, *Stratégie nationale sur les infrastructures essentielles* (Ottawa : Groupe Communication Canada, 2010), p. 2, consulté le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-fra.pdf

20 *Ibid*., p. 6.

21 Eric Cyr, « Strengthening the cybersecurity of critical infrastructure : The need of a targeted legislative reform » (travail redigé dans le cadre du Programme de commandement et d'état-major interarmées, Collège des Forces canadiennes, 2013), p. 7.

22 U.S.-Canada Power System Outage Task Force, « Final Report on the August 14, 2003 Blackout in the United States and Canada : Cause and Recommendations », p. 1, consulté le 4 février 2014, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

En mars 2007, l'expérience « Aurora » conduite au laboratoire national d'Idaho du département de l'Énergie des États-Unis avait pour objectif de confirmer s'il était possible de faire exploser une génératrice électrique de 27 tonnes en n'utilisant rien d'autre qu'un ordinateur et une connexion à internet. Des scientifiques, situés à plusieurs kilomètres du laboratoire, ont réussi à outrepasser la sécurité pour entrer dans le système informatique et prendre contrôle de la génératrice. En quelques minutes, la génératrice a explosé suite à des demandes d'ouvertures et de fermetures excessives de ses circuits. L'expérience a, par le fait même, démontré que d'autres génératrices de la sorte pourraient aussi être la cible d'attaques cybernétiques. Puisque ces modèles de génératrices sont fabriqués à l'extérieur des États-Unis et prennent plusieurs mois à être remplacés, une attaque synchronisée de la part de pirates informatiques pourrait priver d'électricité une région complète du pays pour quelques mois23. À travers les États-Unis comme au Canada, le système de contrôle et d'acquisition de données (Supervisory Control and Data Acquisition - SCADA) est utilisé, comme dans l'expérience « Aurora », pour contrôler les génératrices, les pompes et tous autres systèmes qui propulsent la majorité des infrastructures majeures au service du pays et de sa population24. Bien que SCADA procure beaucoup d'avantages économiques, cette expérience démontre très clairement la fragilité de sa configuration. À la lumière des conséquences d'une panne de courant similaire à celle d'août 2003, il devient évidemment crucial que les infrastructures essentielles soient considérées parmi les priorités du gouvernement.

---

23 Joel Brunner, *America the Vulnerable* (New York : The Penguin Press, 2011), p. 93.

24 National Communications System, Supervisory Control and Data Acquisition (SCADA) Systems (Arlington, VA : Office of the Manager National Communications System, octobre 2004), p.11.

Un article publié en 2009 dans le magazine *Forbes* illustre bien un scénario impliquant plusieurs pannes d'infrastructures essentielles pour le citoyen moyen [Traduction] :

> D'abord votre téléphone cellulaire ne fonctionne pas. Ensuite, vous remarquez que vous ne pouvez plus accéder à Internet. Dans la rue, les guichets automatiques ne distribuent pas d'argent. Les feux de circulation ne fonctionnent pas, et les appels au 911 ne sont pas proprement acheminés aux intervenants d'urgence. La radio annonce en onde que les systèmes de contrôle des barrages, chemins de fer et les centrales nucléaires ont été infiltrés à distance et compromis. Le système de contrôle du trafic aérien s'arrête, laissant des milliers de passagers bloqués, déroutés et incapables de communiquer avec leurs proches. Il s'ensuit une panne d'électricité majeure qui perdure pendant des jours et même des semaines. Notre civilisation numérique frémit face à cet arrêt. Lorsque nous revenons enfin à la réalité, des millions de données des Américains sont absentes de même que des milliards de dollars de crimes ont été perpétrés.25

En 2010, le Canada et les États-Unis ont publié le plan d'action canado-américain sur les infrastructures essentielles. Cette initiative devait permettre « […] au Canada et aux États-Unis de mieux gérer les risques en vue de renforcer la résilience des infrastructures essentielles des deux pays »26. Cependant, au Canada comme aux États-Unis, environ 85% de l'infrastructure critique appartient à l'industrie, aux provinces et aux agences non gouvernementales. Alors que le gouvernement a tendance à se concentrer davantage sur des problèmes stratégiques de haut niveau tels que les attaques terroristes et les catastrophes naturelles, l'industrie quant à elle détient un agenda beaucoup plus centré sur leur marge de profit. Par conséquent, les entreprises sont très réticentes à partager leurs informations critiques avec le gouvernement fédéral. Cependant, il faut viser qu'une relation de confiance à long terme s'installe entre les membres du

---

25 Forbes, « The Growing Cyberthreat », consulté le 4 février 2014, http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon.html

gouvernement et les sièges sociaux d'entreprises pour que celles-ci soient convaincues que leurs informations demeureront protégées avant de les partager27. De nos jours, la cybersécurité des banques de données du gouvernement fédéral représente un élément clé pour l'établissement de cette confiance mutuelle.

En résumé, toutes les infrastructures essentielles qui caractérisent notre civilisation moderne, du commerce aux communications, en passant par les réseaux électriques et de télécommunications, les systèmes bancaires et de fabrication, les réseaux de transport et les services gouvernementaux opèrent dans ce qui est maintenant un réseau global d'un nombre infini de réseaux. Dans un tel contexte, la surveillance des activités à l'intérieur de ce monde virtuel doit être continue, dynamique et polyvalente, contribuant à un mode d'action décisif au maintien de la prospérité économique, mais surtout, à la liberté des habitants de notre planète.

Acteurs du cybermonde

Un nombre infini d'acteurs influencent la virtualité de ce monde intangible. Certains ont un rôle de premier ordre tels que les états et les organismes de gouvernance d'internet, alors que d'autres comme les usagers, ont un rôle de second plan. Cependant, tous interagissent à leur façon pour combiner un monde tantôt convivial, tantôt hostile et imprévisible. La Stratégie de cybersécurité du Canada introduit plusieurs acteurs cruciaux dont le gouvernement fédéral, les

---

26 Sécurité publique Canada, *Plan d'action canado-américain sur les infrastructures essentielles* (Ottawa : Groupe Communication Canada, 2010), p. 3, consulté le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/cnd-ntdstts-ctnpln-fra.pdf

27 Andrew Graham, The Macdonald-Laurier Institute, « Canada's Critical Infrastructre : When is Safe Enough Safe Enough? », p. 8, 21-22, consulté le 4 février 2014, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

gouvernements des provinces et des territoires, le milieu universitaire, les organismes non gouvernementaux, le secteur privé, le secteur des infrastructures essentielles et la population canadienne28. Aux acteurs canadiens il faut ajouter les acteurs internationaux tels que tous les autres pays connectés sur internet et les organismes de gouvernance du cybermonde dont la Société pour l'attribution des noms de domaine et des numéros sur internet (Internet Corporation for Assigned Names and Numbers – ICANN), le Détachement d'ingénierie d'internet (Internet Engineering Task Force – IETF) et le registre internet régional (Regional Internet Registry – RIR). Créée en 1992, la Société d'internet (Internet Society – ISOC) est une association de droit américain qui apporte un soutien organisationnel et financier à l'IETF. En 2005, ISOC est devenue l'autorité morale et technique la plus influente dans l'univers d'internet. Elle obtient entre autres une accréditation au Conseil économique et social des Nations unies29. Depuis quelques années, ces organismes de gouvernance sont joints par une variété de forums internationaux tels que le G8, le G20, l'OCDE, l'Organisation pour la sécurité et la coopération en Europe (Organization for Security and Co-operation in Europe – OSCE), ainsi que l'UNESCO et l'Assemblée générale des Nations unies. L'élaboration d'un glossaire sur la gouvernance de l'internet destiné à la communauté arabophone est un exemple de ce partenariat30. Bien que certains organismes reconnus mettent en place des paramètres d'utilisation de l'internet, il n'en demeure pas moins que le manque de législation reste un enjeu

---

28 Sécurité publique Canada, *Stratégie de cybersécurité du Canada*…, p.7-13.

29 Internet Society, « Que faisons-nous », consulté le 4 février 2014, http://www.internetsociety.org/fr/que-faisons-nous/influence

capital pour la majorité des pays qui favorisent ouvertement une utilisation saine et sécuritaire de cette dimension pour tous les usagers.

Le monde politique

De manière générale, tout ce qui touche le cybermonde a été pendant longtemps très loin des priorités des diverses couches politiques, laissant libre champ aux spécialistes des technologies de l'information. Ainsi, comme le décrit l'auteur Mark Bowden dans *Worm : The First Digital World War*, lorsque ces spécialistes parlent, l'entourage adhère un visage qu'il symbolise par le « glaze ». C'est-à-dire un profond regard troublé causé par un manque total d'intérêt. « Glaze » devient votre visage lorsque « stuff » est la seule définition que vous connaissiez d'un sujet particulier, d'où l'origine de l'appellation « cyber stuff »31. Il est en de même de l'anecdote rapportée par Peter Singer et Allan Friedman, auteurs de *Cybersecurity and Cyberwar : What Everyong Needs to Know*, lorsqu'il raconte qu'ils ont été approchés par un politicien américain, responsable des négociations avec la Chine concernant le cybermonde, afin de connaître ce qu'était un fournisseur d'accès à internet (Internet Service Provider – ISP)32. Ne pas connaître ce qu'est un ISP aujourd'hui lors de négociations impliquant les deux plus grandes puissances du cybermonde est l'équivalent de ne pas avoir connu au temps de la guerre froide, lors des négociations sur la prolifération d'armes nucléaires avec l'URSS, ce qu'était un missile balistique intercontinental (intercontinental ballistic missile – ICBM).

---

30 ICANN, «L'UNESCO, l'ICANN et l'ISOC lancent une initiative pour l'élaboration d'un glossaire sur la gouvernance de l'Internet destiné à la communauté arabophone », consulté le 4 février 2014, http://www.icann.org/fr/news/announcements/announcement-27oct13-fr.htm

31 Mark Bowden, *Worm : The first Digital World War* (New York : Atlantic Monthly Press, 2011), p. 7.

En 2012, dans une allocution au Sommet de cybersécurité de Washington, DC, Janet Napolitano, alors secrétaire à la Sécurité intérieure des États-Unis (United States Secretary of Homeland Security), a mentionné qu'elle n'utilisait pas les courriels, non pas pour des raisons de sécurité, mais parce que ces derniers n'avaient aucune valeur ajoutée pour son travail33. De même, Elena Kagan, juge à la Cour suprême des États-Unis depuis le 7 août 2010, tient des propos semblables concernant l'utilisation des courriels pour huit de ses neuf juges. Ironiquement, ce sont ces analphabètes de la technologie qui ont le pouvoir de décider des politiques, une réalité qui est négligée encore aujourd'hui par le monde politique.

General Michael Hayden, ancien directeur de l'Agence centrale de renseignement (Central Intelligence Agency – CIA), fait la déclaration suivante concernant le manque de connaissances au niveau de la cybersécurité et du danger que cela représente [Traduction] :

> Rien auparavant n'a été aussi important, mais discuté avec autant d'inconsistance et d'incompréhension [...]. J'ai assisté à de très petites réunions de groupe à Washington [...] incapable (ainsi que mes collègues) de décider d'un plan d'action parce que nous n'avions pas une image claire des implications juridiques et politiques à long terme des décisions que nous pourrions prendre34.

Au mois d'août 2012, Ron Deibert, directeur du Centre canadien des études sur la sécurité mondiale de l'École Munk des Affaires internationales de l'Université de Toronto, a publié une étude sur la cybersécurité dans laquelle il mentionne que la sécurité du cybermonde est politique

---

32 Peter Singer et Allan Friedman, *Cybersecurity and Cyberwar : What everyone needs to know* (New York : Oxford University Press, 2014), p. 7.

33 Janet Napolitano, « Uncovering America's Cybersecurity Risk » (Conférence, « Arms race in Cyberspace? »,Newseum, Washington, DC, 28 septembre 2012), consulté le 5 février 2014, http://www.nationaljournal.com/events/cybersecurity-summit

34 Michael V. Hayden, « The Future of Things Cyber », *Strategic Studies Quartely* 5, no. 1 (printemps 2011), p. 3.

puisque les acteurs ne partagent pas tous la même perspective quant à la sécurité et la définition d'une menace. Cette perception du monde cybernétique n'est pas simplement conflictuelle à l'intérieur des acteurs d'un pays, mais à travers le monde entier. Pour les pays démocratiques comme les États-Unis et le Canada, internet est un domaine libre favorisant la prospérité économique et le bien-être des individus à travers les relations sociales et la liberté d'expression. Pour ces états, la cybersécurité joue autour de l'authentification et de l'intégrité du réseau. Pour d'autres pays à régime plus autocratique, cette liberté est beaucoup plus contrôlée. Dans ce cas, la cybersécurité est axée davantage sur la stabilité culturelle du pays et du régime politique en place35. De par cette division pourtant très simple des objectifs entre différents systèmes politiques, on peut déduire que le cybermonde est synonyme aujourd'hui de grandes distinctions, non seulement au sein des différents régimes politiques, mais au sein du secteur privé et des acteurs de la société civile qui dépendent de ce domaine. Tous veulent façonner cette dimension à leur avantage stratégique.

En 2011, une étude comparative de dix Stratégies de cybersécurité nationale a révélé des divergences dans la définition même du terme. Cette incohérence d'interprétation apporte un niveau additionnel de difficulté au niveau de la coopération internationale36. En effet, afin de régulariser internet, il est important de comprendre comment celui-ci fonctionne. En 2008, le

---

35 Ron Deibert, « Distributed Security as Cyber Strategy : Outlining a Comprehensive Approach for Canada in Cyberspace » (Reseach Paper prepared for the Canadian Defence & Foreign Affairs Institute, Toronto University, 2012), p. 1.

36 H.A.M. Luiijf, et coll., « Ten National Cyber Security Strategies : A comparison », *Critical Information Infrastructure Security*, Volume 6983 (Heidelberg : Springer, 2013), p. 3, 15.

gouvernement du Pakistan a ordonné la compagnie de télécommunication Pakistan Telecom d'empêcher l'accès au site « offensant » YouTube. Pour y arriver, la compagnie a mis en marche une fausse campagne de publicité qui précisait que la route virtuelle la plus directe pour aller sur YouTube était à travers Pakistan Telecom. Ainsi, à travers ses installations, cette tactique permettait à la compagnie d'exécuter les ordres du gouvernement. Cependant, la campagne s'est propagée à un point tel que les deux tiers des usagers mondiaux d'internet étaient redirigés vers cette fausse location de YouTube, ce qui eut pour effet de créer une véritable congestion virtuelle sur l'infrastructure de Pakistan Telecom37. Ce sont les ingénieurs de Google qui ont fait une campagne agressive sur l'internet afin de rediriger les usagers vers la véritable adresse de YouTube et mettre fin à ce problème basé sur de fausses informations.

Bien que pour l'instant il soit difficile d'arriver à un consensus envers une définition, Eric A.Fisher, spécialiste au sein de la branche de science et technologie de la division des ressources, science et industrie du Service de recherche du Congrès (Congressional Research Service – CRS), apporte trois éléments essentiels pour définir la cybersécurité [Traduction] :

1. C'est un ensemble d'activités entreprises pour protéger les ordinateurs, les logiciels et les réseaux contre les attaques, la perturbation ou d'autres menaces. Ces activités peuvent aller du contrôle de sécurité et d'accès, aux systèmes de surveillance et de récupération à la mise en œuvre de barrières de sécurité

37 Martin Brown et Earl Zmijewski, « Pakistan Telcom Hijacks YouTube : Or how to SYN-flood DOS yourself while annoying everyone on the planet », APRICOT TAPEI 2008 educational conference, consulté le 5 février 2014, http://www.renesys.com/wp-content/uploads/2013/05/apricot-lightning-08.pdf

physiques ainsi qu'à l'éducation des usagers sur les défis de sécurité du cybermonde.

2. Un sentiment d'être à l'abri des attaques cybernétiques.
3. L'ampleur des activités relatives à l'amélioration de la sécurité pour inclure la qualité de la protection, la recherche et le développement ainsi que des analyses détaillées38.

L'ajout des diverses couches de surveillance par le gouvernement, au travail et même à la maison, est de plus en plus toléré. Des nations complètes frôlent même une certaine paranoïa. Ainsi, la Chine développe présentement son propre réseau de compagnies derrière un gigantesque pare-feu afin que le gouvernement puisse consulter tous les messages entrant et si requis, débrancher d'internet le réseau en entier. Tel que mentionné dans un article publié par le Yale Law School, ces mesures de sécurité contreviennent à la raison d'être et aux valeurs traditionnelles d'internet, soit la collaboration, l'innovation et l'échange d'idées dans un domaine libre et sous contrôle limité du gouvernement39. Un niveau trop élevé de sécurité se transforme à un contrôle excessif et s'éloigne des avantages que procure internet.

Tous ces aspects de sécurité ne sont pas seulement techniques, ils sont aussi organisationnels, juridiques, économiques et sociaux. De plus, la sécurité s'obtient avec un coût

---

38 Eric A. Fisher, « Creating a National Framework for Cybersecurity : An analysis of Issues and Options », *Cybersecurity and Homeland Security* (New York : Nova Science Publishers, 2005), p. 7.

39 Yale Law School, « Arms race in Cyberspace? », *Rebekka Bonner's blog* (blogue), consulté le 5 février 2014, http://www.yaleisp.org/2011/05/arms-race-in-cyberspace

financier, mais surtout, avec un échange contre la liberté des usagers. Enfin, malgré tout ce qui pourrait être sacrifié pour augmenter la sécurité, il n'existe pas de sécurité absolue au niveau de l'informatique, tout comme c'est le cas dans le monde physique.

Les usagers

Pour plusieurs spécialistes du domaine, l'usager typique représente un fort pourcentage de leurs maux de tête et leur principale source de menace. Depuis 2008 Telus Security Solutions s'associe à la Rotman School of Management de l'Université de Toronto afin de produire une étude annuelle sur la sécurité informatique. Le rapport de 2013 est le produit de consultations avec des professionnels de l'informatique occupant des postes de direction à l'intérieur de plusieurs compagnies en importance au Canada. Tous s'accordent pour dire qu'ils ont subi ou subiront une brèche informatique, qu'ils soient en mesure de le détecter ou non. Avant tout, pour ces directeurs de la sécurité informatique, un de leur plus grand souci réside au niveau de la menace interne, soit avec leurs propres usagers. En effet, les secrets intellectuels des compagnies sont souvent révélés au grand jour par les employés de la compagnie, sans que ceux-ci ne se doutent de l'impact de leurs actions. L'éducation des usagers doit donc devenir proéminente au niveau des politiques des compagnies, spécialement en ce qui concerne la manipulation des données essentielles et des propriétés intellectuelles. De plus, l'éducation doit être proactive à l'aide des séances d'information au lieu d'être simplement passive sous forme de courriels de rappel. Ce dernier mode de fonctionnement a tendance à avoir un effet négatif sur les usagers qui, avec le temps, effacent les courriels sans même en prendre connaissance. Lors de l'étude de 2011, il a été démontré que les employés veulent bien se soumettre aux politiques tant et aussi

longtemps qu'ils en comprennent le sens, les risques associés avec la technologie et les raisons d'affaires qui la supportent40.

Ce qui n'a pas encore été détaillé et qui apporte l'amertume cybernétique, c'est-à-dire l'instabilité des usagers, du secteur privé et des infrastructures essentielles est la menace. Omniprésente et de plus en plus invisible, elle dépolarise les objectifs des créateurs de ce domaine prospère.

Les menaces

Arnold Ludwig, dans *The King of the Mountain*, mentionne qu'en plus de 3000 ans d'histoire documentée, l'humanité a vécu seulement 268 années sans guerre majeure. Malgré l'espoir et l'évolution qu'apporte l'âge de l'information, il n'en demeure pas moins que nous vivons aussi dans un monde d'anxiété cybernétique. En effet, selon un sondage rapporté dans *Foreign Policy* concernant l'avenir du monde, le cybermonde est considéré par les répondants comme la seule grande menace émergente de nos jours41. Pour sa part, le *Boston Globe* pousse encore plus loin puisqu'il considère que nous sommes déjà dans une guerre cybernétique en pleine croissance et que celle-ci culminera vers une guerre de tranchées cybernétiques

---

40 Hernan Barros et Walid Hejazi, *2013 Telus-Rotman IT Security Study*, p.3, 6, 8, consulté le 5 février 2014, http://www.telus.com/en_CA/content/pdf/whyTELUS/Rotman_2013_Full_Study.pdf?elq_mid=&elq_cid=1111327

41 David Tohn, « The FP Survey : The Internet », *Foreign Policy*, no. 188 (septembre-octobre 2011), p. 116.

extrêmement sanglante42. Joseph Nye, ancien membre du Pentagone et doyen à la Harvard Kennedy School of Government (HKS), estime que si les usagers perdent confiance en la sécurité et d'internet, ils vont se retirer du cybermonde et échanger leur bien-être pour la sécurité et de la stabilité43. Ces propos rejoignent ceux d'Eric Schmidt, actuellement à la tête de la firme Google, lors d'une conférence de programmeurs informatiques à San Francisco en 1997 [Traduction] « Internet est la première chose que l'être humain ait conçu et qu'il ne comprend pas, la plus grande expérience anarchique que nous ayons jamais vécue »44.

Associé à des frontières indéfiniment disputables se dresse un chaos favorable à qui veut bien en profiter. Ainsi, la menace peut être objective ou très subjective, d'où l'importance de comprendre si l'assaillant veut attaquer une cible en particulier ou simplement attaquer de façon aléatoire.

Classification des agressions

Un code malveillant sans cible précise pourrait, par exemple, infecter un ordinateur via un courriel et chercher des détails de cartes de crédit enregistrés dans la mémoire vive de l'ordinateur pour ensuite renvoyer ces informations à l'endroit d'origine du code malveillant. Les dépenses reliées à ce type d'attaque automatisée demeurent sensiblement les mêmes, peu importe le nombre de victimes. Par contre, une attaque ciblée va sensiblement augmenter les frais et le temps de préparation, mais en théorie, devrait augmenter les gains. Ce genre d'attaque cible des

---

42 boston.com, « Digital trench warfare », consulté le 5 février 2014, http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/06/11/digital_trench_warfare

43 Joseph S. Nye, « Power and National Security in Cyberspace », *America's Cyber Future : Security and Prosperity in the Informationoreign Age*, vol. 2 (Washington, DC : Center for a New American Security, 2011), p. 15.

44 Eric Schmidt et Jared Cohen, *The New Digital Age* (New York : Knopf, 2013), p. 263.

personnes et des compagnies avec un objectif très précis45. La bonne nouvelle pour l'usager moyen est qu'il n'existe que trois actions possibles contre un ordinateur : voler ses données, détourner son identité et confisquer ses ressources46. Ces actions sont certes catastrophiques pour l'individu, mais demeurent assez superficielles d'un point de vue sécurité nationale. Par contre, la dépendance des gouvernements aux banques de données informatiques fait qu'une perte de données pourrait révéler tous les plans stratégiques d'un état. De même, un assaillant qui vole l'identité d'une entreprise lui donne la possibilité de changer des codes maîtres et ainsi altérer la liste des employés ou même ouvrir un barrage électrique. Le fait de confisquer des ressources à une entreprise pourrait l'empêcher de rejoindre ses clients voire même à l'extrême, de réduire la capacité des membres d'une armée de communiquer entre eux. Dans tous les cas, pour que de telles situations se produisent, il doit y avoir un être humain derrière qui l'appuie et l'initie.

Dans un travail de recherche concernant les menaces cybernétiques potentielles envers les États-Unis, Andrew Cutts, du département de la Sécurité intérieure des États-Unis (United States Department of Homeland Security - DHS), propose un continuum des risques cybernétiques nationaux. Tel que démontré à la figure 2.1, les menaces varient du plus dangereux, impliquant un état, au plus nuisible, s'associant à un pirate informatique47.

---

45 Cormac Herley, « The Plight of the Targeted Attacker in a World of Scale », *Microsoft Research* (Redmond, WA, 2010), consulté le 5 février 2014, http://research.microsoft.com/pubs/132068/TargetedAttacker.pdf

46 Singer et Friedman, *Cybersecurity and Cyberwar*…, p. 39.

47 Andrew Cutts, « Warfare and the Continuum of Cyber Risks : A policy Perspective » *The virtual Battlefield : Perspective on Cyber Warfare* (Fairfax : IOS Press, 2009), p. 66-76.

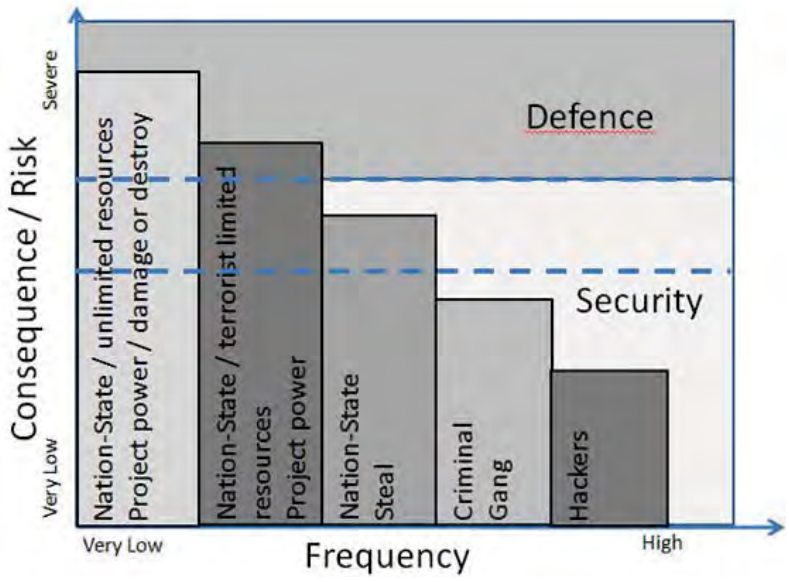


Figure 2.1 – Continuum des risques cybernétiques nationaux

Source: Diagramme adapté d'Andrew Cutts, « Warfare and the Continuum of Cyber Risks : A policy Perspective »

De même, plusieurs états tels que la Russie, Israël, la Chine, l'Inde, la France, la Corée du Sud et les États-Unis, ont déjà ouvertement déclaré que la guerre cybernétique faisait partie intégrante de leur stratégie militaire et qu'elle était intégrée à d'autres opérations de renseignement afin d'attaquer l'équipement militaire et les opérations de leurs adversaires48. Ainsi, au moment d'entrer en Géorgie en 2008, la Russie a orchestré une attaque par déni de

48 Derek S. Reveron, *Cyberspace and National Security : Threats, Opportunities, and Power in a Virtual World* (Washington, D.C. : Georgetown University Press, 2012), p. 173-189, 191-205; ZDNet, « South Korea army, university to start cyberdefense major », consulté le 5 février 2014, http://www.zdnet.com/south-korea-army-university-to-start-cyberdefense-major-2062300991/ ;

service (distributed denial-of-service – DDoS) contre les réseaux du ministère de la Défense du pays. En 2010, Israël s'est associé aux États-Unis afin de ralentir le programme nucléaire de l'Iran. Ensemble, ils ont créé le virus Stuxnet, le plus performant de l'histoire informatique. L'objectif était que les Iraniens attribuent le malfonctionnement des centrifugeuses d'une centrale nucléaire, à des pièces défectueuses, des erreurs de configuration ou simplement à leur incompétence. Le virus Stuxnet ciblait les centrifugeuses de la centrale de Natanz, dont il perturbait légèrement le fonctionnement, entraînant la destruction de plusieurs centaines d'entre elles. L'administration Obama évalue que ce virus a permis de retarder le programme nucléaire iranien de 18 mois à 2 ans49. Ces exemples démontrent bien que déjà les attaques cybernétiques existent au-delà du privé et du commercial et qu'elles sont utilisées par un état contre un autre état.

Les groupes terroristes constituent un autre groupe en importance quant aux menaces cybernétiques. Selon DoD, les groupes terroristes développent sans relâche leurs capacités cybernétiques ainsi que leur doctrine au niveau de la planification, du recrutement, des levés de fonds et de la propagande. Al-Qaeda et Hezbollah ont déjà indiqué leurs intentions de conduire des attaques cybernétiques contre les pays occidentaux50. Les organisations criminelles

---

CBN News, « Israel Building "Digital Iron Dome" », consulté le 5 février 2014, http://www.cbn.com/cbnnews/insideisrael/2012/October/Israel-Building-Digital-Iron-Dome/

49 Derek S. Reveron, *Cyberspace and National Security*…, p. 148-150.; Le Nouvel Observateur, « Stuxnet : Comment les États-Unis et Israël ont piraté le nucléaire iranien », consulté le 5 février 2014, http://rue89.nouvelobs.com/2012/06/04/stuxnet-comment-les-etats-unis-et-israel-ont-pirate-le-nucleaire-iranien-232728 ; Holly Porteus, *The Stuxnet Worm : Just Another Computer Attack or a Game Changer?* (Ottawa : Library of Parliement, 2010), p. 1.

représentent également une menace notamment pour le vol d'identités, le blanchiment d'argent, l'extorsion et le vol de propriétés intellectuelles et de secrets industriels51.

En relation étroite avec l'analyse des risques et le continuum de Cutts, Wesley Wark, professeur à l'École Munk des affaires internationales de l'Université de Toronto fait la distinction entre quatre grandes familles d'attaques sur internet, soit la cyberguerre, le cyberterrorisme, le cybercrime et le cyberespionnage, qui représentent des dangers actuels. De plus, il précise que le secteur privé est plus touché par le cybercrime alors que sont les états qui jouent un rôle de premier plan au niveau de la cyberguerre et du cyberespionnage. Le cyberterrorisme se définirait au fur et à mesure que les groupes terroristes approfondissent leurs connaissances et utilisent à leur avantage le potentiel qu'offre le cybermonde52.

Pour Wark, le cyberespionnage implique des actions offensives et défensives. Du côté défensif, ou du contre-espionnage cybernétique, le mode d'opération implique l'utilisation de vieilles méthodes datant de la guerre froide comme les mesures de protection physique et virtuelle afin d'empêcher l'accès et la manipulation des données par du personnel non autorisé. De plus, et tel qu'expliqué dans les sections précédentes, la sensibilisation des usagers demeure la clé contre le cyberespionnage. Une autre source de protection provient des nombreuses années d'expérience avec les systèmes de renseignement et l'application des lois.

---

50 United States Army Training and Doctrine Command, *Cyber Operations and Cyber Terrorism*, DCSINT Handbook no. 1.02, (Fort Leavenworth, Kansas : Deputy Chief of Staff for Intelligence, 2005), p. 14-16.

51 Business Insider, «Organized Crime Hackers Are The True Threat To American Infrastructure», consulté le 5 février 2014, http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3

52 Wesley Wark, « Cyber-Agression and its Discontents », *Global Brief* (Fall 2012), p. 36.

En ce qui a trait aux actions offensives, l'utilisation du renseignement d'origine électromagnétique (Signals Intelligence – SIGINT) en collaboration avec les outils de renseignement d'origine humaine (Human Intelligence – HUMINT), de renseignement d'origine image (Imagery Intelligence – IMINT) et de renseignement d'origine source ouverte (Open Source Intelligence – OSINT) procurent ce que l'on appelle le renseignement cybernétique53. Nécessairement, la coordination de toutes ces ressources est requise afin que la collecte de toutes ces données procure en fin de compte de l'information pertinente aux personnes concernées. De même, la coordination et la consolidation de tous les efforts sous un même commandement revêtent une importance capitale dans le cadre des FAC.

Par ailleurs, Daniel Ventre, chercheur au Centre de recherches sociologique du droit et des institutions pénales (CESDIP) et professeur à Telecom ParisTech, mentionne dans son ouvrage *La guerre de l'information* que sur papier, une attaque sur l'information peut paraître efficace et puissante. Toutefois, ces attaques ont leurs limites en termes d'utilité et d'efficacité. En effet, ce type d'attaque exige non seulement de posséder des informations et des connaissances de haute qualité sur la cible visée, mais également d'être en mesure d'analyser de façon presque permanente les cibles potentielles. En plus, attaquer la vulnérabilité des systèmes n'est pas nécessairement la meilleure stratégie. Les attaques contre les systèmes d'information doivent viser la volonté de l'ennemi, sa capacité à se battre et la dissuader. Mais elles n'offrent pas la possibilité de contrôler tout un territoire.54

---

53 *Ibid*., p. 37.
54 Daniel Ventre, *La guerre de l'information* (Paris : Lavoisier, 2007), p. 221.

Malgré le regard plus optimiste de Daniel Ventre sur la menace cybernétique, il n'en demeure pas moins que lorsqu'un état ou une entreprise subit une brèche dans sa sécurité informatique, la plupart du temps il en découle des conséquences importantes.

Une brèche qui fait mal

Dans une entrevue à Radio-Canada, Daniel Tobok propriétaire d'une compagnie conduisant des enquêtes d'ampleur internationale en relation avec la cybersécurité, fait le lien entre la plus grande brèche informatique qu'a connu le gouvernement canadien et la transaction infertile (évaluée à 38 milliards de dollars), de tentative d'achat de la Potash Corporation de Saskatchewan en août 2010 par la compagnie australienne BHP Billiton. La Chine, un des plus grands consommateurs d'engrais à base de potasse, était irrévocablement contre cette transaction qui aurait mis le principal producteur d'engrais au monde entre les mains de BHP Billiton. Cette brèche informatique, qualifiée de la plus imposante de l'histoire du Canada par Daniel Tobok, non seulement parce qu'elle a touché plusieurs cibles canadiennes, mais également parce que son empreinte était associée à des adresses IP chinoises qui provenaient de plus d'une centaine de pirates informatiques différents. Cette infiltration a frappé plusieurs firmes d'avocats industriels représentant Potash Corporation et a donné un dur coup à plusieurs agences gouvernementales canadiennes, dont Recherche et développement pour la défense Canada (RDDC) ainsi que les deux centres nerveux de l'économie canadienne, soit le Secrétariat du Conseil du Trésor (SCT) et le ministère des Finances. Plusieurs documents à caractère sensible ont été volés et plusieurs comptes privilégiés ont été infiltrés. À la suite de cette nouvelle, les différentes agences

gouvernementales visées par cette attaque ont été débranchées d'internet jusqu'à ce que la reconnexion soit considérée sécuritaire, soit presque un an plus tard55.

En 2008, les réseaux appartenant au DoD ont également connu une infiltration de ses systèmes informatiques avec l'insertion d'une clé USB dans un de leurs ordinateurs au Moyen-Orient. Introduite par une agence étrangère du renseignement, la clé USB contenait un logiciel malveillant qui s'est téléchargé à l'intérieur d'un réseau opéré par le Commandement central américain (United States Central Command – CENTCOM). Ce logiciel malveillant s'est répandu de manière imperceptible sur les réseaux classifiés et non-classifiés de la Défense américaine, établissant une tête de pont à partir de laquelle les données pouvaient être transférées à des serveurs hébergés à l'étranger. Cet incident, considéré comme la brèche la plus importante des réseaux militaires américains, a servi de leçon au Pentagone. L'Opération « Buckshot Yankee » qui s'en est suivi a marqué un point tournant dans la stratégie de cyberdéfense des États-Unis56.

L'ère cybernétique à un point critique de l'histoire

La menace cybernétique n'a pas la même portée existentielle que la menace nucléaire, cependant, il existe d'importantes similitudes. Ainsi, tel que le reconnaissait Robert McNamara, secrétaire à la Défense des États-Unis entre 1961 et 1968, sans stratégie tangible pour l'utilisation des armes nucléaires, il existait un risque réel de s'annihiler soi-même en même temps que l'adversaire. Dans ces années, le Commandement des Forces aériennes stratégique (Strategic Air Command – SAC) avait un plan très simple pour l'utilisation des armes nucléaires

---

55 CBC News, « Foreign hackers targeted Canadian firms », consulté le 5 février 2014, http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810

56 William J. Lynn III, « Defending a New Domain : The Pentagon's Cyberstrategy », *Foreign Affairs* Volume 89, no. 5 (septembre/octobre 2010), p. 97.

qui consistait à propulser des missiles contre les cibles en URSS, en Chine et aux états du Pacte de Varsovie advenant une attaque imminente de la part de l'URSS. Horrifié par un tel plan dévastateur, McNamara a développé, au temps de l'administration Kennedy, une stratégie de dissuasion qui incluait entre autres l'escalade de la force, le contrôle de l'armement nucléaire ainsi que l'interdiction d'attaquer des populations urbaines. Cette stratégie, diffusée à travers des élocutions publiques du président Kennedy et par des travaux universitaires de l'institut de technologie du Massachusetts (Massachusetts Institute of Technology – MIT) a incontestablement permis d'éviter une guerre nucléaire qui aurait pu tuer des centaines de millions d'êtres humains57.

Aujourd'hui avec l'espace cybernétique, nous sommes à un point critique similaire de l'histoire de l'humanité. Alors qu'en 1960, les missiles balistiques à longue portée pouvaient atteindre Moscou du Wyoming en seulement 35 minutes, aujourd'hui on voyage à la vitesse de la lumière à l'intérieur de l'espace cybernétique. Richard Clarke, conseiller spécial du président George W. Bush au niveau de la guerre cybernétique, évoquait [Traduction] « [que si] un commandant n'attaque pas assez rapidement, son réseau sera probablement détruit en premier. Si un commandant n'anticipe pas un ennemi, il fera face à de nouvelles défenses ou à un état cible déconnecté de l'internet58 ». La rapidité du cycle décisionnel des commandants militaires de niveau stratégique est donc critique lorsque vient le temps d'agir à l'intérieur du cybermonde, un

---

57 Richard Clarke, « War From Cyberspace », *The National Interest* (novembre/décembre 2009), p. 31-32.

58 *Ibid*., p. 32.

autre argument en faveur de l'amalgame des ressources cybernétiques des FAC sous un même commandement.

Résumé du chapitre

L'ère cybernétique, arrivée de façon inopinée, mais accueillie à bras ouvert par la majorité des pays démocratiques pour entre autres des raisons de bien-être et de prospérité économique, défie maintenant les frontières de l'imaginable par la complexité de ses intervenants. Pour les fondateurs d'internet, l'objectif primaire était d'avoir un médium d'échange d'information sans frontière et sans réglementation de la part des divers paliers de gouvernement. Puisqu'il y a toujours deux côtés à la médaille, les âmes pures à l'origine d'internet se sont rapidement fait rattraper par les vilains esprits, les profiteurs, les voleurs, les criminels et les extrémistes. Jamais un endroit n'a été, à la fois, aussi contesté et incompris que l'espace cybernétique. Peu de personnes en position d'autorité comprennent l'ampleur de la cyberdéfense et de sa juridiction. De même, la position des hommes politiques et de loi diffère d'un pays à l'autre, ce qui rend extrêmement difficile d'imposer des sanctions, spécialement lorsqu'une attaque ou une infiltration est d'origine internationale ou subventionnée par un gouvernement d'un pays étranger.

Pour le GC, il est urgent d'agir pour assurer la sécurité de ses citoyens. Pour être efficace à l'intérieur du continuum des risques cybernétiques, il se doit aussi d'agir en collaboration et d'unifier les efforts de ses différents intervenants. Avec un environnement de sécurité de plus en plus complexe, les FAC doivent aussi avoir le même degré d'implication. Tel que décrit dans les quatre types d'agression cybernétique de Wesley Wark, les FAC doivent mettre en place des approches globales, intégrées, flexibles et réseautées en vue d'implanter les politiques de sécurité

du Canada. Ces facteurs doivent devenir les principes régissant le modèle des FAC de l'avenir pour qu'elles soient pertinentes au plan stratégique, réactives sur le plan opérationnel et décisives du point de vue tactique59.

Pour ce faire, des changements majeurs s'imposent au niveau de la structure des FAC afin de devenir un joueur influent de la cyberdéfense. Le prochain chapitre se penche sur la situation actuelle du Canada et des FAC dans le cybermonde, et à titre comparatif, pose un regard sur la situation des forces alliées.

CHAPITRE 3 – LE CANADA ET SES ALLIÉS

À l'automne 2012, le Bureau du vérificateur général du Canada a publié un audit de performance afin de déterminer si les ministères et organismes fédéraux, impliqués dans le développement de la sécurité cybernétique, surtout suite à la publication en 2010 de la Stratégie de cybersécurité du Canada, travaillaient de concert avec les provinces, les territoires et le secteur privé pour protéger l'infrastructure essentielle du Canada contre les cybermenaces. Ce rapport indique entre autres :

> [qu'] en 1996, le gouvernement fédéral a reconnu que les systèmes nécessaires au fonctionnement de l'infrastructure essentielle du Canada pourraient être la cible de cyberattaques et qu'il avait un rôle à jouer dans la protection de ces systèmes contre de telles attaques. En 1999, le Comité spécial du Sénat sur la sécurité et les services de renseignements a recommandé, dans un rapport, que le gouvernement procède à l'examen de sa capacité d'évaluer et de réduire les vulnérabilités de l'infrastructure, de prévenir les attaques matérielles et cybernétiques et d'intervenir le cas échéant60.

---

59 Ministère de la Défense nationale, A-FD-005-002/AF-002, *Concept cadre intégré* (Winnipeg : Bureau de publications de la 17e Escadre, 2009), p. 2, consulté le 5 février 2014, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-fra.pdf

Tel qu'indiqué au chapitre précédent, presque la totalité des entreprises canadiennes a récemment été la cible d'attaques cybernétiques. De même, M. Jim Robbins, président de la compagnie « Electronic Warfare Associates – Canada (EWA-Canada) » signale que [Traduction] « au courant des dernières années […] le nombre de brèches informatiques majeures au sein des grandes entreprises a augmenté de manière significative […] ». Toutefois, seulement une faible partie des infractions est rapportée officiellement. Par conséquent, il devient difficile d'estimer de façon précise l'ampleur de la menace sur les infrastructures essentielles canadiennes. De fait, le Canada est très en retard quant à sa capacité de centraliser, au sein d'un organisme central ou d'un comité responsable de la sécurité cybernétique, l'enregistrement et la consolidation des cyberattaques et ainsi être en mesure d'obtenir des rapports chiffrés et précis. Il est d'ailleurs le seul pays du G8 qui ne dispose pas d'un tel système de collecte des données sur les menaces cybernétiques61.

La peur du cybermonde s'est accompagnée d'une prospérité économique et qui a vu la création d'une multitude d'entreprises en cybersécurité à travers le monde. Aux États-Unis, cela s'est traduit également par la création d'imposantes bureaucraties gouvernementales dont la Division nationale de cybersécurité du département de la Sécurité intérieure (United States Department of Homeland Security's Office of Cybersecurity and Communications – CS&C).

---

60 Bureau du vérificateur général du Canada, « Protéger l'infrastructure canadienne essentielle contre les cybermenaces », *Rapport du vérificateur général du Canada* (Ottawa : Groupe Communication Canada, 2012), p. 6, consulté le 4 mars 2014, http://www.oag-bvg.gc.ca/internet/Francais/parl_oag_201210_03_f_37347.html

61 Mr Robbins is President of EWA-Canada, a Systems Engineering Company which addresses the business and security risks inherent in the use of information technology and helps clients solve their most complex problems related to Information Management, Identity Management and Information Technology Security. Refer to Standing Senate Committee on

Ces différents organismes ont doublé et même parfois triplé leurs effectifs depuis leur institutionnalisation en 2006.

Au Canada, plusieurs acteurs influencent la sécurité à l'intérieur de l'espace cybernétique dont l'industrie privée, les FAC, Sécurité publique Canada (SP), Services partagés Canada (SPC), Industrie Canada (IC) et CSTC. Avec autant d'acteurs en jeu, une coopération entre le secteur privé et le secteur public devient d'une importance capitale afin de préserver la sécurité, le bien-être et la prospérité des Canadiens.

Contrairement à la terre, la mer, l'air et l'espace, l'espace cybernétique n'est pas actuellement une dimension officiellement couverte par la Défense nationale. De même, les politiques en matière de cybersécurité tardent à s'imposer alors que les différentes brèches sur la vie privée des gens, les données des entreprises et des gouvernements, amènent de plus en plus les pays à se pencher sur cette nouvelle réalité. Comme dans tout autre aspect de la sécurité du Canada, les FAC ont certainement leur rôle à jouer pour préserver la sécurité de l'espace cybernétique. Par contre, comme institution elle se doit d'être déterminée.

Le présent chapitre dressera un tableau de la situation du Canada au niveau de la cyberdéfense. La comparaison entre la vision et la volonté des dirigeants politiques avec ce qui, dans les faits, a été réalisé jusqu'à présent en matière de cyberdéfense permettra de faire ressortir plus clairement les lacunes qui existent actuellement au niveau de la sécurité cybernétique de notre pays. Par la suite, nous analyserons plus spécifiquement la structure organisationnelle des différentes ressources des FAC impliquées avec le cybermonde afin de mettre en exergue leurs déficiences. Ce portrait nous amène à démontrer l'importance d'effectuer, à court terme, une

---

National Security and Defence, *Proceedings of the Standing Senate Committee on National*

réorganisation au sein des FAC afin qu'elles deviennent le joueur clé recherché au niveau de la cyberdéfense du Canada.

À titre comparatif, les initiatives des États-Unis, de DoD, des autres alliés de l'alliance des cinq yeux (Five-Eyes Nations - FVEY), du Commandement de la défense aérospatiale de l'Amérique du Nord (North American Aerospace Defense Command - NORAD), de la France et de l'OTAN seront brièvement résumées. Bien qu'une réorganisation des ressources des FAC soit requise à court terme, la majorité de nos alliés n'ont qu'une légère avance par rapport au Canada. Pour l'instant, les FAC n'ont pas accusé un retard significatif par rapport au reste du monde. Cependant, des décisions et des actions doivent être prises rapidement par les hauts dirigeants afin d'éviter que le fossé se creuse de plus en plus par rapport à nos alliés.

Canada

Dans le rapport publié par le vérificateur général du Canada en 2012, le constat est que depuis 2001, les progrès du gouvernement face à ses engagements envers les cybermenaces ont été très lents et ce, malgré la mise en place de plusieurs stratégies et l'attribution de fonds spécifiques. Ainsi, la création en 2005 du Centre canadien de réponse aux incidents cybernétiques (CCRIC), qui relève de SP, aurait dû engendrer une bonne connaissance de la situation et des éléments nécessaires pour la protection des infrastructures essentielles. Cependant, depuis son ouverture, le centre n'a jamais surveillé les cybermenaces à temps plein. De même, le rapport stipule que :

> Le fait de ne pas être ouvert en tout temps empêche le CCRIC de connaître pleinement la situation relative à l'évolution des cybermenaces nationales et internationales. Les heures d'ouverture limitées nuisent également à la capacité du Centre à fournir aux intervenants de l'infrastructure essentielle de l'information et

---

Security and Defence, Issue 6, Evidence - Meeting of May 7, 2012.

> des analyses pertinentes, en temps opportun. Sans celles-ci, les propriétaires et les exploitants d'éléments de l'infrastructure essentielle peuvent plus difficilement réagir aux cyberattaques qui pourraient causer des perturbations62.

Dans son travail de recherche intitulé « *Strengthening The Cybersecurity of Critical Infrastructure : The Need of a Targeted Legislative Reform* », le lieutenant-colonel (lcol) Eric Cyr analyse la Politique de sécurité nationale, la Loi sur la gestion des urgences, la Stratégie nationale sur les infrastructures essentielles ainsi que la Stratégie de cybersécurité du Canada, afin de déterminer si le cadre législatif et les politiques permettent au gouvernement de respecter son mandat de protéger la nation advenant que les propriétaires d'infrastructures essentielles négligent les aspects sécuritaires. Ces mêmes documents ont aussi servi de référence au vérificateur général pour établir son rapport. Le lcol Cyr arrive à la conclusion que le gouvernement ne possède ni le cadre règlementaire ni le soutien législatif nécessaire pour renforcer la cybersécurité au sein du secteur privé, responsable du maintien des infrastructures essentielles. Pourtant, pour pouvoir assurer la sécurité, le gouvernement devrait être en mesure d'imposer des normes minimums de cybersécurité à travers tout le réseau d'infrastructures essentielles et de disposer, au besoin, des mesures discrétionnaires63. Dans un article paru dans le *Huffington Post* en mai 2011, Ron Deibert fait le même constat [Traduction] « la stratégie de cybersécurité n'est pas à la hauteur de l'ampleur des défis ni des stratégies équivalentes publiées par nos alliés comme les États-Unis »64. Le rapport du vérificateur général précise que :

---

62 Bureau du vérificateur général du Canada, « Protéger l'infrastructure …», p. 18.
63 Cyr, « Strengthening the cybersecurity of critical infrastructure …», p. 50-52.

> Sécurité publique Canada doit assumer un rôle de premier plan à l'échelle nationale en matière de sécurité publique et de protection civile. Il ne dirige toutefois pas les provinces, les territoires, les propriétaires d'éléments de l'infrastructure essentielle et les autres ministères quant à la manière d'exercer leurs activités. Selon le mandat du Bureau de la protection des infrastructures essentielles et de la protection civile, la Politique de sécurité nationale, la stratégie nationale et le plan d'action sur les infrastructures essentielles et la Stratégie de cybersécurité du Canada, Sécurité publique Canada doit assurer son rôle de direction et de coordination en offrant aux propriétaires et aux exploitants d'éléments de l'infrastructure essentielle un soutien et des services auxquels ils n'auraient peut-être pas accès autrement. Il peut notamment établir des partenariats et fournir une tribune pour favoriser le partage d'information sur les cybermenaces en temps opportun entre les intervenants. Surveiller la situation en ce qui a trait à l'évolution de la cybermenace à l'échelle nationale et internationale afin d'obtenir rapidement des avertissements pertinents sur les vulnérabilités liées à la cybersécurité et d'analyser les cybermenaces touchant les intervenants responsables de l'infrastructure essentielle. Finalement, accroître la capacité de protéger l'infrastructure essentielle en améliorant le cadre stratégique, la sensibilisation et l'éducation ainsi que la recherche et le développement65.

À la lumière de ces commentaires et constats, il devient évident que le cadre législatif qui permettrait au gouvernement d'agir promptement et adéquatement, afin de protéger les infrastructures essentielles, doit être revu et corrigé. D'après le lcol Cyr, le gouvernement a plutôt tendance à être réactif que proactif, c'est-à-dire que la plupart du temps, les lois suivent des évènements malheureux. Ainsi, ce n'est que le 1er avril 2002, à la suite des évènements du 11 septembre 2001, que l'Administration canadienne de la sûreté du transport aérien (ACSTA) a été établie66. Par contre, il concède que, dans certains cas, comme pour les règlements sur la sécurité des véhicules automobiles ou ceux sur la sécurité des produits alimentaires et de

---

64 Ron Deibert, « Cyber Security : Canada is Failing the World », *Huffington Post*, 26 mai 2011, consulté le 4 mars 2014, http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html

65 Bureau du vérificateur général du Canada, « Protéger l'infrastructure …», p. 8.

consommation, les cadres réglementaires du gouvernement fédéral ont répondu de façon efficace aux préoccupations de sécurité nationale et de la sécurité publique, en suivant l'évolution de la menace et en assurant la prospérité économique du secteur privé. Selon le lcol Cyr, ces règlements représenteraient des exemples à suivre67.

L'aspect important à considérer avec les infrastructures essentielles est qu'un manque au niveau de la cybersécurité dans un domaine peut avoir un impact substantiel dans un autre secteur interrelié68. Ainsi, Richard Clarke, ancien coordinateur national pour la sécurité, la protection des infrastructures essentielles et le contreterrorisme aux États-Unis, explique que la réglementation excessive apporte parfois une hausse des prix à la consommation sans résoudre les véritables causes du problème. Inversement, le refus de règlementer peut entraîner des situations embarrassantes comme ce fut le cas avec la peinture au plomb dans des jouets pour enfants69.

En plus de la réglementation, la capacité organisationnelle constitue un facteur essentiel à une réponse efficace contre la cybermenace. En effet, les différents acteurs du cybermonde provenant de l'entreprise privée et du gouvernement canadien, incluant les FAC, doivent être structurés de manière à pouvoir s'adapter à la menace et à prendre les actions appropriées, et ce, dans un délai suffisamment expéditif pour contrer la menace et éliminer les impacts sur la population canadienne.

---

66 Administration canadienne de la sûreté du transport aérien, *ALLER DE L'AVANT : Rapport annuel 2010* (Ottawa : Groupe Communication Canada, 2010), p. 5, consulté le 4 mars 2014, http://www.acsta.gc.ca/sites/default/files/imce/Rapportannuel2010.pdf

67 Cyr, « Strengthening the cybersecurity of critical infrastructure …», p. 64-67.

68 Eric A. Fisher, *Creating a National Framework for Cybersecurity*…, P. 55.

Ministères et organismes gouvernementaux

Parmi les ministères et organismes gouvernementaux impliqués avec le cybermonde, IC a les responsabilités suivantes en tant que ministère principal pour les questions liées aux fonctions de soutien en cas d'urgence :

1. La coordination avec l'industrie des télécommunications;
2. Le rétablissement et l'expansion des infrastructures et des services de télécommunications;
3. La protection et le rétablissement des ressources cybernétiques et des ressources de technologie de l'information liées aux télécommunications à l'échelle nationale; et
4. La coordination des mesures fédérales pour assurer les télécommunications temporaires d'urgence requises et le rétablissement de l'infrastructure de télécommunications
   touchée70.

---

69 Richard A. Clarke et Robert K. Knake, *Cyber War : The Next Threat to National Security and What to Do About It* (New York : HarperCollins Publisher, 2010), p. 134.

70 Sécurité publique Canada, *Plan Fédéral d'Intervention d'Urgence* (Ottawa : Groupe Communication Canada, 2009), p. A5-A6. Consulté le 4 mars 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-fra.pdf

En ce moment, la responsabilité du spectre électromagnétique est partagée entre IC, en vertu de la Loi sur la radiocommunication, et le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), au titre de la Loi sur la radiodiffusion et de la Loi sur les télécommunications. Cette stratégie correspondait bien aux besoins du 20e siècle. Toutefois, elle n'est plus adéquate alors qu'aujourd'hui, nous sommes en présence d'entreprises totalement intégrées offrant des services téléphoniques, des services sans fil, de radiodiffusion et d'internet. Il n'est plus logique d'avoir un seul organisme de réglementation pour les fournisseurs de services filaires et deux pour les fournisseurs de services sans fil. Pour être plus précis, la réglementation manque de cohérence et il est difficile d'optimiser les avantages sociaux et économiques pour les Canadiens71. Tout comme pour les FAC qui ont un besoin urgent de restructurer leurs ressources cybernétiques, le GC doit comprendre la réalité du cybermonde, tel qu'expliqué tout au long de ce travail de recherche, afin d'améliorer ses politiques et réglementations auprès des intervenants de cette dimension.

Face à l'importance des technologies et en réponse au rapport du vérificateur général, IC a publié en 2014 Canada numérique 150, un plan audacieux pour guider l'avenir numérique du pays. En préambule, le Premier ministre Stephen Harper indique « [que Canada numérique 150] établit une vision de ce que le Canada peut accomplir d'ici la célébration de notre 150^{e} anniversaire en 2017, et au-delà »72. Ce plan propose cinq grands piliers qui sous-tendent un Canada numérique prospère :

---

71 CRTC, « Note pour une allocution de Konrad von Finckenstein, c.r., Président, Conseil de la radiodiffusion et des télécommunications canadiennes », consulté le 4 mars 2014, http://www.crtc.gc.ca/fra/com200/2010/s100422.htm

72 Industrie Canada, *Canada numérique 150*…, p. 3.

1. Un Canada branché;
2. Un Canada protégé;
3. Les possibilités économiques;
4. Le gouvernement numérique; et
5. Le contenu canadien73.

En ce qui concerne un Canada protégé, soit l'objet même du présent travail de recherche, le plan précise que la population canadienne sera protégée contre les menaces en ligne et le mauvais usage de la technologie numérique. Ainsi :

1. Les Canadiens auront confiance que leurs transactions en ligne sont sûres;
2. Le Canada sera un chef de file de la protection de la vie privée en ligne de ses citoyens;
3. Nos familles seront protégées contre la cyberintimidation et les autres menaces en ligne74.

Afin d'atteindre ces objectifs audacieux, le GC mise sur une longue liste de nouvelles initiatives et de réalisations accomplies au courant des dernières années, dont les principales sont :

1. La Loi sur la protection des renseignements personnels et les documents électroniques afin de mieux protéger la vie privée en ligne de tous les Canadiens;
2. Déposition d'une loi exhaustive en matière de cyberintimidation;

---

73 *Ibid*., p. 6.

3. Adoption de la loi canadienne anti-pourriel, une référence mondiale qui entrera en vigueur le 1er juillet 2014;
4. Mise en place de plans pour déposer de nouveaux règlements sur les monnaies virtuelles afin de lutter contre le blanchiment d'argent et le financement des activités terroristes;
5. Création des lois rigoureuses, comme la Loi concernant la déclaration obligatoire de la pornographie juvénile sur Internet par les fournisseurs;
6. La Stratégie de cybersécurité du Canada;
7. Nouveaux services d'authentification pour les consommateurs, dont le Service de courtier de justificatifs d'identité et CléGC, qui facilitent la gestion et la protection des noms d'utilisateur, des identités et des mots de passe en ligne75.

À la lumière de la situation actuelle et du rapport cité du vérificateur général, le plan semble extrêmement audacieux. Toutefois, un tel plan dresse la table pour une meilleure collaboration intergouvernementale ainsi qu'avec le secteur privé, en plus de favoriser une amélioration du commandement et du contrôle des diverses ressources cybernétiques gouvernementales. En lien avec cette vision pour notre pays, le 4 août 2011, le GC a créé SPC qui a comme mandat de transformer fondamentalement la façon dont le GC gère son infrastructure de technologie de l'information76.

---

74 *Ibid*., p. 11.
75 *Ibid*., p. 12.
76 Services partagés Canada, « Mandat », consulté le 4 mars 2014, http://www.ssc-spc.gc.ca/pages/mndt-fra.html

En raison de ses responsabilités sur les réseaux non-classifiés du GC, la création de SPC a une incidence directe sur les opérations des FAC, en particulier lors d'une situation d'opérations domestiques. Il devient donc nécessaire de renforcer les priorités opérationnelles avec la nouvelle interface entre SPC et les FAC, soit la nouvelle organisation localisée dans la chaîne de commandement du sous-ministre adjoint (Gestion de l'information) (SMA(GI)).

Enfin, pour les FAC, l'entité la plus importante du cybermonde et avec laquelle un partenariat solide est nécessaire est le CSTC, qui représente l'autorité technique canadienne au niveau du SIGINT. Même si les FAC et CSTC relèvent tous les deux du même ministre, ces deux organisations ont des rôles et des responsabilités distinctes et n'ont aucune obligation de collaborer de façon étroite. En fait, le mandat et les pouvoirs du CSTC sont énoncés dans la Loi sur la défense nationale qui stipule notamment que le CSTC doit poursuivre trois finalités :

1. Acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;
2. Fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada; et
3. Fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère77.

Pour que les FAC deviennent un joueur pertinent et influent au niveau de la cyberdéfense et que sa voix soit entendue par le CSTC, une réorganisation au niveau du commandement et contrôle de ses ressources cybernétiques est requise à court terme. À cette fin, la prochaine section traite de la chaîne de commandement actuelle au niveau de ces ressources.

Forces armées canadiennes

Dans son mémoire de maîtrise intitulé « *Considerations : Canadian Forces' Efforts In The Electromagnetic Spectrum And Cyber Operation Environment* », le lcol Jason Walkling analyse les diverses organisations des FAC qui ont un rôle à jouer au niveau du cybermonde[78]. Au niveau tactique, chaque élément, soit la Marine royale canadienne (MRC), Aviation royale canadienne (ARC), Armée canadienne (AC) et les Forces d'opérations spéciales (FOS) agit directement dans le cybermonde par la conduite de leurs opérations quotidiennes. Leur implication, bien qu'importante, se limite à la guerre électronique, en particulier au niveau de l'empreinte électromagnétique et de la sécurité de l'information partagée. Au niveau opérationnel, le Commandement des opérations interarmées du Canada (COIC) agit à titre d'employeur de forces sans pour autant détenir une structure de commandement envers les générateurs de forces. Dans ces conditions, les différentes organisations des FAC jouant un rôle à l'intérieur du cybermonde ne sont pas coordonnées par une structure organisationnelle, mais bien par leur chaîne de commandement respective. SMA(GI) occupe une place de premier plan au

---

77 Centre de la sécurité des télécommunications Canada, « Nos activités et notre raison d'être », consulté le 24 mars 2014, http://www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-fra.html

78 J.C. Walkling, « Considerations : Canadian Forces' Efforts In The Electromagnetic Spectrum And Cyber Operating Environment » (travail rédigé dans le cadre du Programme de commandement et d'état-major interarmées, Collège des Forces canadiennes, 2013), p. 52-69.

sein du cybermonde. En effet, il dispose des deux organisations militaires les plus actives dans ce domaine, soit le directeur général – Opérations (Gestion de l'information) (DGOGI) et le Groupe des opérations d'information des Forces canadiennes (GOIFC), subordonné au DGOGI. Comme quelques-unes des organisations du Ministère de la Défense nationale (MDN), SMA(GI) se retrouve à cheval entre le CEMD et le sous-ministre (SM), ce qui limite les actions et décisions de la part de la chaîne de commandement opérationnelle des FAC79. La figure 3.1 démontre la distinction unique entre les deux chaînes de commandement qui priment au sein du MDN, soit celle du CEMD et celle du SM.

Pour amplifier davantage les complications liées aux multiples chaînes de commandement des ressources cybernétiques, le Chef du Renseignement de la Défense (CRD) détient le contrôle opérationnel de GOIFC pour les tâches quotidiennes au niveau du renseignement d'origine électromagnétique (Signals Intelligence – SIGINT). Par contre, CRD ne détient aucun contrôle sur le Centre d'opération des réseaux des Forces canadiennes (CORFC) qui défend les différents réseaux de la défense à travers les six missions qui lui sont confiées80. La figure 3.2 révèle deux particularités supplémentaires. Tout d'abord, on y retrouve le directeur général de la Cybersécurité (DG Cyber), une nouvelle organisation créée en avril 2011 sous le commandement du Chef du Développement des forces (CDF). Dans un témoignage au Parlement le brigadier-général (bgén) Loos, alors responsable de DG Cyber, indique que « […] l'organisation a pour

---

79 *Ibid*., p. 52-69.

80 La mission du CORFC peut être divisée en six champs principaux constituant les fonctions opérationnelles de l'unité et comportant plusieurs opérations. Les principaux champs de la mission du CORFC sont les suivants : exploitation des systèmes nationaux, gestion des incidents, défense des réseaux informatiques, opérations de sécurité, connaissance de la situation au niveau de l' ITI et gestion des problèmes. Sous-ministre adjoint (Gestion de l'information), « Mission du CORFC », consulté le 24 mars 2014 sur le RÉD, http://img-ggi mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/cfn-cor/index-fra.asp.

principale tâche de cerner et de développer les capacités futures au niveau cybernétique. Cela comprend un travail conceptuel critique, ainsi que la conception et l'établissement de capacités cybernétiques »81. Lors du même témoignage, il présente le plan de travail de son organisation qui est divisée en quatre volets :

> […] le premier a trait aux politiques. Tout comme notre équipe du sous-ministre adjoint aux politiques, nous faisons des suggestions à Sécurité publique Canada sur la mise en œuvre de la Stratégie du Canada en matière de sécurité cybernétique, et nous participons à l'élaboration de politiques concernant le rôle des forces armées dans l'environnement cybernétique. Le deuxième porte sur le commandement et le contrôle, et comprend la conception d'un régime d'autorité, de responsabilité et de reddition de comptes pour les capacités cybernétiques qui relèvent des commandants opérationnels. Comme pour la Stratégie nationale en matière de sécurité cybernétique, notre approche consiste à éviter de traiter tout ce qui concerne la « cybernétique » comme fondamentalement nouvelle, et à tenter plutôt d'intégrer, dans la mesure du possible, nos activités cybernétiques dans les cadres de planification et d'opération existants. Le troisième volet est le renforcement des capacités. Il consiste notamment à assurer que les ressources sont adéquatement axées sur les fonctions fondamentales, et à contribuer à la synchronisation des divers programmes des forces liés à la cybernétique. L'une des grandes priorités, pour renforcer notre capacité cybernétique dans les Forces canadiennes, est de fournir aux commandants une image commune de la situation opérationnelle et de leur permettre de mieux comprendre leur environnement cybernétique, favorisant ainsi une prise de décisions plus éclairée en temps opportun. Finalement viennent les ressources humaines et la formation. On définit les besoins en matière de formation, on élabore un programme permettant de rassembler les compétences spécialisées requises pour opérer de façon efficace dans l'environnement cybernétique et on met en œuvre des mesures pour conserver ces compétences, éviter l'érosion des compétences et assurer un niveau de rétention du savoir approprié82.

La seconde organisation particulière est l'équipe des opérations cybernétiques interarmées (Joint Cyber Operations Team – JCOT) qui est imbriquée au sein du COIC et qui a pour mission

---

81 Parlement du Canada, Comité sénatorial permanent de la sécurité nationale et de la défense, *Témoignages*, le lundi 5 novembre 2012, consulté le 24 mars 2014, http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-f.HTM

82 *Ibid*.

de [Traduction] « […] fournir une expertise et des conseils [sur toutes les activités opérationnelles cybernétiques] au personnel du COIC en appui aux missions domestiques et expéditionnaires des FAC »83.

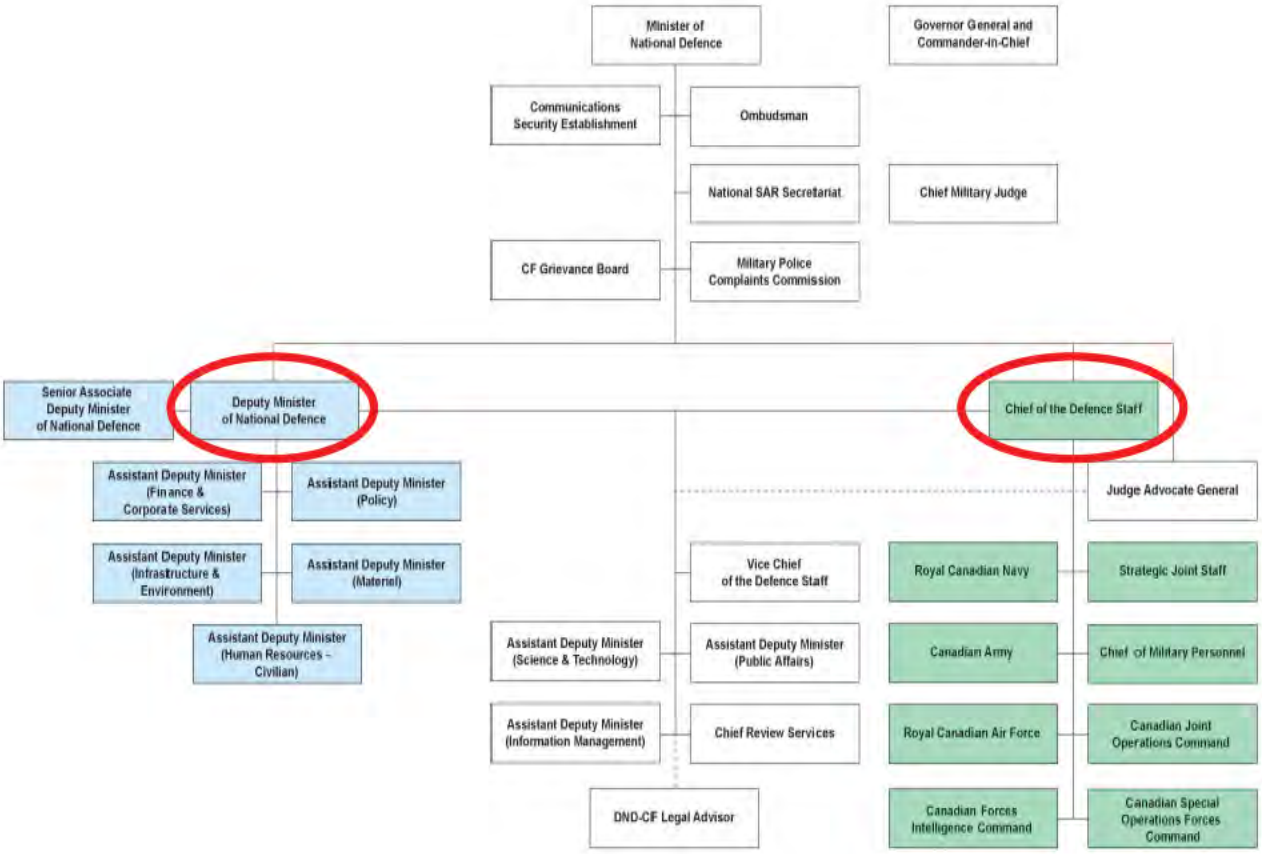


Figure 3.1 – Structure organisationnelle au sein du MDN

Source: Réseau étendu de la Défense (RÉD)

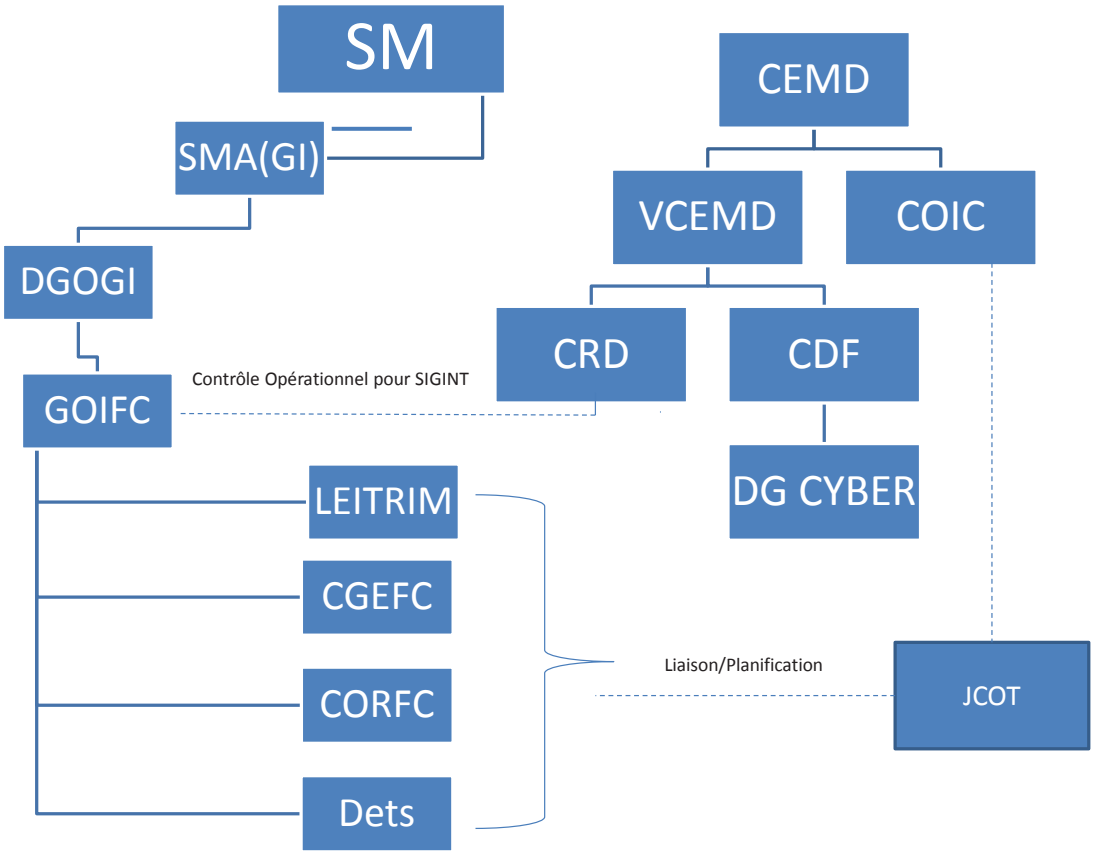


Figure 3.2 – Commandement et contrôle des ressources cybernétiques

Source: Diagramme adapté de l'équipe des opérations cybernétiques interarmées, *Joint Cyber Operations Team (JCOT) : Concept of Operations*, Version 2.0.84

Il s'agit donc de deux nouvelles formations majeures dans le domaine cybernétique et qui apportent des éléments supplémentaires de coordination pour le DGOGI et le GOIFC. Elles ont un rôle important à jouer, mais possèdent un chef différent. Puisque le cybermonde semble être

---

83 Ministère de la Défense nationale, *Joint Cyber Operations Team (JCOT) : Concept of Operations*, Version 2.0 (Ottawa : Joint Cyber Operations Team, mars 2013), p. 5.

84 Ministère de la Défense nationale, *Joint Cyber Operations Team*…, p. 4.

le nouvel élément d'intérêt des FAC, plusieurs veulent agir comme d'acteurs primordiaux, ce qui, par contre, ne favorise pas l'économie d'effort pourtant un de nos principes de guerre85.

La situation du Canada et des FAC face au cybermonde est, à quelques exceptions près, comparable avec celles de nos alliés. En effet, tous les joueurs sont en quête d'efficience.

Alliés et Alliances

La complexité du cybermonde est un facteur qui affecte aussi nos alliés au niveau de l'interprétation des différents acteurs de cette nouvelle réalité. Tous cherchent à influencer la diffusion des données, mais d'abord et avant tout, ils cherchent à protéger leur propre population contre des attaques potentielles. Cette section pose un regard sur nos alliés principaux, principalement les États-Unis, pays avec lequel notre partenariat est le plus critique au niveau de la cybersécurité.

États-Unis

Dans leur stratégie de sécurité nationale de 2010, les États-Unis considèrent que [Traduction] « Les menaces qui pèsent sur la cybersécurité constituent l'une des principales entraves à notre sécurité nationale et à la sécurité publique, tout en représentant l'un des plus importants défis économiques que nous devons relever en tant que nation »86.

De même, l'Agence nationale de la sécurité (National Security Agency – NSA) estime qu'en 2011 seulement, plus d'un billion de dollars (1 000 milliards de dollars) ont été dépensés

---

85 Ministère de la Défense nationale, B-GL-300-001/FP-002, *OPÉRATIONS TERRESTRES* (Ottawa : MDN Canada, 2008), p. 3-8.

86 Executive Office of the President of the United States, *National Security Strategy* (Washington, D.C. : U.S. Government Printing Office, 2010), p. 27.

envers la gestion de l'espionnage et du crime cybernétique87. De façon plus précise, un rapport préparé par le Bureau exécutif du contre-espionnage des États-Unis (Office of the National Counterintelligence Executive) pour le Congrès indique que la Chine est l'espion mondial le plus actif et le plus persistent contre l'économie des États-Unis88. Toujours en 2011, la Maison-Blanche a publié la stratégie internationale pour le cybermonde afin de promouvoir un environnement global à l'intérieur de l'espace cybernétique qui soit ouvert, interopérable, sécuritaire et fiable89. Depuis, le président Obama tente tant bien que mal de faire passer la loi Liberman-Collins, rejeté à deux reprises par le Congrès dont la dernière fois en novembre 2012. Depuis, le sous-comité de la sécurité intérieure sur la cybersécurité, la protection des infrastructures et des technologies a toutefois fait approuver la loi « HR 3696 ». Le président du sous-comité, Michael McCaul, considère que cette loi reconnaît la menace grandissante du cybermonde et renforce les capacités de DHS à protéger les infrastructures critiques. Avec la première étape franchie, si cette loi devient officiellement adoptée, elle renforcerait le partenariat entre l'industrie et le gouvernement en matière de cybersécurité90.

---

87 Wark, « Cyber-Agression …», p. 35.

88 Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace : Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011* (Washington, D.C. : U.S. Government Printing Office, 2011), p. 5, consulté le 24 mars 2014, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

89 Thomas M. Chen, *An Assessment Of The Department Of Defense Strategy For Operating In Cyberspace* (Carlisle : United States Army War College Press, 2013), p. 7.

90 Eric Chabrow, « Cybersecurity Bill Advances in House », *BankInfoSecurity*, 16 janvier 2014, consulté le 24 mars 2014, http://www.bankinfosecurity.com/cybersecurity-bill-advances-in-house-a-6401

Bien que la loi ne soit pas encore officiellement adoptée, on voit bien, à travers ces approches législatives que les États-Unis considèrent l'importance de légiférer afin de protéger les infrastructures essentielles contre les attaques cybernétiques. Cette situation législative est identique à celle du Canada. Par contre, l'implication de la Défense dans la cybersécurité est beaucoup plus imposante aux États-Unis qu'elle ne l'est au Canada.

Pour DoD comme pour toutes les Forces armées des différents pays développés, le cybermonde est très différent des domaines opérationnels habituels qui sont la mer, la terre, l'air et l'espace. En effet, ce nouveau domaine est la création de l'homme et ses menaces y sont furtives en plus d'être difficilement attribuable à l'auteur. Pour faire valoir l'ampleur de l'empreinte du DoD à l'intérieur du cybermonde, le secrétaire de la Défense Robert Gates affirme dans une déclaration devant un comité sénatorial en 2009 « [que] DoD opère plus de quinze milles différents réseaux et environ sept millions d'appareils distincts de la technologie de l'information […] »91. Afin d'officialiser le cybermonde comme un domaine opérationnel et de maintenir la sécurité des États-Unis face à l'émergence des cybermenaces, DoD a publié en 2011 la stratégie d'opération à l'intérieur de l'espace cybernétique. Cette dernière, considérée comme complémentaire à celle publiée par la Maison-Blanche la même année, met l'emphase sur cinq initiatives stratégiques [Traduction] :

1. Considérer l'espace cybernétique comme un autre domaine opérationnel;
2. Employer de nouveaux concepts d'opération pour protéger les réseaux du DoD;

3. Faire équipe avec les autres agences gouvernementales et le secteur privé;
4. Façonner les relations avec les alliés et différents partenaires internationaux avec pour objectif d'affermir la sécurité cybernétique; et,
5. Utiliser les ressources nationales et la recherche et développement pour favoriser l'entraînement du personnel en vertu de l'évolution technologique92.

Un an auparavant, soit en mai 2010, le Commandement cybernétique des États-Unis (U.S. Cyber Command – CYBERCOM) a été officiellement activé à l'intérieur de la structure organisationnelle du Commandement stratégique des États-Unis (U.S. Strategic Command – USSTRATCOM) structure qui se rapporte directement au secrétaire de la Défense. Le CYBERCOM a trois missions. Tout d'abord, il est responsable des opérations quotidiennes pour la défense des réseaux du DoD et supporte à partir du cybermonde, les missions militaires et de contre-terrorisme. Ensuite, il est la seule chaîne de commandement militaire du cybermonde. Ainsi, il est responsable de coordonner le travail des différentes branches militaires pertinentes au cybermonde dont le Commandement cybernétique de l'armée américaine (U.S. Army Cyber Command), le Commandement cybernétique de la flotte navale (U.S. Fleet Cyber Command / U.S. 10th fleet), la 24^{e} unité de la force aérienne qui joue aussi le rôle d'unité cybernétique pour la force aérienne des États-Unis (24th Air Force), le Commandement cybernétique du Corps des Marines des États-Unis (U.S. Marine Corps Forces Cyber Command) et le Commandement

---

91 Robert M. Gates, « Submitted Statement to Senate Armed Services Committee », *Hearing before Senate Armed Services Committee* (Washington, D.C. : U.S. Senate, 2009), p. 8, consulté le 24 mars 2014, http://www.loc.gov/law/find/gates.php

92 Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C. : U.S. Governement Printing Office, July 2011), p. 5-12.

cybernétique de la Garde côtière des États-Unis (U.S. Coast Guard Cyber Command). Enfin, sa troisième mission est de travailler en collaboration avec une variété de partenaires internes et externes au gouvernement américain. Ainsi, avec DHS, il travaille en étroite collaboration avec le secteur privé afin de partager l'information concernant les diverses menaces et les vulnérabilités existantes93.

Bien que DoD investissent largement dans la protection de ses propres réseaux, il est inévitable que des intrusions puissent ne pas être perçues et arrêtées aux frontières des réseaux. Il devient alors nécessaire d'être en mesure de poursuivre ces intrusions à partir de l'intérieur des réseaux du DoD. Ainsi, la défense active continue d'être une priorité pour le Pentagone. Selon le secrétaire adjoint de la Défense des États-Unis, William J. Lynn III [Traduction] :

> […] cette défense active est possible en raison de la consolidation des capacités cybernétiques de la Défense sous un même commandement en les liant aux ressources de SIGINT requises pour anticiper les intrusions et les attaques. L'établissement de cette collaboration entre ressources était à la base de la mise en place du USCYBERCOM 94.

Lynn met beaucoup d'emphase sur l'importance de la collaboration pangouvernementale ainsi qu'avec le secteur privé en indiquant que le Pentagone met son expertise et ses dix années d'expérience disponible en support aux infrastructures essentielles du pays. De même, le partenariat « Enduring Security Framework » qui réunit les PDG et les directeurs de la technologie (Chief Technology Officer – CTO) des compagnies majeures de défense et des technologies de l'information se rencontrent régulièrement avec les hauts fonctionnaires de DHS, DoD et du renseignement national (National Intelligence – NI). DoD considère ce type de

---

93 Lynn, « Defending a New Domain …», p. 102.
94 *Ibid*., p. 103.

partenariat comme étant crucial puisque DHS est responsable de la protection des domaines « .gov » et « .com », deux domaines dont DoD dépend tout particulièrement pour ses opérations95.

Les institutions gouvernementales américaines poussent encore plus loin la recherche et le développement. Ainsi, le programme « National Cyber Range », développé par la même agence qui a mis sur pied l'ARPANET, procure un modèle de l'internet permettant à DoD, de tester sa cyberdéfense, dans un environnement de simulation avant d'intégrer une nouvelle technologie. Suivant les pratiques de l'industrie, les administrateurs des réseaux de la Défense sont maintenant entraînés pour conduire du piratage éthiquement approuvé (ethical hacking). Utilisant les techniques d'intrusion connues des adversaires, ce mode d'opération permet d'identifier les faiblesses de ses propres réseaux avant que l'ennemi en prenne avantage96.

Selon Thomas M. Chen, Ph. D., professeur à l'université Swansea du Royaume-Uni et spécialiste de la sécurité internet, bien que plusieurs progrès ont suivi l'unification des ressources cybernétiques sous le CYBERCOM, le manque de direction claire en rapport au commandement et contrôle entre le CYBERCOM et les commandants militaires des régions demeure une inquiétude très importante97. De plus, le Bureau du vérificateur général américain (Government Accountability Office – GAO), souligne le manque de gouvernance du personnel civil dans les opérations de cyberguerre de même qu'au niveau des exigences et des capacités de mission pour

---

95 *Ibid*., p. 104-105.
96 *Ibid*., p. 105-106.
97 Chen, *An Assessment Of The Department Of Defense Strategy* …, p. 12.

organiser, entraîner et équiper les forces cybernétiques98. De plus, et il s'agit là selon Chen d'un élément important, la stratégie publiée par DoD ne clarifie pas la manière dont le budget sera investi pour accomplir les diverses initiatives99.

Malgré la vision et les bonnes intentions de DoD pour faire face aux menaces du cybermonde, il reste donc plusieurs étapes capitales à franchir avant d'atteindre les objectifs. Par contre, tel que le soutient Chen, ces initiatives de DoD lancent un message clair aux autres organismes gouvernementaux des États-Unis ainsi qu'à tous ses alliés à propos de l'importance et du sérieux des opérations cybernétiques100.

Dans le cadre de ses recherches sur l'approche des alliés face à la menace cybernétique, Walkling considère que le gouvernement américain, tout comme le gouvernement canadien, fait face à des tensions à l'intérieur du Congrès ce qui limite sa capacité d'intervention auprès du secteur privé, responsable de la majorité des infrastructures essentielles du pays. De plus, Walkling souligne l'importance d'avoir un commandant militaire opérationnellement responsable de l'environnement domestique, puisque les Forces armées pourraient avoir à intervenir à l'intérieur de ses propres frontières101.

Five-Eyes Nations

---

98 United States Government Accountability Office, *Defense Department Cyber Efforts : DoD Faces Challenges In Its Cyber Activities* (Washington, D.C. : U.S. Government Printing Office, 2011), consulté le 7 avril 2014, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=131495&lng=en

99 Chen, *An Assessment Of The Department Of Defense Strategy* …, p. 12-13.

100 *Ibid*., p. 10.

101 Walkling, « Considerations : Canadian Forces' Efforts In The Electromagnetic Spectrum …», p. 80-83.

Les autres alliés de l'alliance du Five-Eyes Nations (FVEY), soit le Royaume-Uni, la Nouvelle-Zélande et l'Australie, contrairement aux États-Unis, ressemblent plus au Canada en termes d'importance de leurs forces armées, et constituent par le fait même de bons éléments de comparaison pour le Canada.

Dans son analyse, Walkling aborde les diverses approches des membres du FVEY et indique qu'ils ont tous, comme le Canada, publié une stratégie de sécurité nationale ou une stratégie de cybersécurité afin d'identifier la présence d'une menace et l'orientation du gouvernement pour protéger les infrastructures essentielles au bien-être de sa population. La consolidation des efforts et la création d'un centre de sécurité nationale, comparable au CCRIC, démontrent que le Canada et ses alliés semblent tous se diriger dans la même direction en termes de cybersécurité. De plus, bien qu'une vision soit élaborée, dans la plupart des pays également, beaucoup de progrès reste à faire pour être pertinent et pleinement fonctionnel à l'intérieur du cybermonde102.

NORAD

Pour NORAD, la guerre cybernétique est la prochaine menace en importance, elle constitue donc une très grande priorité pour sa chaîne de commandement. En effet, la proactivité dans ce domaine se manifeste par la mise en place du Centre cybernétique interarmées (CCI), sous la division des opérations USNORTHCOM/NORAD (J3). Le centre comprend entre autres des membres des opérations, du renseignement et des systèmes de commandement et contrôle. De plus, il intègre 12 membres du CYBERCOM. Le CCI a trois missions principales. Tout d'abord, il doit accroître la connaissance de la situation de l'espace cybernétique au sein du

quartier général, ensuite il apporte des éléments de défense aux réseaux du NORAD et finalement, il procure de l'information aux autorités civiles concernant les conséquences des actions prises dans le cybermonde[103].

L'étroite collaboration des ressources cybernétiques vers l'atteinte d'un objectif commun entre le NORAD et le CYBERCOM peut représenter un exemple à suivre pour la collaboration entre les FAC et le CCRIC, sous la tutelle de SP.

FRANCE

Dans le dernier Livre blanc sur la Défense et la Sécurité nationale (LBDSN) de la France, la cyberdéfense a été élevée au rang de priorité[104]. Le ministre de la Défense, Jean-Yves Le Drian, a indiqué le 7 février 2014, lors de l'annonce du Pacte de Défense Cyber 2014-2016, que les réseaux de la Défense avaient été la cible de 780 incidents informatiques en 2013, contre 420 un an plus tôt et 195 en 2011. Au final, le ministre a indiqué que le Pacte Défense Cyber profitera aussi bien au ministère de la Défense qu'à l'ensemble de la communauté nationale de cybersécurité. La France prévoit un financement de près d'un milliard d'euros entre 2014 et 2019 pour supporter les efforts dans le domaine de la cybersécurité. Au niveau opérationnel, un volet cyber sera systématiquement intégré aux exercices de différents niveaux menés par les forces afin de vérifier la capacité des armées à tous les échelons à opérer malgré les cybermenaces et intégrer les problématiques liées au cyberespace dans leur espace de manœuvre. Une unité

---

102 *Ibid*., p. 90-97.

103 NORAD, « **NORAD, USNORTHCOM Joint Cyber Center stands up** », consulté le 7 avril 2014, http://www.norad.mil/Newsroom/tabid/3170/Article/1738/norad-usnorthcom-joint-cyber-center-stands-up.aspx

projetable assistera bientôt les états-majors engagés dans des opérations extérieures et sera connectée au Centre d'analyse de lutte informatique défensive (CALID). De plus, en juin 2013, le ministre a annoncé que la France allait se doter de capacités offensives sur le sujet105.

Enfin, le ministre mentionne en préambule au Pacte Défense Cyber que ce plan prévoit des améliorations internes dont :

> [perfectionner] notre posture réactive en amplifiant la mise en place des capacités du Commandement opérationnel de cyberdéfense créé en 2011 au sein du Centre de Planification et de Conduite des Opérations (CPCO) et son irrigation au sein de toutes les unités des armées et des entités du ministère106.

Bien que localisé à un échelon moins élevé dans la hiérarchie que le CYBERCOM, le Commandement opérationnel de cyberdéfense permet l'intégration des éléments cybernétiques du ministère de la Défense sous une même chaîne de commandement tout en supportant les efforts pangouvernementaux du président de la République.

OTAN

Comme membre de cette alliance, le Canada doit s'assurer de rencontrer les normes afin de demeurer un collaborateur pertinent en temps de paix en plus d'être en mesure d'être interopérable avec les forces déployées en théâtre d'opérations sous l'égide de l'OTAN.

---

104 Ministère de la Défense, *Livre Blanc : Défense et Sécurité Nationale 2013* (Paris : Direction de l'information légale et administrative, 2013), p. 94.

105 Vincent Lamigeon, « Cyberguerre : La France fourbit ses armes », *Challenges*, 21 janvier 2014, consulté le 7 avril 2014, http://www.challenges.fr/economie/20140121.CHA9418/cyberguerre-la-france-fourbit-ses-armes.html

106 Ministère de la Défense, *Pacte Défense Cyber : 50 mesures pour changer d'échelle* (Paris : Direction de l'information légale et administrative, 2014), p. 5.

En termes de cybersécurité, les ministres de la Défense des divers pays membres de l'OTAN ont approuvé en 2011, la nouvelle version de la politique de cyberdéfense. En vertu du volet « Recherche et Formation » de cette politique, l'OTAN poursuit l'amélioration du Centre d'excellence pour la cyberdéfense en coopération à Tallinn en Estonie (Cooperation Cyber Defence Centre of Excellence – CCD COE). La mise en place de ce centre fait suite aux attaques cybernétiques perpétrées contre l'Estonie en 2007. Le centre conduit des travaux de recherche et de la formation dans le domaine de la cyberdéfense. De plus, il a organisé en novembre 2013, l'exercice Cyber Coalition (CC13) qui vise à tester les procédures OTAN de gestion de crise et de partage de l'information. Outre sa priorité première de protéger ses propres systèmes de communication, il apporte une aide aux alliés pour renforcer leurs moyens de cyberdéfense tout en cherchant à approfondir sa coopération avec les organisations internationales, y compris l'Union européenne et le secteur industriel à travers le Groupe consultatif industriel de l'OTAN (NIAG). Par ailleurs, en 2012, la cyberdéfense a commencé à être intégrée au processus OTAN de planification de défense (NATO Defence Planning Process - NDPP). En avril 2013, une nouvelle étape capitale a été franchie en relation avec la cyberdéfense lors de la mise en œuvre de l'infrastructure de gestion de défense et des capacités analytiques du réseau de base au Centre technique de la capacité de réaction aux incidents informatiques de l'OTAN (NATO Computer Incident Response Capability – NCIRC), à Mons en Belgique107.

Toujours en 2013, le **« Tallinn Manual » sur la loi internationale applicable à la guerre cybernétique a été publié par un groupe d'experts sous l'égide du CCD COE.**

---

107 OTAN, « L'OTAN et la cyberdéfense », consulté le 7 avril 2014, http://www.nato.int/cps/fr/natolive/topics_78170.htm

Michaels Schmitt, éditeur du manuel et professeur au collège de guerre navale des États-Unis (U.S. Naval War College – NWC) mentionne à la presse associée « que tout le monde perçoit internet comme le« Wild, Wild West ». Ce qu'ils ont oublié, c'est que le droit international s'applique aux armes cybernétiques comme il s'applique à toutes les autres formes d'armement »108. Le « Tallinn Manual » est le fruit d'un travail acharné et conjoint entre Schmitt et des spécialistes internationaux des domaines juridiques et militaires et propose 95 règles à suivre pour apporter une base de réglementation dans le monde virtuel109.

En plus de tout ce qui a déjà été mentionné pour l'OTAN, un groupe d'experts a publié en 2010, une étude stratégique en prévision de l'année 2020 dans laquelle figurent plusieurs recommandations concernant la cyberdéfense dont celle [Traduction] « [qu'] au fil du temps, l'OTAN devra envisager de construire un réseau adéquatement adapté à la cyberdéfense en y intégrant des capacités passives et actives »110.

Comme membre le plus influent de tous les pays associés à l'OTAN, les États-Unis ont toujours fortement contribué à la mise en place de la réglementation et continue de le faire de nos jours avec en premier plan, la cyberdéfense. De même, le Canada doit continuer d'améliorer sa

---

108 Nerea Rial, « NATO targets hacktivists in new cyberwar directive », *New Europe Online*, consulté le 7 avril 2014, http://www.neurope.eu/article/nato-targets-hacktivists-new-cyberwar-directive

109 Michael N. Schmitt, « International Law in Cyberspace : The Koh Speech and Tallinn Manual Juxtaposed », *Harvard International Law Journal*, Vol. 54 (décembre 2012), p. 14, consulté le 7 avril 2014, https://www.usnwc.edu/getattachment/5067e23e-b849-4f60-a9f7-63e5238d4f6f/HILJ-Online_54_Schmitt.aspx

110 OTAN, « NATO 2020 : Assured Security; Dynamic Engagement », consulté le 7 avril 2014, http://www.nato.int/strategic-concept/expertsreport.pdf

réglementation et ses processus afin que ses acteurs du cybermonde deviennent des joueurs importants sur la scène internationale à travers, entre autres, des alliances comme l'OTAN.

Résumé du chapitre

Face aux initiatives des États-Unis, de l'OTAN et de ses autres alliés principaux (FVEY et la France), le Canada se doit d'améliorer la gestion de ses intervenants et de ses interventions à l'intérieur du cybermonde. Tout d'abord, comme le mentionne Eric Cyr, le cadre législatif doit être revu et corrigé afin de permettre au gouvernement une main mise sur tous les acteurs du cybermonde, en particulier les ministères et organismes gouvernementaux ainsi que les entreprises privées qui ont un rôle primaire avec les infrastructures essentielles de notre pays. Ensuite, une forte collaboration pangouvernementale doit se forger avec le secteur privé afin d'établir les rôles et les responsabilités de chacun des acteurs du cybermonde et être mieux en mesure d'assurer la coordination de tous les acteurs. En réponse au rapport du vérificateur général de 2012, le GC a publié en 2014 Canada numérique 150, un plan audacieux et visionnaire qui propose cinq grands piliers pour soutenir un Canada numérique prospère.

Pour les FAC, ceci implique une ouverture vers une nouvelle réglementation et une réorganisation institutionnelle afin de suivre l'évolution en matière cybernétique de notre gouvernement, des Forces armées alliées et des alliances dont nous sommes membres. Pour le moment, l'emploi de la force et la coordination des résultats sont extrêmement difficiles, car plusieurs commandants sont impliqués avec la gestion et le commandement de ces ressources. L'analyse de Jason Walkling, sur les différentes approches des alliés face à la menace

cybernétique, fait bien ressortir l'importance de la consolidation des moyens cybernétiques sous un même commandement.

Le prochain chapitre propose un changement de l'institution des FAC par la mise sur pied d'un Commandement cybernétique, une initiative similaire à celle de DoD mais à plus petite envergure. Sans aborder le cadre législatif de l'espace cybernétique, puisqu'à lui seul il représente un domaine de recherche complet, la nouvelle structure consolide toutes les ressources du cybermonde des FAC. Cette initiative faciliterait l'emploi de la force et l'obtention des résultats escomptés en plus de favoriser la collaboration pangouvernementale et avec le secteur privé. De plus, cette nouvelle structure permettrait une participation coordonnée de nos ressources aux diverses initiatives telles que celles mises sur pied par l'OTAN tout en demeurant un joueur pertinent aux yeux de nos alliés.

CHAPITRE 4 – CONCEPTION DU COMMANDEMENT CYBERNÉTIQUE

Lorsque le général Hillier a accepté le poste de CEMD en 2005, il avait la ferme intention d'apporter des changements institutionnels majeurs aux FAC. Avant tout il était motivé par l'atteinte de l'efficience opérationnelle. Comme toutes autres forces armées modernes, les FAC étaient structurées d'abord et avant tout pour la guerre conventionnelle, conséquence de son engagement dans les conflits européens et envers l'OTAN. Cette approche laissait prévoir que les FAC s'engageraient dans des opérations du type maintien de la paix en tant que partenaire d'une coalition111. Avec la fin de la guerre froide et le début d'un nouveau genre d'intervention dans des conflits principalement interétatiques, une restructuration devenait prioritaire. Comme

---

111 Michael K. Jeffery, *Inside Canadian Forces Transformation : Institutional Leadership As A Catalyst For Change* (Kingston : Canadian Defence Academy Press), p. 40-41.

le général britannique Sir Rupert Smith le mentionne « […] la guerre parmi la population dominera les types de conflits du XXI[e] siècle »112.

Hillier a été confronté à quelques-uns de ses généraux très résistants au changement et extrêmement fermés à l'idée de prendre des risques. Certains ont même compromis des étapes cruciales du changement proposé par le CEMD. Des subordonnés en sont même venus à percevoir Hillier comme un chef qui n'était pas à l'écoute et qui ne comprenait pas les risques institutionnels qui découleraient de ses changements113. Lors de la rétrospective sur la Transformation des FAC de 2005, conduite en 2007, il a été conclu que d'autres changements seraient encore requis pour améliorer l'institution. Toutefois, ces changements devaient attendre une réduction du tempo opérationnel des FAC114. En effet, les déploiements successifs en Afghanistan d'un nombre important de troupes imposaient le rythme dans l'institution. Le Canada a complété son engagement en Afghanistan en mars 2014, réduisant du coup le tempo opérationnel des FAC et le nombre de troupes déployées outre-mer. Cette diminution de la cadence devient un excellent moment pour considérer un changement institutionnel qui permettrait de répondre d'une manière flexible et pertinente à la menace actuelle et bien réelle, soit l'agression cybernétique. Cette agression sera décomposée en quatre volets spécifiques d'agression selon le modèle proposé par Wark.

Un Commandement cybernétique développé à partir du modèle analytique « Design Thinking » est élaboré dans le présent chapitre comme solution de réponse à la menace

---

112 General Sir Rupert Smith, *The Utility of Force : The Art of War in the Modern World* (London:Penguin Books, 2005), p.271.

113 Jeffery, *Inside Canadian Forces Transformation* …, p. 105.

114 *Ibid*., p. 117.

cybernétique. En premier lieu, l'environnement cybernétique relié aux FAC est défini afin de consolider les éléments importants à considérer pour la nouvelle structure organisationnelle. Ensuite, les problèmes en relation avec l'organisation actuelle sont analysés de manière à optimiser la résolution de ceux-ci dans les changements proposés. En troisième lieu, une approche conceptuelle est proposée qui tient compte de l'environnement et des problèmes spécifiques aux FAC. Finalement, l'approche proposée est comparée à deux autres options. Cette comparaison fait ressortir encore plus clairement que la création d'un Commandement cybernétique est l'option qui répond réellement aux besoins et à la réalité des FAC.

Conception d'un Commandement cybernétique à l'aide du « Design Thinking »

Jusqu'à présent, l'option d'un Commandement cybernétique n'a pas encore été analysée par les FAC. En utilisant un modèle conceptuel fréquemment utilisé par les forces américaines, le « Design Thinking », il sera possible de faire ressortir les raisons qui justifient la pertinence de la mise en œuvre d'un Commandement cybernétique comme stratégie contre la cybermenace. Ce modèle propose une approche conceptuelle qui met l'accent sur la pensée critique, l'innovation et la créativité.

L'Association internationale pour l'éducation technologique de l'Amérique (America's International Technology Education Association - AITEA) défini le « Design Thinking » [Traduction] « [comme] un processus décisionnel itératif qui produit des plans par lesquels les ressources sont converties en produits ou systèmes qui répondent aux besoins et aux désirs humains ou de solution de problèmes »115. Selon les auteurs de l'article « The Art of Design : A

---

115 Stefan J. Banach et Alex Ryan, « The Art of Design : A Design Methodology », *Military Review* (March – April 2009), p. 105.

Design Methodology », le colonel (col) Stefan Banach, directeur de SAMS et Alex Ryan, Ph. D., professeur adjoint à la même école, la définition de AITEA implique que la conception n'est pas linéaire et que son processus ne se termine pas avec le développement d'une solution. Puisqu'elle se concentre sur la solution des problèmes, elle requiert une ou plusieurs interventions et non seulement une connaissance situationnelle. Pour bien faire comprendre ce qu'ils entendent par la conception, les auteurs expliquent que les scientifiques décrivent comment le monde est, alors que les concepteurs suggèrent plutôt comment le monde pourrait être116. Dans un article récent, le bgén à la retraite Huba Wass de Czege explique la pertinence de ce modèle pour l'armée de terre des États-Unis (U.S. Army) et comment elle facilite les étapes de planification et d'exécution lorsqu'elle est combinée à la doctrine existante117. Ainsi il explique comment le général Petraeus a utilisé le « Design Thinking » pour conceptualiser la stratégie Anaconda, qu'il a repris en avril 2008 lors de sa présentation au Congrès pour représenter son approche opérationnelle afin de défaire Al-Qaeda en Irak. Au sujet de cette méthode de conception, Petraeus mentionne « que la pratique de la conception bénéficie d'une multitude de points de vue provenant des officiers militaires, des universitaires, des fonctionnaires des différents organismes gouvernementaux ou des organisations non gouvernementales (ONG) »118.

Une façon simplifiée de cette méthodologie est présentement utilisée à SAMS et comporte trois espaces spécifiques d'analyse telle qu'illustrée à la figure 4.1, soit le cadre

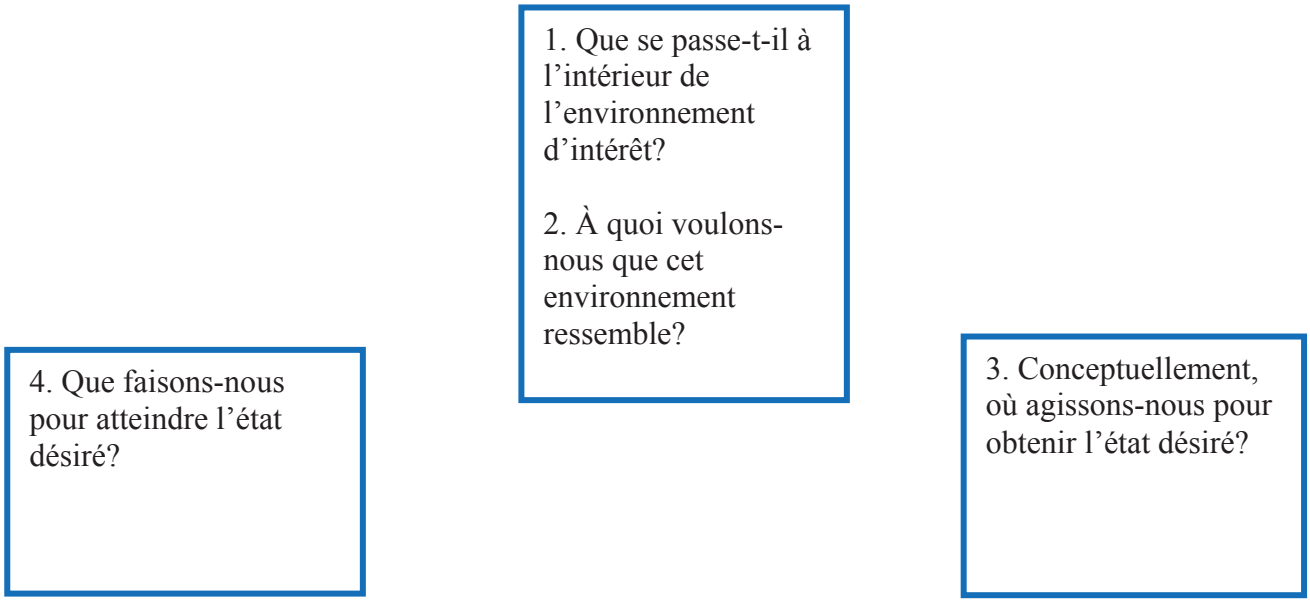
---

116 *Ibid*., p. 105.

117 Huba Wass de Czege, « Systemic Operational Design : Learning and Adapting in Complex Missions », *Military Review* (janvier – février 2009), p. 2.

environnemental, le cadre du problème et l'approche conceptuelle119. De plus, le lcol Celestino Perez, Jr., Ph.D., professeur adjoint au Collège de commandement et d'état-major de l'U.S. Army du Fort Leavenworth, précise quatre questions fondamentales que doit inclure la conceptualisation d'une solution [Traduction] :

1. Que se passe-t-il à l'intérieur de l'environnement d'intérêt?
2. À quoi voulons-nous que cet environnement ressemble?
3. Conceptuellement, où agissons-nous pour obtenir l'état désiré?
4. Que faisons-nous pour atteindre l'état désiré?120



---

118 David Petraeus, « Multi-National Force-Iraq Commander's Counterinsurgency Guidance », *Military Review* Special Edition, Couterinsurgency Reader II (août 2008), p. 211.

119 Banach et Ryan, « The Art of Design … », p. 109.

120 Celestino Perez, Jr., « A Practical Guide to Design : A Way To Think About It, and a Way to Do it », *Military Review* (mars - avril 2011), p. 44.

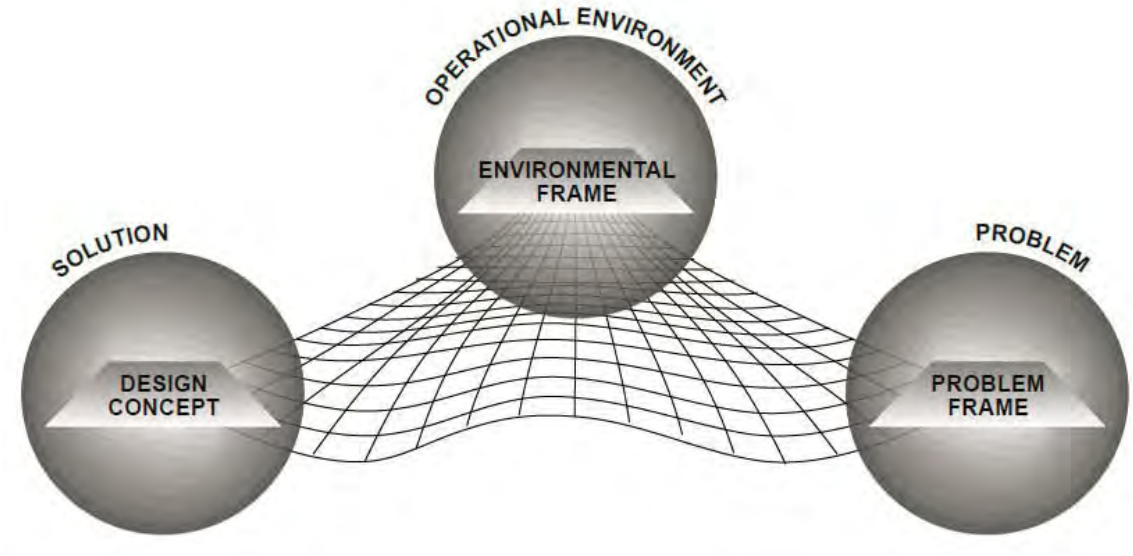


Figure 4.1 – Les trois espaces de la conception d'une solution

Source: Diagramme adapté de Banach et Ryan dans « The Art of Design : A Design Methodology ».

Chacun de ces trois espaces est regardé plus en détail dans les paragraphes qui suivent afin de développer une solution au problème de menaces du monde virtuel en tenant compte de l'environnement et de la réalité actuelle des FAC.

Cadre environnemental

Selon Banach et Ryan, la compréhension du cadre environnemental demande la conceptualisation de l'environnement comme un système qui comprend l'histoire, l'état actuel et les objectifs à atteindre des acteurs impliqués. De même, il est important de faire ressortir le flux des échanges et les relations entre les acteurs et d'identifier la propension de l'environnement à présenter des modèles de comportement121.

---

121 Banach et Ryan, « The Art of Design … », p. 110.

La figure 4.2 illustre ce premier espace de la conceptualisation pour les FAC au niveau du cybermonde et tient compte de la description des acteurs présentés dans les chapitres précédents.

En termes d'historiques, les éléments les plus importants et les références à utiliser pour développer la marche à suivre par rapport à la cybermenace sont les documents suivants : Canada numérique 150, le rapport du vérificateur général de 2012 et la Stratégie de cybersécurité du Canada publiée en 2010. La Stratégie de cybersécurité doit porter sur trois éléments essentiels, soit protéger les systèmes gouvernementaux, nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral et aider les Canadiens à se protéger en ligne122.

122 Sécurité publique Canada, *Stratégie de cybersécurité du Canada*…, p.7.

Historique
- COIC créé en 2012
- JCOT créé en 2012
- DG Cyber créé en 2011
- Canada numérique 150 publié en 2014
- Rapport vérificateur général de 2012
- Stratégie de cybersécurité publiée en 2010

Diplomatie
- Protéger la population contre les cyberattaques
- Créer une alliance entre toutes les ministères et organismes gouvernementaux impliqués avec la cybersécurité.
- Créer une alliance avec le secteur privé responsable des infrastructures essentielles
- Absence d'une politique étrangère sur la cybersécurité

Information
- Centre canadien de réponse aux incidents cybernétiques (CCIRC)

Militaire
- Plusieurs organisations des FAC impliquées avec la cybersécurité.
- Besoin de centraliser l'effort

Économie
- Favoriser la prospérité économique des Canadiens
- Protéger les propriétés intellectuelles

Alliances
- États-Unis (CYBERCOM)
- Five –Eyes Nations
- France
- OTAN

Système désiré
- FAC deviennent un acteur important de la cyberdéfense du Canada et au sein de nos alliances

Figure 4.2 – Cadre environnemental

Source: Diagramme adapté de Banach et Ryan dans « The Art of Design : A Design Methodology ».

Tel que définit au chapitre 3, les FAC comptent sur le GOIFC, plus précisément sur le CORFC afin de protéger ses propres réseaux et systèmes. Pour répondre à la menace toujours grandissante à l'intérieur du cybermonde, DG Cyber a été créé en 2011. Localisé à l'intérieur de la chaîne de commandement de CDF, l'objectif de cette nouvelle organisation est d'institutionnaliser les opérations des FAC à l'intérieur du cybermonde123. Bien que sa mission

123 BGen Greg Loos, « The Cyber environment : Adopting a CND mindset to secure our freedom of action » (Conférence donnée par DG Cyber le 20 septembre 2011), p. 2, site de DG Cyber sur le RÉD, consulté le 22 avril 2014, http://cfd.mil.ca/sites/intranet-eng.aspx?page=15861.

soit noble, DG Cyber doit travailler en étroite collaboration avec le GOIFC afin d'obtenir l'information courante sur les activités des réseaux d'entreprise et COIC pour intégrer tous les vecteurs relatifs à l'espace cybernétique aux diverses opérations des FAC.

L'analyse DIME (diplomatie, information, militaire, économie) procure l'information supplémentaire requise afin de définir l'environnement opérationnel des FAC à l'intérieur du cybermonde. Tout d'abord, du côté diplomatique, l'objectif primaire du gouvernement du Canada (GC) est de protéger la population contre toutes formes d'attaques cybernétiques qui auraient un impact majeur sur sa sécurité et sa prospérité124. Par conséquent, un partenariat solide entre tous les ministères et organismes gouvernementaux impliqués au niveau de la cybersécurité demeure la clé pour le gouvernement du Canada. Tel que mentionné dans la Stratégie de cybersécurité :

> Les Canadiens confient au gouvernement leurs renseignements personnels et organisationnels, et ils comptent également sur lui pour leur fournir des services. Ils s'en remettent au gouvernement pour défendre la souveraineté cybernétique du Canada de même que pour assurer la sécurité nationale et promouvoir nos intérêts économiques125.

Pour accomplir cette tâche à multiples facettes, le GC se doit d'utiliser tous ses intervenants du cyberespace d'une manière efficiente. En plus d'un partenariat à l'intérieur du gouvernement fédéral, la Stratégie de cybersécurité met l'accent sur un partenariat étendu en indiquant :

> [qu'] en collaboration avec les gouvernements provinciaux et territoriaux ainsi que le secteur privé, le gouvernement appuiera des initiatives et prendra des mesures

---

124 Sécurité publique Canada, *Stratégie de cybersécurité du Canada*…, p.1.
125 *Ibid*., p.7.

> pour renforcer la résilience cybernétique du Canada, y compris celles des secteurs d'infrastructures essentielles126.

Malgré les bonnes intentions du GC d'impliquer davantage le secteur privé pour sécuriser l'espace cybernétique, Ron Deibert indique dans son étude d'août 2012 sur la cybersécurité que les lois existantes ne sont pas assez directives et laissent beaucoup trop de discrétion aux compagnies de décider elles-mêmes quelles sont les infiltrations cybernétiques qui nécessitent d'être rapportées et quand le rapport d'incident doit être émis. Deibert croit même [Traduction] « [que] le manque de communication public en temps opportun [de la part du secteur privé] sur les violations des données ainsi que leur faible engagement de ressources pour la sécurité informatique sont deux enjeux majeurs de la sécurité cybernétique canadienne »127.

Tout comme ce qui se passe au niveau national peut avoir des répercussions au niveau mondial, ce qui se passe ailleurs peut revenir et nous atteindre ici au Canada. Ainsi, selon Deibert l'élément manquant de la Stratégie de cybersécurité du Canada est l'absence d'une politique étrangère pour le cybermonde128. Paul Meyer, un ancien employé des Affaires étrangères, Commerce et Développement Canada, argumente [Traduction] :

> [que] le temps est venu pour le Canada de développer une politique étrangère dédiée avec une stratégie diplomatique associée pour la promouvoir [...]. À moins d'engager de façon active le cybermonde comme un problème mondial, nous risquons de vivre dans un espace cybernétique largement déterminé par les autres129.

---

126 *Ibid*., p.7.

127 Ron Deibert, « Distributed Security as Cyber Strategy… », p. 19.

128 *Ibid*., p. 20.

129 Paul Meyer, « A Cyber Foreign Policy : Time for Canada to Get One », *Policy Options*, décembre 2010, consulté le 22 avril 2014, http://www.irpp.org/fr/options-politiques/bilan-de-lannee-2/a-cyber-foreign-policy-time-for-canada-to-get-one-fr-ca/

Parallèlement, une structure organisationnelle efficace et efficiente au sein des FAC en matière de ressources cybernétiques favoriserait les relations avec les forces armées de nos partenaires économiques principaux et leur permettrait, en plus, de devenir un joueur clé des alliances telles que l'OTAN et le FVEY. Ainsi, les FAC se positionneraient comme un acteur, à partir duquel le GC pourrait projeter sa politique étrangère.

Sans surprise l'échange d'information est définitivement au cœur de la cybersécurité. Jon Penney, professeur à « Schulich School of Law » de l'Université Dalhousie d'Halifax en Nouvelle-Écosse, membre du « Berkmark Certer for Internet & Society » de l'Université Harvard et chercheur du « Citizen lab » de l'École Munk des Affaires internationales de l'Université de Toronto, précise [Traduction] « [que] la divulgation complète, l'examen du public et la transparence sont, sans aucun doute, le fondement sur lequel des solutions plus intelligentes et complètes seront construites »130.

Tel que mentionné au chapitre 3, le GC a mis sur pied le CCRIC en 2005 afin de recueillir, analyser et diffuser de l'information sur les cybermenaces aux ministères fédéraux, aux gouvernements provinciaux et territoriaux et au secteur privé131. Le CCRIC doit servir de centre nerveux vers lequel toutes formes d'information détenues par les divers acteurs du cybermonde doivent être dirigées. L'information ainsi reçue par le CCRIC doit être rendue disponible à l'ensemble des intervenants du cybermonde, qu'ils proviennent de l'intérieur du GC ou de l'extérieur. Le partenariat doit être solide et transparent. À cette fin, les FAC se sont

---

130 Jon Penney, « Time to Get Transparent about Cyber Security », *InfoWar Monitor*, 29 juillet 2011, consulté le 22 avril 2014, http://www.infowar-monitor.net/2011/07/time-to-get-transparent-about-cyber-security/

131 Bureau du vérificateur général du Canada, « Protéger l'infrastructure …», p. 3.

engagées à fournir l'information au CCRIC. Dans sa présentation du 20 septembre 2011, DG Cyber a présenté le diagramme de transfert d'information à l'intérieur des FAC en réponse à un incident au niveau des réseaux d'entreprise.

Comme il est possible de le voir sur la figure 4.3, les FAC rendent compte au GC par le plan de gestion des incidents informatiques (Government of Canada Information Technology Incident Management Plan – GC IT IMP) à travers le CORFC.

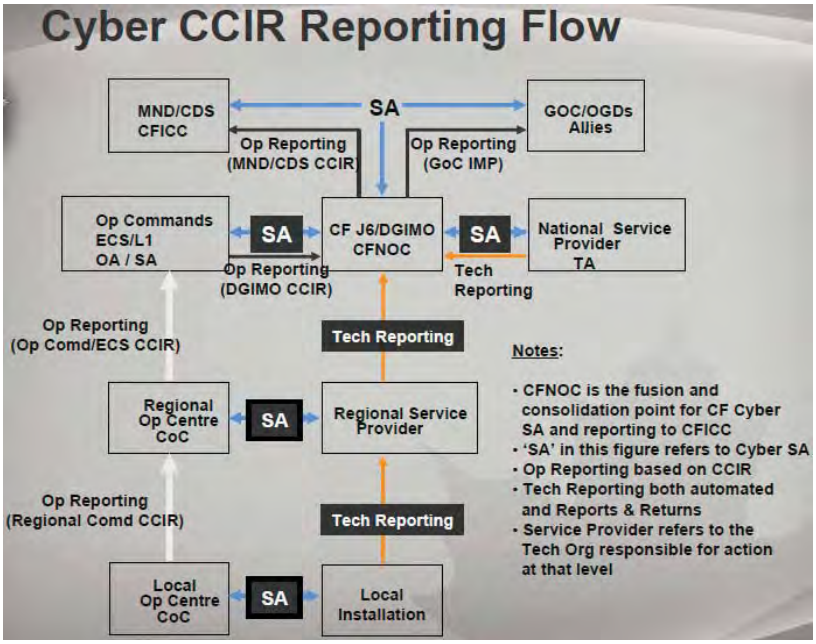


Figure 4.3 – Diagramme de transfert d'information lors d'incidents

Source: DG Cyber « The Cyber environment : Adopting a CND mindset to secure our freedom of action ».

Du point de vue militaire, Milton Mueller, professeur à « School of Information Studies » de l'Université de Syracuse et auteurs de deux livres sur la gouvernance de l'internet, émet des avertissements sur l'approche à adopter par les gouvernements pour la cybersécurité. Entre

autres, il prévient [Traduction] « [qu'] à bien des égards, la centralisation et la militarisation recherchées par les gourous de sécurité vont rendre la situation encore moins sécuritaire »132.

Bien qu'un peu extrême, ce type d'avertissement est pertinent pour les Forces armées des divers pays impliqués avec le cybermonde, car la militarisation de la cyberdéfense ne permettrait pas d'atteindre l'objectif recherché par la plupart des gouvernements des pays développés qui sont en faveur, tout comme les fondateurs, d'un internet libre et prospère. Pour les FAC, qui ont majoritairement des actions furtives au niveau de l'espace cybernétique, cet avertissement indique qu'ils doivent éviter de s'approprier d'un rôle trop étendu au sein de la cyberdéfense du Canada.

Pour revenir à la présente situation des FAC, les figures 3.1 et 3.2 démontrent la complexité de la chaîne de commandement au sein des différentes organisations impliquées avec le cybermonde. Ce manque de centralisation des actions favorise des initiatives indépendantes et non intégrées telles que le Protocole d'entente (PE) entre le Comité de la politique et des plans de défense (CPPC) de l'OTAN et SMA (GI) qui autorise l'échange d'information entre le CPPC et le CORFC133. Par contre, advenant que l'information échangée soit centralisée au sein du Commandement cybernétique et disponible à tous les intervenants du cybermonde, ce PE serait alors très pertinent.

---

132 Milton Mueller, « Feeble' governance? The push to discredit multistakeholder institutions », *Internet Governance Project*, 18 avril 2012, consulté le 22 avril 2014, http://www.internetgovernance.org/2012/04/18/feeble-governance-the-push-to-discredit-multistakeholder-institutions/

133 Ministère de la Défense nationale, *Memorandum of Understanding Between Canada and NATO – Cooperation on Cyber Defence* (Ottawa : SMA(GI), 2012).

En ce qui concerne le dernier élément de l'analyse DIME soit l'économie, le GC est conscient que le cyberespace est favorable à la prospérité de sa population et il s'engage, à travers la Stratégie de cybersécurité et Canada numérique 150, d'assurer la sécurité et la prospérité du Canada et de son cyberespace134. En d'autres termes, cela signifie que la population du Canada est libre d'utiliser le cybermonde pour socialiser, améliorer sa qualité de vie et pour y faire des affaires, tout en demeurant confiante que le cyberespace va demeurer sécuritaire, spécialement en ce qui concerne les propriétés intellectuelles, l'identité des utilisateurs et les infrastructures essentielles reliées entre elles par internet. Il s'agit d'un engagement important, surtout dans le cadre actuel où peu de gens comprennent le niveau d'implication pour rendre le cyberespace sécuritaire pour la population du Canada. D'ailleurs, même Canada numérique 150 est un exemple de ce manque de connaissances où l'information en surface est très bien étalée, sans pour autant aborder la sécurité en profondeur135.

Les alliances représentent déjà un ingrédient capital de l'environnement des FAC. Dans le contexte de la cybersécurité il faut donc aussi considérer les initiatives de notre partenaire principal, les États-Unis. En 2010, le CYBERCOM a été officiellement activé à l'intérieur de la structure organisationnelle du USSTRATCOM. Cette initiative a permis, entre autres, de concentrer les acteurs du cybermonde de DoD sous une même chaîne de commandement. De plus, selon Thomas Chen, les initiatives de DoD continuent de lancer un message clair à tous ses alliés à l'effet que les États-Unis reconnaissent l'importance et le sérieux des opérations cybernétiques.

---

134 Sécurité publique Canada, *Stratégie de cybersécurité du Canada*…, p.1; Industrie Canada, *Canada numérique 150*…, p. 5.

Dans le même ordre d'idée, mais à un niveau opérationnel et tactique, les alliés du FVEY apportent des initiatives et des visions qui mettent l'accent sur la portée de la cybersécurité. D'ici 2015, le Royaume-Uni aura mis sur pied le Groupe des opérations cybernétiques de la défense (Defence Cyber Operations Group – DCOG)136. Cette nouvelle organisation constituera la fédération des unités cybernétiques de la Défense et aura comme mission [Traduction] :

> […] de maintenir la cybersécurité à travers le ministère de la Défense (MoD) et assurer l'intégration cohérente des activités cybernétiques dans tous les volets des opérations de défense. Ceci permettra une approche beaucoup plus ciblée de la part de MoD au niveau du cyberespace, en assurant la résilience de nos réseaux vitaux et en positionnant le cybermonde au cœur des opérations de la défense, de la doctrine et de la formation. Nous travaillerons également à développer, tester et valider l'utilisation des capacités cybernétiques comme un moyen potentiellement plus efficace et abordable vers l'atteinte des objectifs de sécurité nationale137.

De même, l'Australie, qui sert souvent de référence pour les FAC, a annoncé dans sa Stratégie de cybersécurité l'intention de créer le Centre des opérations de cybersécurité (Cyber Security Operations Centre – CSOC). La Défense, les organisations du renseignement de la défense, les organisations de science et technologie de la défense et d'autres agences de renseignement et de sécurité gouvernementales seront toutes représentées au sein du CSOC138. En janvier 2013, le Premier ministre de l'Australie a publié sa plus récente stratégie de sécurité

---

135 Industrie Canada, *Canada numérique 150*…, p. 11-13.

136 Gouvernement du Royaume-Uni, « hc 106 Defence and Cyber-security – Session 2012-13 », 18 April 2012 (prepared 9 May 2012), consulté le 22 avril 2014, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm

137 Ministère de la Défense du Royaume-Uni, « Defence Cyber Operations Group », diapo 10, consulté le 22 avril 2014, http://www.google.ca/url?sa=t&rct=j&q=defence%20cyber%20operations%20group&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.science.mod.uk%2Fcontrols%2Fgetpdf.pdf%3F606&ei=JQ_zUJHMBqbc2QWo-oCwBA&usg=AFQjCNHy4kB9a-T6IlEVKybfV_HxZHHnDA&bvm=bv.1357700187,d.b2I

nationale dans laquelle il annonce au cours des prochains cinq ans, un processus de mise en place d'une politique cybernétique intégrée avec l'objectif de consolider les efforts du gouvernement en matière de cybersécurité139.

Tel qu'indiqué au chapitre 3, la France vient de créer son Commandement cybernétique de niveau opérationnel. Tout comme les autres alliés du Canada, la France consolide ses efforts et met l'accent sur l'importance de la cybersécurité pour sa propre sécurité et prospérité.

En plus des initiatives abordées précédemment, l'OTAN a pris acte du fait que le degré de sophistication croissant des cyberattaques imposait qu'elle s'attèle d'urgence à la protection de ses systèmes d'information et de communication et l'a annoncé dans son nouveau concept stratégique et dans sa déclaration du sommet de Chicago en 2012. La cyberdéfense a également été intégrée à l'initiative de défense intelligente de l'OTAN durant ce même sommet. Cette initiative vise à instaurer un nouvel état d'esprit afin que les pays unissent leurs efforts pour développer et maintenir des capacités dont ils ne pourraient supporter seuls les coûts de développement ou d'acquisition, dégageant ainsi des moyens permettant de renforcer d'autres capacités140. Pour qu'elles soient entendues de ses alliés, les FAC doivent devenir un joueur clé de ces initiatives. Cependant, pour atteindre cet objectif, un ajustement au niveau de la structure des FAC demeure essentiel.

Cadre du problème

---

138 Australia Department of Defence, « Cyber Security Operations Centre », consulté le 22 avril 2014, http://www.dsd.gov.au/infosec/csoc htm.

139 Gouvernement d'Australie, *Strong and Secure : A Strategy for Australia's National Security* (Canberra, AS : Department of the Prime Minister and Cabinet, 2013), p. 40.

140 OTAN, « L'OTAN et la cyberdéfense », consulté le 22 avril 2014, http://www.nato.int/cps/fr/natolive/topics_78170.htm

Dans son article intitulé « Seven Design Theory Considerations : An Approach to Ill-Structured Problems », le major Ben Zweibelson, un vétéran des guerres d'Iraq et d'Afghanistan et détenteur d'une maîtrise en art des opérations militaires du Programme de commandement et d'état-major des forces aériennes des États-Unis, aborde la définition de « meta-problem » utilisée par les théoriciens du design lorsqu'il s'agit d'un problème qui va au-delà du domaine tactique et linéaire. Le préfixe meta change la signification même du terme problème qui s'étend alors de spécifique vers une valeur holistique et beaucoup plus large. De plus, Zweibelson soutient qu'avec la théorie de la conceptualisation, les questions utilisées lors de l'analyse de l'environnement d'un problème soulèvent des questions supplémentaires, ce qui est une bonne chose avec la conceptualisation, car elles permettent une analyse en profondeur de l'environnement. L'élément important à retenir et à considérer dans le cadre de l'analyse environnementale des FAC et qui ressort de la réflexion de Zweibelson est que généralement les gouvernements et les forces armées adoptent des solutions simples et rapides à des problèmes complexes. Ils auraient tendance à aborder le problème seulement avec une vision à court terme. Tandis que les techniques traditionnelles de résolution de problème au sein des militaires résultent presque toujours par des ajustements procéduraux, le « Design Thinking » permet d'aborder en profondeur des phénomènes complexes et conduit à des processus émergents à l'intérieur d'un système complexe et adaptatif. Ainsi, le défi n'est pas uniquement dans des modifications à la doctrine[141].

---

141 Major Ben Zweibelson, « Seven Design Theory Considerations : An Approach to Ill-Structured Problems », *Military Review* (novembre- décembre 2012), p. 81.

En complément à Zweibelson, Banach et Ryan précisent que la compréhension du cadre du problème demande l'analyse, entre autres, des actions amies, ennemies et neutres afin de comprendre la logique de chacun des acteurs et pourquoi ils agissent ainsi à l'intérieur de l'environnement d'étude. Les auteurs mentionnent que souvent les systèmes de collaboration et les systèmes d'opposition créent des tensions en se faisant concurrence pour obtenir le soutien ou en tentant d'influencer les mêmes circonstances de l'environnement opérationnel. L'identification de ces points de convergence et de ces relations contribue à éclairer le vrai problème142.

Compte tenu de l'environnement et des acteurs présentés aux chapitres précédents, la figure 4.4 illustre ce deuxième espace de la conceptualisation pour les FAC au niveau du cybermonde.

142 Banach et Ryan, « The Art of Design … », p. 112.

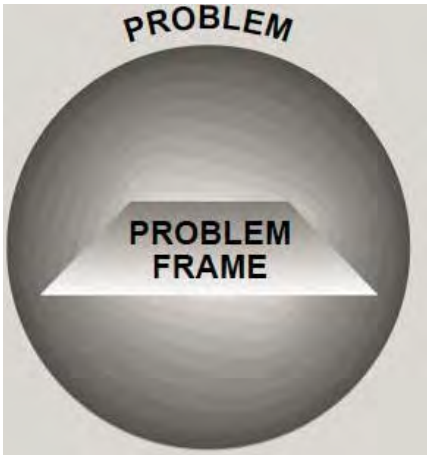
Système Courant

Forces Amies (Plusieurs chaînes de commandement)
- COIC (Lien avec JCOT)
- CDF (DG Cyber)
- CRD (Autorité pour SIGINT)
- SMA(GI) (DGOGI, GOIFC)

Forces Ennemies
- Cyberespionnage
- Cybercrime
- Cyberterrorisme
- Cyberguerre
- Cyberattaques contre les réseaux des FAC
- Cyberattaques contre les réseaux du GC
- Cyberattaques contre les infrastructures essentielles
- Vol industriel via le cybermonde

Système Désiré

Interventions
- Joueur clé de la cyberdéfense du Canada à travers un commandement pertinent, crédible et influent
- Partenaire important avec les autres ministères et organismes gouvernementaux
- Partenaire pour le secteur privé
- Acteur important au sein des alliances



Limites des actions
- Agir en collaboration avec les autres ministères et organismes gouvernementaux
- Partenariat important avec les États-Unis (CYBERCOM)
- Joueur clé au sein de l'OTAN

Communication
- Un commandement responsable d'obtenir et de fournir l'information concernant la cyberdéfense
- Partage de l'information avec les autres ministères et organismes gouvernementaux

Figure 4.4 – Cadre du problème

Source: Diagramme adapté de Banach et Ryan dans « The Art of Design : A Design Methodology ».

Tout d'abord, le présent système dans sa forme actuelle est à la source du problème quant à l'implication des FAC au niveau de la cyberdéfense. Tel que défini aux figures 3.1 et 3.2 ainsi qu'au sein du cadre environnemental de la section précédente, les organisations des FAC impliquées avec le cybermonde se retrouvent sous des chaînes de commandement différentes. Pour reprendre l'explication de Zweibelson, lorsque le problème est abordé d'une manière simple et linéaire, il en résulte une solution procédurale telle que la création du JCOT, ce qui constitue une solution ponctuelle, mais qui ne répond pas au fond du problème. De même, le lgén à la retraite Michael Jeffery mentionne dans son analyse de la Transformation de 2005

[Traduction] « [que] ces changements sont principalement le résultat de réactions tactiques aux problèmes par opposition à une vision cohérente de la direction vers laquelle les FAC doivent se diriger »143. Jeffery ajoute que les racines, la culture et l'héritage demeurent sacrés à l'intérieur de toutes organisations des FAC et que la résistance aux changements perdure toujours au sein des officiers généraux. À cette fin il précise ce qui suit [Traduction] :

> La planification stratégique continue d'être conduite par la croyance que toutes les opérations resteront conventionnelles et que les dernières années représentent une anomalie à la réalité. De plus, malgré tous les efforts d'entretenir des opérations interarmées, les environnements principaux des FAC demeurent centrés sur leur propre monde et beaucoup plus intéressés par des opérations combinées avec leurs alliés144.

En surface, la source du problème quant à la réponse aux cybermenaces semble provenir de la structure organisationnelle. Par contre, lorsque nous allons plus en profondeur, le problème se trouve aussi dans la résistance aux changements et l'inflexibilité de la chaîne de commandement à modifier la structure organisationnelle ce qui relève plutôt de la culture organisationnelle. Cet élément doit donc être pris en compte dans toute solution proposée.

Toujours reliée à l'institution, l'autorité dont dispose DGOGI, malgré son statut de commandant de formation, demeure limitée en ce qui concerne les ordres qu'il peut donner à des commandants opérationnels. DGOGI ne peut pas dicter à un commandant d'escadre ou de base de débrancher un ou ses réseaux en raison, par exemple, d'une infiltration reliée à une opération de cyberespionnage ennemie. Ce manque d'autorité augmente énormément le risque opérationnel des FAC qui sont très dépendantes de ses réseaux d'entreprise.

---

143 Michael K. Jeffery, *Inside Canadian Forces Transformation* …, p. 10.
144 *Ibid*., p. 10-11.

En résumé, les problèmes principaux au sein des FAC se situent dans sa propre chaîne de commandement et dans l'autorité qui est déléguée aux responsables de la GI/TI. De plus, il y a toujours des batailles d'égos lorsque des ressources sont prises à un commandement pour en donner à un autre. Ce fut le cas par exemple, lors du transfert des ressources de l'Armée canadienne vers le Commandement des Forces d'opérations spéciales du Canada (COMFOSCAN) et la mise sur pied du nouveau commandement et de sa nouvelle unité, le Régiment d'opérations spéciales du Canada (Canadian Special Operations Regiment – CSOR) en 2006.

Plusieurs problèmes persistent aussi au sein du GC. Ainsi, entre 2001 et 2009, le gouvernement a fait peu de progrès dans ses efforts pour diriger et coordonner la protection de l'infrastructure essentielle du Canada contre les cybermenaces, et ce, malgré l'évolution rapide de ces dernières. Depuis la publication de la Stratégie de cybersécurité en 2010, le gouvernement a réalisé certains progrès au chapitre de la protection de ses systèmes contre les cybermenaces, de la communication avec les propriétaires et les exploitants d'éléments de l'infrastructure essentielle.

Le rapport de 2012 du vérificateur général du Canada stipule :

> [qu'] il y a 11 ans, le gouvernement annonçait qu'il allait former des partenariats avec les autres ordres de gouvernement et avec les propriétaires et exploitants d'éléments de l'infrastructure essentielle du pays pour protéger celle-ci. Les réseaux sectoriels à l'appui de ces partenariats ne sont toujours pas pleinement établis et ils n'englobent pas l'ensemble des intervenants concernés. Le peu de progrès réalisé à cet égard nuit à la capacité de SP de communiquer avec les propriétaires et exploitants d'éléments de l'infrastructure essentielle145.

Le même rapport ajoute ce qui suit concernant l'efficacité du CCRIC :

> Sept ans après que le CCRIC ait été créé pour recueillir, analyser et diffuser de l'information sur les cybermenaces aux ministères fédéraux, aux gouvernements provinciaux et territoriaux et au secteur privé, de nombreux intervenants ne comprennent pas bien le rôle et le mandat du Centre. Dès lors, le Centre n'est pas en mesure de surveiller entièrement l'évolution des cybermenaces au Canada, ce qui l'empêche de fournir en temps opportun des conseils sur la façon de se défendre contre les nouvelles cybermenaces. De plus, le Centre n'est toujours pas en fonction 24 heures par jour, sept jours par semaine, comme on l'avait prévu au départ, ce qui peut retarder la détection de nouvelles menaces et la diffusion d'information à ce sujet aux intervenants146.

Une rectification de la situation actuelle au sein de la structure et des processus cybernétiques du GC devient donc prioritaire, avant même d'entreprendre des initiatives internationales avec nos alliés. Si le Canada veut être un partenaire influent de niveau international, il doit en premier lieu résoudre ses propres problèmes à l'intérieur de sa structure. Deibert est du même avis et soutient [Traduction] « [que] le Canada ne peut résoudre tous les problèmes d'ordre international, mais peut au moins commencer par résoudre ses propres processus et normaliser l'interaction de niveau international des compagnies canadiennes »147. À ce titre, une structure efficace et efficiente des ressources cybernétiques des FAC permettrait d'effectuer une meilleure analyse des menaces cybernétiques potentielles contre le Canada, de soutenir le GC dans la protection des infrastructures essentielles de la Défense nationale et d'appuyer les autres ministères et organismes gouvernementaux dans la protection et les réponses aux menaces cybernétiques contre les diverses infrastructures essentielles du Canada.

---

145 Bureau du vérificateur général du Canada, « Protéger l'infrastructure …», p. 3.
146 *Ibid*., p. 3.

147 Ron Deibert, « Distributed Security as Cyber Strategy… », p. 22.

En ce qui concerne les forces ennemies, le chapitre 2 aborde les quatre types d'agression cybernétique. Selon Ward, le cybercrime et le cyberespionnage constituent les menaces qui exigent une réaction immédiate.

Ainsi en 2013, la Maison-Blanche annonçait qu'elle envisageait de punir les pays qui sont toujours inactifs contre les pirates informatiques et qui volent délibérément des secrets corporatifs comme c'est le cas en Chine, en Inde et en Russie.

Selon le continuum des risques cybernétiques nationaux, les cybermenaces dirigées par un état représentent les plus dangereuses et impliquent les conséquences les plus dévastatrices pour la cible. Par contre, la menace peut aussi provenir d'un pirate informatique isolé et équipé d'un simple ordinateur à partir de sa résidence. Pour y remédier, il faut se demander quels critères d'analyse sont utiles pour distinguer le pirate qui relève du droit de la cybercriminalité de celui qui constitue un acte d'agression contre un état. Daniel Ventre propose de tels critères qui permettent de dresser le portrait de pirates informatiques et d'en imaginer une classification en fonction :

1. de leur âge;
2. de leur propension à rester discrets ou à rechercher la célébrité;
3. de leurs motivations;
4. de leur pouvoir de nuisance / de l'impact des attaques;
5. de la nature de leurs commanditaires;
6. de leur degré de liberté;

7. des cibles;

8. de leur degré de relation avec d'autres pirates;

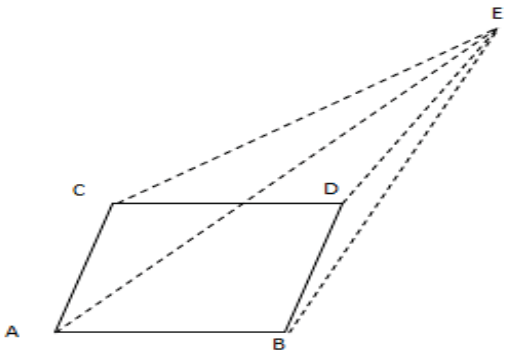
9. de leur capacité à penser et à suivre une stratégie; ou,

10. du niveau technique des attaques148.

En préambule à sa description des acteurs d'agressions cybernétiques, Ventre mentionne :

> [que] les doctrines militaires distinguent habituellement deux forces en présence dans une crise ou un conflit : son propre camp, qu'il faut protéger et celui de l'ennemi ou adversaire qu'il faut attaquer et vaincre. Les doctrines relatives aux opérations d'information, à la guerre de l'information, recourant aux diverses opérations que sont les opérations psychologiques, les attaques par réseaux d'ordinateurs, et autres, se sont longtemps appuyées sur une vision bipolaire de l'environnement […]. Mais il semblerait préférable de détailler les acteurs et leurs relations respectives. Distinguons :
> 1. Notre camp que nous désignerons par A;
>
> 2. L'ennemi, l'adversaire, que nous désignerons par B;
>
> 3. Les alliés de A, que nous désignerons par C;
>
> 4. Les alliés de B, que nous désignerons par D;
>
> 5. Les tiers, désignés par E, qui sont neutres dans la relation A-B-C-D149.

148 Daniel Ventre, *La guerre de l'information* …, p. 226-228.
149 *Ibid*., p. 223-224.



Figur

e 4.5 – Acteurs de la sphère de l'information - situation de conflit

Source: Diagramme produit par Daniel Ventre, *La guerre de l'information*

Selon cette description, E est une tierce partie, mais à travers laquelle une attaque des réseaux par virus informatique peut être lancée. Ce type d'attaque peut toucher sans discernement A,B,C ou D. Sans qu'il n'y ait de lien politique entre E et les autres, l'action qui émane de E, peut toutefois momentanément servir les intérêts de l'une ou l'autre des parties. Cette illustration, bien que simpliste comparativement à tous les acteurs réels du cybermonde, met en lumière le niveau de complexité de la cybermenace et qui doit être pris en compte et analysé par le GC et les FAC. L'environnement asymétrique avec lequel le Canada et les FAC ont dû composer dans leur intervention en Afghanistan est encore plus complexe dans le cas d'une cybermenace.

Pour compléter l'analyse du cadre du problème, il est nécessaire de regarder le système désiré afin de préparer la table pour la dernière section du « Design Thinking », soit l'approche

conceptuelle. À cette fin, trois paramètres doivent être considérés, le caractère des interventions, la limite des actions et les méthodes de communication.

Mis à part la responsabilité de protéger ses propres réseaux informatiques, la grande priorité des FAC dans le cadre de ses interventions dans le cybermonde est de devenir un contributeur de premier plan en soutien à la politique étrangère du GC. Les autres ministères et organismes fédéraux, de même que le secteur privé, s'attendent justement à ce que les FAC protègent ses propres réseaux et partagent l'information qu'elles possèdent au niveau de la cyberdéfense de notre pays. Également, ce niveau de partage d'information doit être reflété au sein des alliances et avec nos partenaires économiques principaux.

En regard à la limite des actions, les FAC doivent se limiter à agir en collaboration avec les autres ministères et organismes fédéraux et éviter toutes formes d'interventions suivant des initiatives parallèles. Pour être pertinentes, les bonnes personnes doivent être désignées pour les bons comités et les diverses initiatives du GC et ces personnes doivent demeurer membres des comités désignés pour des périodes prolongées. Pour l'instant, le manque de synchronisme au niveau de la chaîne de commandement des FAC ne favorise en rien la stabilité des différents membres des comités cybernétiques. En dépit du fait que les FAC veulent devenir un joueur clé au sein des comités et initiatives du GC, il demeure important de respecter les frontières délimitées par le rôle et les responsabilités du CSTC, qui est l'autorité technique canadienne au niveau du SIGINT.

À l'intérieur de ces limites, une meilleure organisation des ressources cybernétiques des FAC permettrait d'être un meilleur partenaire avec CSTC, le GC et ses alliés. De même, les FAC pourraient planifier et conduire des opérations cybernétiques en supportant le GC au niveau de sa

politique étrangère. Ainsi, la projection de la puissance cybernétique canadienne pourrait se faire à travers des mécanismes tels que celui de la Défense nationale.

En dernier lieu, la communication représente un critère d'importance pour le système désiré. Pour devenir un meilleur partenaire avec CSTC et soutenir le GC dans la mise en œuvre de sa politique étrangère, les FAC doivent mettre en place un mécanisme pour observer, analyser et signaler toutes formes de cyberintrusions à l'intérieur de ses réseaux d'entreprise. Pour ce faire, le processus d'échange d'information entre le CORFC et le CCRIC, tel qu'expliqué précédemment, doit être maintenu et amélioré. De même, le CORFC doit devenir un joueur clé au niveau du processus d'échange d'information avec les alliés et les alliances telles que le CYBERCOM et le CCD COE de l'OTAN à Tallinn en Estonie.

Pour atteindre cet objectif, des initiatives telles que le Protocole d'entente (PE) qui autorise l'échange d'information entre le CPPC et le CORFC doivent être maintenues, améliorées et mises en place lorsque requises. Par contre, ces dernières doivent être centralisées au niveau d'un seul commandement. De plus, CORFC doit demeurer à la fine pointe de la technologie et maintenir une expertise des plus spécialisées au niveau de ses ressources humaines. La mise en place d'un métier spécialisé du cybermonde au sein des FAC représente une option à considérer afin d'assurer une main d'œuvre à la hauteur des défis sans cesse émergents qu'impose le cyberespace. La création du Commandement cybernétique présente ici une option solide pour le commandement et le contrôle des divers vecteurs du cybermonde.

Approche conceptuelle

Maintenant que les portions environnement et problème ont été analysées, la prochaine étape porte sur la conception du modèle qui servira à résoudre, ou du moins à réduire les problèmes qui règnent dans l'environnement actuel.

Dans son article intitulé « Design : Tools of the Trade », M. Jack Kem, Ph.D., professeur adjoint au Collège de commandement et d'état-major de l'U.S. Army à Fort Leavenworth, aborde le sujet de l'état final désiré par la définition suivante [Traduction] :

> L'état final recherché est constitué des conditions qui représentent le contexte environnemental et lorsqu'atteint, répondent aux objectifs des politiques, des ordres et des directives émises au commandant. Plus précisément, l'état final recherché est la liste des conditions désirées qui décrivent le contexte d'un potentiel état futur de l'environnement opérationnel. Ainsi, l'état final recherché implique une transformation des conditions existantes aux conditions souhaitées150.

Selon Banach et Ryan, lors de l'élaboration de la solution, la synthèse est nécessaire pour créer une stratégie cohérente d'intervention. L'objectif est d'exploiter le potentiel de transformation des tensions du système, tout en atténuant les conséquences négatives reliées à l'instabilité et au changement. Une façon d'exploiter les tensions est d'identifier les capacités et les vulnérabilités qui résident avec le système d'opposition151.

Compte tenu de l'environnement et des problèmes présentés au courant de ce chapitre, la figure 4.6 illustre les considérations à mettre en lumière pour l'approche conceptuelle.

---

150 Jack D. Kem, *Design : Tools of the Trade* (Fort Leavenworth, Kansas : U.S. Army Command and General Staff College, May 2009), p. 16.

151 Banach et Ryan, « The Art of Design … », p. 112.

Stratégie

- À travers une réorganisation de sa structure organisationnelle, les FAC vont devenir un partenaire de premier plan pour CST et nos alliés. De plus, une telle réorganisation permettrait au GC de projeter la force cybernétique comme un instrument de pouvoir et de puissance de sa politique étrangère.

Activités parallèles

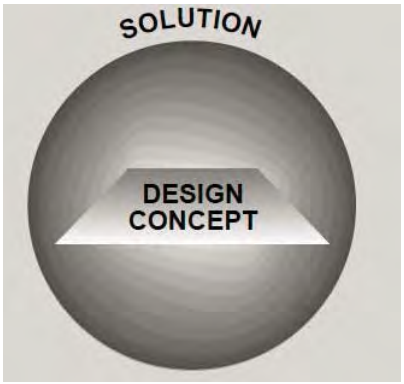
- DG Cyber
- JCOT
- CYBERCOM
- OTAN (CCD COE, NCIRC, Tallinn Manual)
- FVEY, France (Commandement cybernétique de niveau opérationnel)

Ressources

- Amalgamation des ressources de cyberdéfense des FAC sous un commandement unique ou réorganisation structurelle plus simple.

Relations

- CST
- Alliances
- GC
- Secteur privé



Risques

- Limites des actions
- Communication
- Développement de la force
- Emploi de la force
- Génération de la force
- Gestion du talent

Figure 4.6 – Approche conceptuelle

Source: Diagramme adapté de Banach et Ryan dans « The Art of Design : A Design Methodology ».

Le concept stratégique qui permettrait d'améliorer la situation courante est une réorganisation de la structure organisationnelle des FAC avec l'objectif clairement exprimé de devenir un partenaire de premier plan pour CSTC et ses alliés. De plus, une telle réorganisation permettrait au GC de projeter la force cybernétique comme un instrument de pouvoir et de puissance de sa politique étrangère.

Une telle réorganisation serait sans doute confrontée à d'autres activités et initiatives déjà en cours avec le potentiel de se retrouver à contrecourant les unes des autres. D'un autre côté, une unification des efforts permettrait de mettre l'accent sur les bonnes initiatives en plus de

donner l'autorité d'action à un commandant sur l'infrastructure d'entreprise des FAC. Une telle autorité diminuerait les risques opérationnels sur les réseaux d'entreprise des FAC et augmenterait sa crédibilité envers CSTC. De plus, ceci permettrait un engagement de meilleure qualité avec ses alliés, spécialement les États-Unis qui ont récemment mis sur pied le CYBERCOM sous la direction d'un général quatre étoiles152. De plus, tel qu'indiqué dans les précédents chapitres, la France et le Royaume-Uni ont également mis sur pied un commandement cybernétique de niveau opérationnel. Bien qu'à échelon moins élevé que le CYBERCOM, l'objectif demeure tout de même d'unifier les ressources et l'effort à l'intérieur de l'espace cybernétique. L'OTAN s'engage aussi à combattre la menace cybernétique avec plusieurs initiatives. Dans ce cas également, un constat du besoin d'unification des efforts est révélé par l'engagement des membres à partager leur savoir et leurs connaissances de la situation.

Le bien-fondé de la création de COIC en octobre 2012 repose en majeure partie sur le rapport de l'équipe de la transformation, dirigée par le lgén à la retraite Andrew Leslie. Une des justifications pour un employeur unique de forces était de profiter des capacités en développement telles que les forces du renseignement et cybernétiques :

> Parallèlement, le passage à une entité unique d'emploi des forces interarmées présente une occasion fort utile d'intégrer davantage les capacités [C3IRSR] des FAC en une seule organisation globale. Ainsi, on tirerait profit des progrès positifs réalisés par le CRD, afin de constituer une capacité nationale du renseignement qui engloberait les fonctions d'emploi des forces et de mise sur pied de forces pour les unités et les capacités établies, notamment le GOIFC et le CORFC. De plus, on permettrait ainsi l'élaboration et le développement de capacités émergentes, comme le cyberespace, qui auraient lieu à l'aide d'une solide surveillance axée sur l'emploi des forces, renforçant de cette façon la culture organisationnelle

---

152 Richard Clarke, « War From Cyberspace … », p. 31.

> opérationnelle qui est absolument nécessaire pour assurer une évolution saine de ces capacités hautement spécialisées153.

Selon les recommandations dans ce rapport, une consolidation des ressources cybernétiques des FAC représenterait la solution idéale pour résoudre les problèmes identifiés à la section précédente et devenir un partenaire de premier plan à l'intérieur de l'environnement décrit plus tôt dans ce chapitre. Contrairement à l'édification sous COIC, tel que semble proposer le rapport de l'équipe de la transformation, ce présent travail de recherche suggère plutôt une modification de la structure organisationnelle pour créer le Commandement cybernétique. Une analyse des avantages et inconvénients de ces différentes options est exposée plus loin dans ce chapitre.

Pour ce qui est des relations des FAC au niveau du domaine cybernétique, son partenaire principal doit sans aucun doute être CSTC. Une fois que la relation avec CSTC sera solidifiée, la prochaine étape sera d'établir une crédibilité éprouvée avec ses alliés à travers les alliances tels que l'OTAN et les FVEY. Au final, l'expertise des FAC pourra être mise à contribution afin de soutenir la protection des infrastructures essentielles canadiennes en collaboration avec le secteur privé.

Les risques reliés à un statu quo demeurent au niveau du contrôle des actions des diverses organisations cybernétiques des FAC. Sans une chaîne de commandement unique qui détient l'autorité de décider des actions, initiatives, participation à des comités, et autres, il y a risque de duplication de l'effort, d'un manque de synchronisme avec les priorités et que l'information

---

153 Chef de l'équipe de la transformation des FAC, *Rapport sur la transformation 2011* (Ottawa: Groupe Communication Canada, 2011), p. 73.

capitale ne parvienne pas aux bonnes personnes en temps opportun. Un processus de communication adéquat demeure la clé du succès afin de maintenir une connaissance de la situation à jour permettant d'agir selon l'émergence des menaces.

La génération et l'emploi de la force cybernétique demeurent aussi à risque advenant un statu quo de la présente structure organisationnelle étant donné le nombre de chaînes de commandement impliquées dans le commandement opérationnel des diverses organisations jouant un rôle dans le cybermonde. De plus, le développement de la force, qui est en majeure partie dirigée par CDF, ne sera pas coordonné de manière efficiente puisqu'il est aussi planifié et exécuté par les diverses chaînes de commandement des organisations concernées. Enfin, la gestion du talent n'est pas du tout considérée dans l'état actuel des choses, laissant place à de la formation ponctuelle selon les tendances du moment et du besoin opérationnel présent. À travers la gestion des carrières, qui est conduite par une autre entité des FAC, les diverses chaînes de commandement espèrent avoir la meilleure personne pour un travail et des tâches données.

Au final, le Commandement cybernétique semble la solution idéale pour combler le vide institutionnel existant au sein des FAC. Par contre, une telle réorganisation nécessitera un travail de longue haleine pour les organisations et tout le personnel impliqué avec cette restructuration.

La figure 4.7 suggère une structure potentielle du Commandement cybernétique. Bien entendu, celle-ci demeure une idée embryonnaire qui nécessitera une analyse plus complète, spécialement en ce qui a trait aux spécialistes et conseillers techniques tels que le conseiller juridique et le conseiller politique. De plus, une analyse subséquente sera requise pour déterminer les liens opérationnels et techniques avec les organisations extérieures aux FAC telles

que CSTC, le CCRIC, le CCD COE, et qui devraient être membre des divers comités consultatifs et législatifs du GC ainsi que des comités incluant le secteur privé.

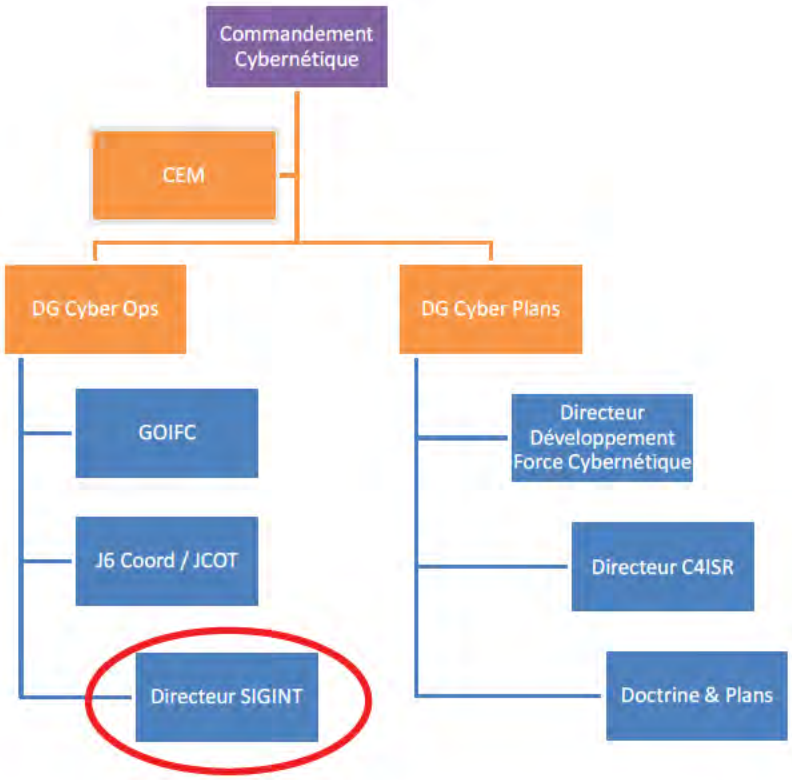


Figure 4.7 – Structure potentielle du Commandement cybernétique

Source: Diagramme adapté des organigrammes de SMA(GI) et VCEMD.

Cette nouvelle structure propose un amalgame de DGOGI et de DG Cyber, renommés dans l'ordre DG Cyber Ops et DG Cyber Plans. De plus, elle incorpore JCOT avec J6 Coord et un directeur pour l'autorité SIGINT en provenance de CRD. L'avantage majeur de cette réorganisation demeure l'économie de l'effort puisque les principaux acteurs du cybermonde sont maintenant réunis sous un même commandement, une solution favorable à l'environnement

et aux problèmes actuels analysés aux sections précédentes de ce chapitre. De plus, cette unification donnera l'autorité requise au nouveau commandement afin qu'il puisse prendre les actions nécessaires sur les réseaux d'entreprise des FAC, spécialement lorsqu'il y a infiltration reliée à une opération de cyberespionnage ennemie. En intégrant J6 Coord et JCOT sous DG Cyber Ops, la planification et l'exécution de toutes les actions requises à l'intérieur du cybermonde lors de la conduite d'opérations des FAC se feront sous l'autorité d'un seul commandant. Bien entendu, une étroite collaboration avec SMA(GI) et COIC s'avèrera capitale pour l'utilisation de l'infrastructure d'entreprise et pour obtenir l'effet désiré au moment choisi dans la conduite des opérations.

Un autre avantage sera l'incorporation d'un directeur, en provenance de CRD, qui détiendra l'autorité technique pour tout ce qui est SIGINT dans les FAC. De même, la chaîne de commandement de GOIFC se simplifiera, passant de trois (SMA(GI), CRD et COIC) à une seule.

Par contre, une réorganisation d'une telle ampleur s'accompagne de quelques désavantages. Le principal est sans aucun doute la résistance aux changements potentielle tel qu'indiqué précédemment dans ce chapitre par les citations du lgén Jeffery. De même, lorsque viendra le temps de transférer DGOGI de SMA(GI), le directeur SIGINT de CRD et DG Cyber de CDF vers le nouveau commandement cybernétique, il risque d'y avoir plusieurs tensions à l'intérieur des FAC et du MDN.

Dans leur article intitulé « The Rhythme of Change », Quy Nguyen Huy, professeur à l'Institut européen d'administration des affaires (INSEAD) de Fontainebleau en France et Henry Mintzberg, titulaire de la chaire Cleghorn à la Faculté d'administration de l'Université McGill de

Montréal, où il enseigne depuis 1968, identifient trois types de changement, le changement dramatique, le changement systématique et le changement organique154 . Parmi les trois types, seul le changement dramatique provient du haut de la chaîne de commandement. De plus, ils affirment que la combinaison des trois est nécessaire pour mettre en œuvre un changement durable et efficace155. Les auteurs représentent leur théorie par la pyramide du changement, illustrée à la figure 4.8.

Dans le cadre du changement suggéré au sein des FAC, ce triangle du changement se traduit tout d'abord par une volonté du CEMD en collaboration avec le SM et le ministre de la Défense nationale de publier un arrêté ministériel d'organisation (AMO) et une ordonnance d'organisation des Forces canadiennes (OOFC)156. Avant que le changement soit institutionnalisé, il est nécessaire d'avoir le soutien des officiers généraux impliqués avec cette réorganisation, c'est-à-dire le Vice-chef d'état-major de la Défense (VCEMD), CRD, CDF et SMA(GI). Enfin, pour que le changement soit un succès, les personnes qui feront le changement, soit les commandants des formations et des unités impliquées, particulièrement DG Cyber, DGOGI et GOIFC, doivent comprendre l'essence de ce changement majeur et en être partie prenante.

---

154 Quy Nguyen Huy et Henry Mintzberg, « The Rhythm of Change », *MIT Sloan Management Review* (été 2003), p. 79.

155 *Ibid*., p. 84.

156 Défense nationale et les Forces canadiennes, « La Direction – Histoire et patrimoine », consulté le 22 avril 2014, http://www.cmp-cpm.forces.gc.ca/dhh-dhp/adh-sdh/index-fra.asp

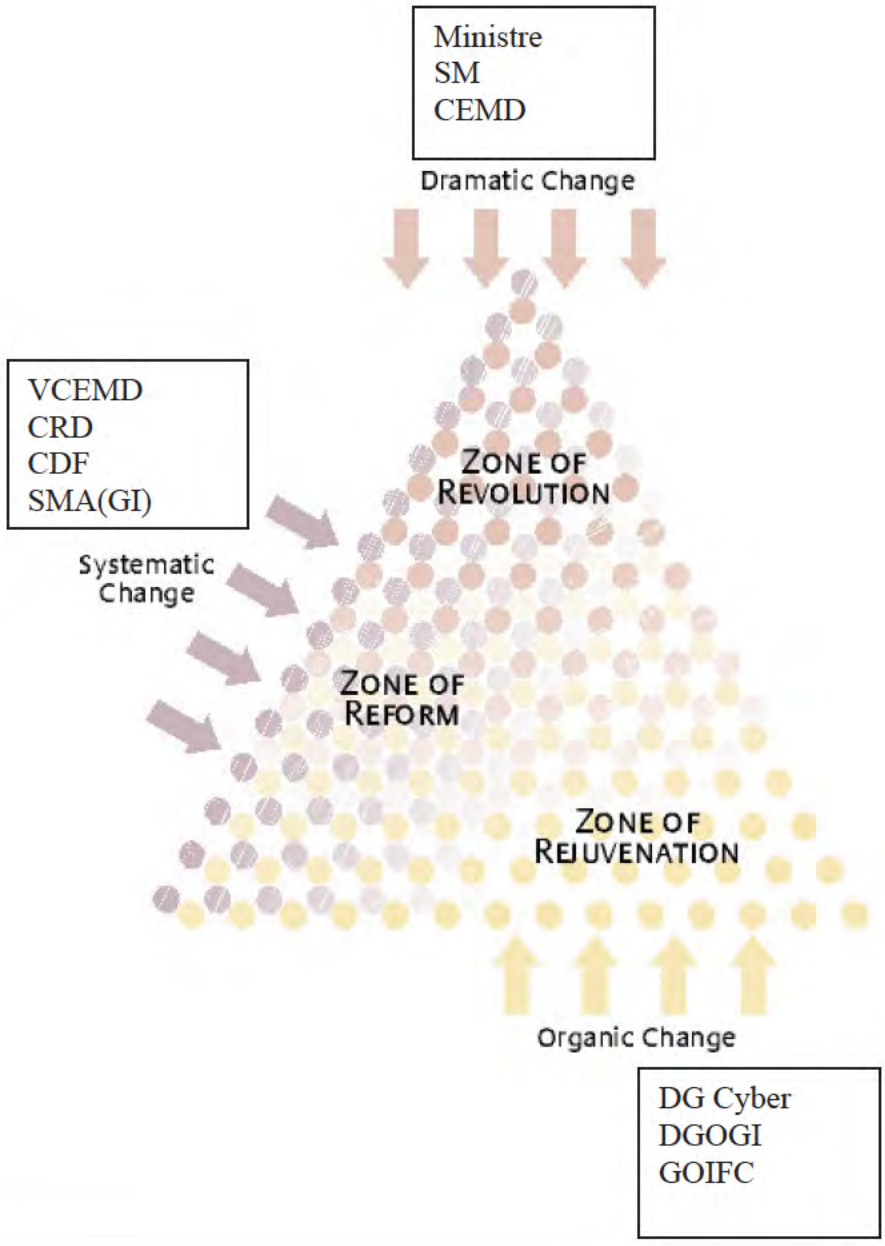

Ministre
SM
CEMD
Dramatic Change
VCEMD
CRD
CDF
SMA(GI)
Systematic Change
ZONE OF REVOLUTION
ZONE OF REFORM
ZONE OF REJUVENATION
Organic Change
DG Cyber
DGOGI
GOIFC

Figure 4.8 – Le triangle du changement

Source: Diagramme adapté de Huy et Mintzberg « The Rhythm of Change ».

Bien que cette solution demeure celle recommandée par l'auteur, l'analyse conceptuelle du Commandement cybernétique a conduit à deux autres solutions potentielles.

Options supplémentaires à considérer

Une première solution pourrait simplement être le statu quo tel que défini à la figure 3.2. Comparativement à la création d'un commandement cybernétique, le statu quo préserve la présente structure organisationnelle, évitant du coup la résistance aux changements des officiers généraux et de passer à travers les étapes de gestion du changement.

Cependant, cette option perpétue l'ensemble des inconvénients déjà énumérés en matière de capacité de réponse des FAC aux cybermenaces. Rappelons comme principal inconvénient la distorsion au niveau des organisations impliquées avec le cybermonde en raison de leur chaîne de commandement disparate. Ce désavantage majeur est défavorable à l'atteinte du résultat stratégique envisagée pour les FAC avec l'espace cybernétique. De plus, la diversité de la chaîne de commandement apporte un déséquilibre au niveau de la génération et du développement de la force, ce qui rend l'emploi de la force extrêmement difficile en opération.

La seconde option serait de créer des organisations cybernétiques sous chacun des trois environnements principaux (MRC, ARC, AC). Ces organisations seraient sous le commandement opérationnel des commandants d'élément, mais deviendraient sous le contrôle opérationnel de COIC lors d'opérations, tel qu'illustré à la figure 4.9. Tout comme le statu quo, cette dernière option permet de conserver l'intégrité de la structure organisationnelle. Par contre,

elle ajoute une couche additionnelle à la complexité de la présente chaîne de commandement des acteurs cybernétiques des FAC. De plus, la génération et le développement de la force demeurent non standardisés en raison de cette chaîne de commandement disparate. Enfin, avec cette option, personne ne détient l'unique autorité d'agir au sein de l'espace cybernétique afin de contenir des infiltrations ennemies lorsqu'elles surviennent.

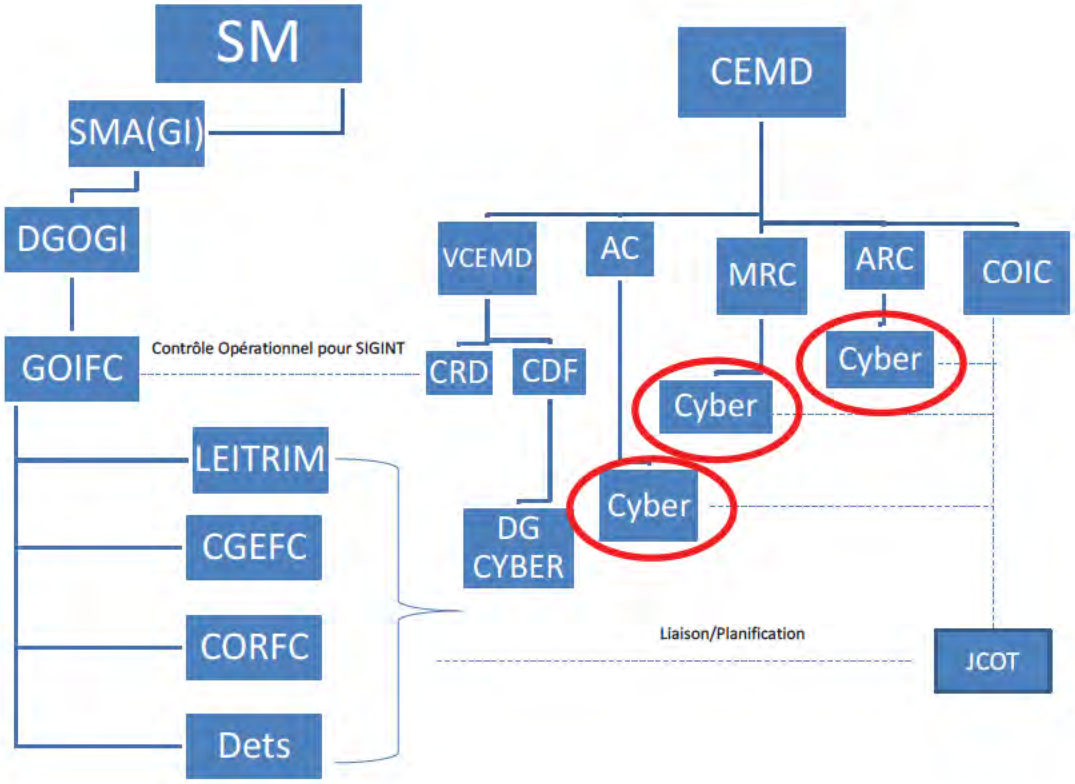


Figure 4.9 – Ajout d'unités cybernétiques au sein des environnements

Source: Diagramme adapté des diverses structures organisationnelles des FAC.

Bien que la création d'un commandement cybernétique entraîne une lourdeur en matière de gestion du changement, elle offre toutefois l'option de choix pour répondre à l'objectif stratégique des FAC à l'intérieur de l'espace cybernétique. Par contre, tel qu'indiqué précédemment, cette option suggère un niveau d'analyse supplémentaire, spécialement en ce qui concerne le rôle des conseillers techniques (conseiller juridique et politique), ainsi qu'au niveau des relations avec CSTC, les autres ministères et organismes fédéraux, le secteur privé et les alliés.

Résumé du chapitre

À partir du « Design Thinking », un modèle conceptuel utilisé au niveau des forces américaines et qui met l'emphase sur la pensée critique, l'innovation et la créativité pour élaborer des solutions, la proposition d'un Commandement cybernétique pour les FAC a été argumentée et justifiée. À cette fin, ce chapitre a cherché à consolider l'ensemble de l'information énumérée tout au long de ce travail de recherche pour analyser l'environnement et les problèmes au sein des FAC en matière de cybersécurité. Cette analyse et identification des problèmes constituent les deux premières étapes du « Design Thinking ».

Ainsi, il ressort que l'absence d'une politique étrangère du GC au niveau de la cyberdéfense présente une lacune capitale pour l'amélioration des processus d'intervention gouvernementale dans le cybermonde. Aussi, une structure organisationnelle efficace et efficiente des ressources cybernétiques au sein des FAC favoriserait les relations avec les forces armées des principaux partenaires économiques du Canada en plus de permettre aux FAC de devenir un joueur clé au sein des alliances telles que l'OTAN. De plus, une telle réorganisation

permettrait au GC de projeter, à partir des FAC, la force cybernétique comme un instrument de pouvoir et de puissance de sa politique étrangère.

Plusieurs autres problèmes au sein du GC et des FAC ont été identifiés en lien avec la nouvelle réalité des cybermenaces. Entre autres, le manque de progrès des politiques du gouvernement entre les années 2001 et 2009, ainsi que les heures d'activités encore limitées du CCRIC après neuf ans de mise en service, font en sorte que le GC n'évolue pas au même rythme que ses alliés principaux, ce qui a pour effet de miner la crédibilité canadienne en matière de cyberdéfense. Plusieurs experts recommandent que le GC améliore et définisse ses propres lois et processus à l'interne avant d'interagir sur la scène internationale. Pour les FAC, une réorganisation de ses ressources cybernétiques est également de mise afin de devenir un acteur pertinent et influent de la cyberdéfense du Canada.

La dernière phase de la démarche d'analyse reposait sur la conception du Commandement cybernétique. La proposition demeure une idée légitime, mais encore embryonnaire, car elle nécessiterait une analyse plus complète sur certains aspects. Ce qui est suggéré est de fusionner DGOGI et DG Cyber, et de les renommer DG Cyber Ops et DG Cyber Plans. De plus, il est proposé d'incorporer JCOT avec J6 Coord et un directeur pour l'autorité SIGINT en provenance de CRD. L'avantage majeur de cette réorganisation demeure l'économie d'effort, car les principaux acteurs du cybermonde seraient ainsi réunis sous un même commandement.

La proposition de création d'un Commandement cybernétique a été comparée avec deux autres options, soit le statu quo et la création d'unités cybernétiques distinctes sous les environnements (MRC, ARC, AC). L'avantage majeur de ces deux options est de conserver la présente structure organisationnelle des FAC, évitant du coup la résistance aux changements de

l'institution ainsi que d'avoir à compléter les multiples étapes de gestion du changement. Par contre, il s'agirait de solutions à court terme qui mettent l'accent plutôt sur la préservation et la protection des structures et non pas sur l'adaptation et l'innovation. La cybermenace représente une nouvelle force ennemie qui exige de sortir des sentiers battus pour y faire face avec une vision différente et surtout, avec une structure susceptible d'évoluer et de s'adapter aux changements rapides du monde virtuel et des progrès technologiques. Ce sont les raisons pour lesquelles l'auteur de ce présent mémoire, soutenu par l'analyse effectuée à partir d'un modèle éprouvé, favorise la mise en œuvre du Commandement cybernétique. Certes, il s'agit d'une solution exigeant un changement plus important, mais qui demeure sans conteste, l'option idéale pour faire face à ce nouvel espace de menaces extrêmement complexe.

CHAPITRE 5 – CONCLUSION

Le présent travail de recherche a mis un accent particulier sur la complexité de l'espace cybernétique, une nouvelle réalité mondiale qui est à la source de scandales majeurs avec entre autres le site WikiLeaks, la conception d'armes cybernétiques ingénieuses telles que le virus Stuxnet et l'infiltration des réseaux informatiques des firmes d'avocats industriels représentant Potash Corporation, une brèche qui s'est propagée jusqu'à l'intérieur de certains ministères et organismes gouvernementaux, dont Recherche et développement pour la défense Canada, le Secrétariat du Conseil du Trésor et le ministère des Finances. Face à cette menace proéminente qui porte atteinte à la sécurité du Canada et n'ayant toujours pas de rôle défini au sein de la cybersécurité du pays, les FAC se doivent de revoir leur stratégie. Une structure organisationnelle efficace et efficiente permettrait tout au moins de regrouper les efforts des organisations cybernétiques sous un seul commandement. Un tel changement permettrait sans

doute aux FAC de devenir un joueur de premier plan de l'espace cybernétique sur la scène nationale et internationale, un objectif auquel aspirent plusieurs hauts dirigeants des FAC.

À la base de cet objectif se trouve la compréhension du cybermonde où l'émergence d'internet a changé la vie de millions de personnes de façon positive, apportant prospérité, bien-être et liberté. Les Canadiens, qui comptent parmi les plus grands utilisateurs d'internet au monde, réalisent depuis le monde virtuel des revenus plus importants qu'avec l'agriculture. Par contre, une forte utilisation d'internet entraîne inévitablement des problèmes de sécurité. En effet, le Canada se classe au sixième rang des pays qui hébergent le plus de logiciels malveillants sur leurs serveurs. Les infrastructures essentielles, telles que les centrales électriques, les systèmes de distribution de gaz naturel, les systèmes d'approvisionnement alimentaires et les infrastructures des technologies de l'information, sont toutes reliées par ces serveurs et sont donc à risque. L'envergure des interrelations entre tous ces réseaux et systèmes connectés crée un environnement de dépendance mutuelle. En plus, presque tous les secteurs traversent les frontières publiques-privées et atteignent plusieurs couches gouvernementales. Par conséquent, il est primordial de mettre l'accent sur une collaboration saine et productive entre les paliers du gouvernement et le secteur privé en y imposant un agenda réaliste et complet.

Bien qu'une analyse sur la politique et les usagers ait mis en évidence l'incompréhension qui semble entourer l'espace du monde virtuel, l'intention n'est surtout pas de discréditer les progressions importantes réalisées au courant des dernières années pour mieux gérer le cybermonde, spécialement avec la publication de Canada numérique 150 et la Stratégie de cybersécurité du Canada. Par contre, le manque de législation et de juridiction de la plupart des gouvernements occidentaux limite leurs actions pour intervenir auprès des acteurs, spécialement

les propriétaires d'infrastructures essentielles qui négligent leur devoir de contrôle au niveau de la cybersécurité. Dans un sens, les politiques et les lois du monde virtuel sont mûres pour un changement de paradigme et ce n'est qu'en continuant d'identifier et de décrier les problèmes, tout en célébrant les réussites, que ces dernières finiront par voir le jour.

Tous les gouvernements alliés et partenaires économiques du Canada ont mis la cybersécurité au cœur de leur priorité. Les États-Unis ont récemment institutionnalisé le CYBERCOM, un commandement de niveau stratégique qui joue un rôle majeur avec l'unification des ressources cybernétiques de la défense américaine. La France a, quant à elle, créé son Commandement opérationnel de cyberdéfense qui permet l'intégration des éléments cybernétiques du ministère de la Défense sous une même chaîne de commandement tout en supportant les efforts pangouvernementaux du président de la République. D'ici 2015, le Royaume-Uni aura mis sur pied le DCOG, un commandement de niveau opérationnel qui permettra aussi un amalgame des diverses ressources et initiatives de la défense en matière de cybersécurité.

Une des lacunes importantes qui ressort de l'analyse du contexte canadien en utilisant la méthode « Design Thinking », est l'absence d'une politique étrangère du GC au niveau de la cyberdéfense, ce qui limite les possibilités d'amélioration des processus d'intervention gouvernementale dans le cybermonde. Une structure organisationnelle efficace et efficiente des ressources cybernétiques des FAC permettrait au GC de projeter la force cybernétique comme un instrument de pouvoir et de puissance de sa politique étrangère. De plus, une telle structure favoriserait les relations avec les forces armées des principaux partenaires économiques du

Canada et permettrait ainsi aux FAC de devenir un joueur clé au sein des alliances telles que l'OTAN.

Sur le plan conceptuel, ce qui est suggéré est de fusionner DGOGI et DG Cyber, et de les renommer DG Cyber Ops et DG Cyber Plans. De plus, il est suggéré d'incorporer JCOT avec J6 Coord et un directeur pour l'autorité SIGINT en provenance de CRD. L'avantage majeur de cette réorganisation demeure l'économie de l'effort puisque les principaux acteurs du cybermonde seraient ainsi réunis sous un même commandement. À ce stade, le modèle est toujours heuristique. Il n'est d'ailleurs pas conçu pour fournir la solution immédiate aux défis actuels des FAC avec l'espace cybernétique. Toutefois, il pourrait permettre aux hauts dirigeants de poser différentes questions empiriques ce qui permettrait de découvrir de nouvelles réponses pour proposer des solutions pratiques et novatrices. À l'image de la lettre d'Albert Einstein au président Roosevelt, ce travail de recherche attire l'attention sur des faits et des recommandations qui ne peuvent être simplement mis au rancart.

Appendice 1

Liste des acronymes

Acronyme (Français)	Définition	Acronym (English)
AC	Armée canadienne	AC
ARC	Aviation royale canadienne	RCAF
C3IRSR	Commandement, Contrôle, Communications, Informatique, Renseignement, Surveillance et Reconnaissance	C3IRSR
CCRIC	Centre canadien de réponse aux incidents cybernétiques	CCIRC
CDF	Chef du Développement de la force	CFD
CEM	Chef d'état-major	COS
CEMD	Chef d'état-major de la Défense	CDS
CGEFC	Centre de guerre électronique des Forces canadiennes	CFEWC
COIC	Commandement des opérations interarmées du Canada	CJOC
COMFOSCAN	Commandement des Forces d'opérations spéciales du Canada	CANSOFCOM
CORFC	Centre d'opération des réseaux des Forces canadiennes	CFNOC
CRD	Chef du Renseignement de la Défense	CDI
CRTC	Conseil de la radiodiffusion et des télécommunications canadiennes	CRTC
CSTC	Centre de la sécurité des télécommunications du Canada	CSEC
DGOGI	Directeur Général – Opérations (Gestion de l'information)	DGIMO

Acronyme (Français)	Définition	Acronym (English)
FAC	Forces armées canadiennes	CAF
FOS	Forces d'opérations spéciales	SOF
GC	Governement du Canada	GC
GOIFC	Groupe des opérations d'information des Forces canadiennes	CFIOG
GRC	Gendarmerie royale du Canada	RCMP
IC	Industrie Canada	IC
MND	Ministère de la Défense nationale	DND
MRC	Marine royale canadienne	RCN
ONG	Organisations non gouvernementales	NGO
OTAN	Organisation du traité de l'Atlantique Nord	NATO
RDDC	Recherche et développement pour la défense Canada	DRDC
RÉD	Réseau étendu de la Défense	DWAN
ROEM	Renseignement d'origine électromagnétique	SIGINT
ROHUM	Renseignement d'origine humaine	HUMINT
ROIM	Renseignement d'origine image	IMINT
ROSC	Régiment d'opérations spéciales du Canada	CSOR
ROSO	Renseignement d'origine source ouverte	OSINT
SCT	Secrétariat du Conseil du Trésor	TBS
SDCA	Stratégie de défense *Le Canada d'abord*	CFDS
SM	Sous-Ministre	DM

Acronyme (Français)	Définition	Acronym (English)
SMA(GI)	Sous-Ministre Adjoint (Gestion de l'information)	ADM(IM)
SP	Sécurité publique Canada	PSC
SPC	Services partagés Canada	SSC
VCEMD	Vice-chef d'état-major de la Défense	VCDS
	Réseau de l'Agence des projets de recherche avancés (États-Unis)	ARPANET
	Centre d'excellence pour la cyberdéfense en coopération (NATO)	CCD COE
	Commandement central américain	CENTCOM
	Directeur de la technologie	CTO
	Centre des opérations de cybersécurité (Australie et Royaume-Uni)	CSOC
	Commandement cybernétique des États-Unis	CYBERCOM
	Groupe des opérations cybernétiques de la défense (Royaume-Uni)	DCOG
	Directeur Général de la Cybersécurité	DG Cyber
	Département de la Sécurité intérieure des États-Unis)	DHS
	Département de la Défense des États-Unis	DoD
	Système de noms de domaine	DNS
	Conseil de réseautage fédéral américain	FNC
	Five-Eyes Nations (États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande et Canada)	FVEY
	Bureau du vérificateur général américain	GAO

Acronyme (Français)	Définition	Acronym (English)
	Plan de gestion des incidents informatiques du GC	GC IT IMP
	Société pour l'attribution des noms de domaine et des numéros sur internet	ICANN
	Détachement d'ingénierie d'internet	IETF
	Protocoles de communication de réseau informatique conçus pour être utilisés par internet	IP
	Société d'internet	ISOC
	Équipe des opérations cybernétiques interarmées	JCOT
	Ministère de la Défense (s'applique pour le Royaume-Uni, l'Australie et la Nouvelle-Zélande)	MoD
	Administration nationale de l'aéronautique et de l'espace (États-Unis)	NASA
	Centre technique de la capacité de réaction aux incidents informatiques de l'OTAN	NCIRC
	Renseignement National (États-Unis)	NI
	Commandement de la défense aérospatiale de l'Amérique du Nord	NORAD
	Agence nationale de la sécurité (États-Unis)	NSA
	Fondation nationale pour la science (États-Unis)	NSF
	Registre internet régional	RIR
	École d'études militaires et stratégiques avancées de Fort Lavenworth (États-Unis)	SAMS
	Système de contrôle et d'acquisition de données	SCADA
	Protocole de transport	TCP
	Royaume-Uni	UK

Acronyme (Français)	Définition	Acronym (English)
	États-Unis	US

BIBLIOGRAPHIE

30 trillion individual web pages. « How Search Works », accédé le 4 février 2014, http://www.google.com/intl/fr/insidesearch/howsearchworks/thestory

Adams, John. « The Government of Canada and Cyber Security : Security Begins at Home », extrait de *Journal of Military and Strategic Studies* Volume 14, Issue 2 (2012), p. 1.

Australie. Australia Department of Defence. « Cyber Security Operations Centre », accédé le 22 avril 2014, http://www.dsd.gov.au/infosec/csoc.htm.

———. Gouvernement d'Australie. *Strong and Secure : A Strategy for Australia's National Security,* Canberra, AS : Department of the Prime Minister and Cabinet, 2013.

Banach, Stefan J., et Alex Ryan. « The Art of Design : A Design Methodology », extrait de *Military Review* (March – April 2009), p. 105-115.

Barros, Hernan, et Walid Hejazi. *2013 Telus-Rotman IT Security Study*, accédé le 5 février 2014, http://www.telus.com/en_CA/content/pdf/whyTELUS/Rotman_2013_Full_Study.pdf?elq_mid=&elq_cid=1111327

Beidleman, Scott W. « Defining and Deterring Cyber War », travail rédigé dans le cadre du Programme de maîtrise en études stratégique,US Army War College, 2009.

boston.com, « Digital trench warfare », accédé le 5 février 2014, http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/06/11/digital_trench_warfare

Bowden, Mark Bowden. *Worm : The first Digital World War*, New York : Atlantic Monthly Press, 2011.

Brown, Martin, et Earl Zmijewski. « Pakistan Telcom Hijacks YouTube : Or how to SYN-flood DOS yourself while annoying everyone on the planet », APRICOT TAPEI 2008 educational conference, accédé le 5 février 2014, http://www.renesys.com/wp-content/uploads/2013/05/apricot-lightning-08.pdf

Brunner, Joel. *America the Vulnerable*, New York : The Penguin Press, 2011.

Business Insider. «Organized Crime Hackers Are The True Threat To American Infrastructure», accédé le 5 février 2014, http://www.businessinsider.com/organized-crime-hackers-are-the-true-threat-to-american-infrastructure-2013-3

Canada. Administration canadienne de la sûreté du transport aérien. *ALLER DE L'AVANT : Rapport annuel 2010*, Ottawa : Groupe Communication Canada, 2010, accédé le 4 mars 2014, http://www.acsta.gc.ca/sites/default/files/imce/Rapportannuel2010.pdf

———. Bureau du vérificateur général du Canada. « Protéger l'infrastructure canadienne essentielle contre les cybermenaces », *Rapport du vérificateur général du Canada*, Ottawa : Groupe Communication Canada, 2012, accédé le 4 mars 2014, http://www.oag-bvg.gc.ca/internet/Francais/parl_oag_201210_03_f_37347.html

———. Centre de la sécurité des télécommunications Canada. « Nos activités et notre raison d'être », accédé le 24 mars 2014, http://www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-fra.html

———. CRTC. « Note pour une allocution de Konrad von Finckenstein, c.r., Président, Conseil de la radiodiffusion et des télécommunications canadiennes », accédé le 4 mars 2014, http://www.crtc.gc.ca/fra/com200/2010/s100422.htm

———. Industrie Canada. *Canada numérique 150*, Ottawa : Groupe Communication Canada, 2014.

———. Ministère de la Défense nationale. A-FD-005-002/AF-002, *Concept cadre intégré*, Winnipeg : Bureau de publications de la 17e Escadre, 2009, accédé le 5 février 2014, http://publications.gc.ca/collections/collection_2012/dn-nd/D2-265-2010-fra.pdf

———. Ministère de la Défense nationale. Chef de l'équipe de la transformation des FAC. *Rapport sur la transformation 2011*, Ottawa: Groupe Communication Canada, 2011, accédé le 28 avril 2014,

———. Ministère de la Défense nationale. *Directives du chef d'état-major de la Défense à l'intention des Forces armées canadiennes*, Ottawa : Groupe Communication Canada, 2013.

———. Ministère de la Défense nationale. *Joint Cyber Operations Team (JCOT) : Concept of Operations*, Version 2.0, Ottawa : Joint Cyber Operations Team, mars 2013.

———. Ministère de la Défense nationale. *Memorandum of Understanding Between Canada and NATO – Cooperation on Cyber Defence*, Ottawa : SMA(GI), 2012.

———. Ministère de la Défense nationale. « Mission du CORFC », consulté le 24 mars 2014 sur le RÉD, http://img-ggi.mil.ca/aim-pgg/org/dgi-dgo/cfi-goi/cfn-cor/index-fra.asp.

———. Ministère de la Défense nationale. B-GL-300-001/FP-002, *OPÉRATIONS TERRESTRES*, Ottawa : MDN Canada, 2008.

———. Parlement du Canada. Comité sénatorial permanent de la sécurité nationale et de la défense, *Témoignages*, le lundi 5 novembre 2012, accédé le 24 mars 2014, http://www.parl.gc.ca/content/sen/committee/411%5CSECD/49784-f.HTM

———. Sécurité publique Canada. *Plan d'action canado-américain sur les infrastructures essentielles*, Ottawa : Groupe Communication Canada, 2010, accédé le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/cnd-ntdstts-ctnpln-fra.pdf

———. Sécurité publique Canada. *Plan Fédéral d'Intervention d'Urgence*, Ottawa : Groupe Communication Canada, 2009, accédé le 4 mars 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/mrgnc-rspns-pln/mrgnc-rspns-pln-fra.pdf

———. Sécurité publique Canada. *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, Ottawa : Groupe Communication Canada, 2010, accédé le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fra.pdf

———. Sécurité publique Canada. *Stratégie nationale sur les infrastructures essentielles*, Ottawa : Groupe Communication Canada, 2010), accédé le 4 février 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-fra.pdf

———. Services partagés Canada. « Mandat », accédé le 4 mars 2014, http://www.ssc-spc.gc.ca/pages/mndt-fra.html

CBC News. « Foreign hackers targeted Canadian firms », accédé le 5 février 2014, http://www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810

CBN News. « Israel Building "Digital Iron Dome" », accédé le 5 février 2014, http://www.cbn.com/cbnnews/insideisrael/2012/October/Israel-Building-Digital-Iron-Dome/

Chabrow, Eric. « Cybersecurity Bill Advances in House », extrait de *BankInfoSecurity*, 16 janvier 2014, accédé le 24 mars 2014, http://www.bankinfosecurity.com/cybersecurity-bill-advances-in-house-a-6401

Chen, Thomas M. *An Assessment Of The Department Of Defense Strategy For Operating In Cyberspace,* Carlisle : United States Army War College Press, 2013.

Clarke, Richard. « War From Cyberspace », extrait de *The National Interest*, (novembre/décembre 2009), p. 31-32.

Clarke, Richard, et Robert K. Knake. *Cyber War : The Next Threat to National Security and What to Do About It*, New York : HarperCollins Publisher, 2010.

Common Dreams. « Internet Tubes Speech Turns Spotlight, Ridicule onto Sen. Stevens », accédé le 4 février 2014, http://www.commondreams.org/headlines06/0715-06.htm

commScore. « 2013 Canada digital future in focus », accédé le 28 janvier 2014, http://www.comscore.com/fre/Insights/Presentations_and_Whitepapers/2013/2013_Canada_Digital_Future_in_Focus2

Cutts, Andrew. « Warfare and the Continuum of Cyber Risks : A policy Perspective », extrait de *The virtual Battlefield : Perspective on Cyber Warfare*, Fairfax : IOS Press, 2009.

Choucri, Nazli. *Cyberpolitics in International Relations*, Cambridge, Massachusetts : The MIT Press, 2012.

Cyr, Eric. « Strengthening the cybersecurity of critical infrastructure : The need of a targeted legislative reform », travail rédigé dans le cadre du Programme de commandement et d'état-major interarmées, Collège des Forces canadiennes, 2013.

Deibert, Ron. « Cyber Security : Canada is Failing the World », extrait de *Huffington Post*, 26 mai 2011, accédé le 4 mars 2014, http://www.huffingtonpost.ca/2011/05/26/cyber-security-canada-stephen-harper-g8_n_867136.html

———. « Distributed Security as Cyber Strategy : Outlining a Comprehensive Approach for Canada in Cyberspace », Reseach Paper prepared for the Canadian Defence & Foreign Affairs Institute, Toronto University, 2012.

Défense nationale et les Forces canadiennes. « La Direction – Histoire et patrimoine », accédé le 22 avril 2014, http://www.cmp-cpm.forces.gc.ca/dhh-dhp/adh-sdh/index-fra.asp

États-Unis. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, Washington, D.C. : U.S. Governement Printing Office, July 2011.

———. Executive Office of the President of the United States. *National Security Strategy*, Washington, D.C. : U.S. Government Printing Office, 2010.

———. Office of the National Counterintelligence Executive. *Foreign Spies Stealing US Economic Secrets in Cyberspace : Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Washington, D.C. : U.S. Government Printing Office, 2011, accédé le 24 mars 2014, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

———. United States Army Training and Doctrine Command. *Cyber Operations and Cyber Terrorism*, DCSINT Handbook no. 1.02, Fort Leavenworth, Kansas : Deputy Chief of Staff for Intelligence, 2005.

———. United States Government Accountability Office. *Defense Department Cyber Efforts : DoD Faces Challenges In Its Cyber Activities*, Washington, D.C. : U.S. Government Printing

Office, 2011, accédé le 7 avril 2014, http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=131495&lng=en

France. Ministère de la Défense. *Livre Blanc : Défense et Sécurité Nationale 2013*, Paris : Direction de l'information légale et administrative, 2013.

———. Ministère de la Défense. *Pacte Défense Cyber : 50 mesures pour changer d'échelle,* Paris : Direction de l'information légale et administrative, 2014.

Fisher, Eric A. « Creating a National Framework for Cybersecurity : An analysis of Issues and Options », extrait de *Cybersecurity and Homeland Security*, New York : Nova Science Publishers, 2005.

Forbes. « How Many Things Are Currently Connected To The "Internet Of Things" (OIT)? », accédé le 4 février 2014, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/

———. « The Growing Cyberthreat », accédé le 4 février 2014, http://www.forbes.com/2009/10/20/digital-warfare-cyber-security-opinions-contributors-john-p-avlon.html

Gates, Robert M. « Submitted Statement to Senate Armed Services Committee », *Hearing before Senate Armed Services Committee*, Washington, D.C. : U.S. Senate, 2009, accédé le 24 mars 2014, http://www.loc.gov/law/find/gates.php

Glenny, Misha. « Canada's weakling web defenses », extrait de *Globe and Mail*, 18 mai 2011.

Gorman, Siobhan. « Chinese hackers suspected in long-term Nortel breach », extrait de *The Wall Street Journal*, 14 février 2012.

Graham, Andrew. The Macdonald-Laurier Institute. « Canada's Critical Infrastructre : When is Safe Enough Safe Enough? », accédé le 4 février 2014, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf

Grant, Tavis. « Canada urged to pull up its socks in Internet economy », extrait de *Globe and Mail*, 19 mars 2012.

Hammerseley, Ben. « My speech to the IAAC ». Discours, Information Assurance Advisory Council, Londres, GB, septembre 2011, accédé le 4 février 2014, http://benhammersley.com/2011/09/my-speech-to-the-iaac/

Hayden, Michael V. « The Future of Things Cyber », extrait de *Strategic Studies* Quartely 5, no. 1 (printemps 2011), p. 3.

Herley, Cormac. « The Plight of the Targeted Attacker in a World of Scale », extrait de *Microsoft Research*, Redmond, WA, 2010, accédé le 5 février 2014, http://research.microsoft.com/pubs/132068/TargetedAttacker.pdf

Huy, Quy Nguyen, et Henry Mintzberg. « The Rhythm of Change », extrait de *MIT Sloan Management Review* (été 2003), p. 79, 84.

ICANN. «L'UNESCO, l'ICANN et l'ISOC lancent une initiative pour l'élaboration d'un glossaire sur la gouvernance de l'Internet destiné à la communauté arabophone », accédé le 4 février 2014, http://www.icann.org/fr/news/announcements/announcement-27oct13-fr.htm

Internet Society. « Brief History of the Internet », accédé le 4 février 2014, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

———. « Que faisons-nous », accédé le 4 février 2014, http://www.internetsociety.org/fr/que-faisons-nous/influence

Jeffery, Michael K. *Inside Canadian Forces Transformation : Institutional Leadership As A Catalyst For Change*, Kingston : Canadian Defence Academy Press.

Jeuge-Maynart, Isabelle. *Le Petit Larousse Illustré*, Paris : Larousse, 2007.

Kem, Jack D. *Design : Tools of the Trade*, Fort Leavenworth, Kansas : U.S. Army Command and General Staff College, May 2009.

Kotter, John P. *Leading Change*, Boston, Massachusetts : Harvard Business Review Press, 2012.

Lamigeon, Vincent. « Cyberguerre : La France fourbit ses armes », extrait de *Challenges*, 21 janvier 2014, accédé le 7 avril 2014, http://www.challenges.fr/economie/20140121.CHA9418/cyberguerre-la-france-fourbit-ses-armes.html

Le Nouvel Observateur. « Stuxnet : Comment les États-Unis et Israël ont piraté le nucléaire iranien », accédé le 5 février 2014, http://rue89.nouvelobs.com/2012/06/04/stuxnet-comment-les-etats-unis-et-israel-ont-pirate-le-nucleaire-iranien-232728

Loos, Greg. « The Cyber environment : Adopting a CND mindset to secure our freedom of action », conférence donnée par DG Cyber le 20 septembre 2011, site de DG Cyber sur le RÉD, accédé le 22 avril 2014, http://cfd.mil.ca/sites/intranet-eng.aspx?page=15861.

Luiijf H.A.M., Kim Besseling, Maartje Spoelstra et Patrick de Graaf. « Ten National Cyber Security Strategies : A comparison », extrait de *Critical Information Infrastructure Security*, Volume 6983, Heidelberg : Springer, 2013.

Lynn, William J. « Defending a New Domain : The Pentagon's Cyberstrategy », extrait de *Foreign Affairs* Volume 89, no. 5 (septembre/octobre 2010), p. 97-102.

Meyer, Paul. « A Cyber Foreign Policy : Time for Canada to Get One », extrait de *Policy Options*, décembre 2010, accédé le 22 avril 2014, http://www.irpp.org/fr/options-politiques/bilan-de-lannee-2/a-cyber-foreign-policy-time-for-canada-to-get-one-fr-ca/

Mueller, Milton. « Feeble' governance? The push to discredit multistakeholder institutions », extrait de *Internet Governance Project*, 18 avril 2012, accédé le 22 avril 2014, http://www.internetgovernance.org/2012/04/18/feeble-governance-the-push-to-discredit-multistakeholder-institutions/

Murphy, Tara. « Security Challenges in the 21st Century Global Commons », extrait de *Yale Journal of International Affairs* Volume 5, Issue 2 (2010), p. 2, accédé le 4 février 2014, http://yalejournal.org/wp-content/uploads/2010/09/105205murphy.pdf

Napolitano, Janet. « Uncovering America's Cybersecurity Risk », conférence, « Arms race in Cyberspace? », Newseum, Washington, DC, 28 septembre 2012, consulté le 5 février 2014, http://www.nationaljournal.com/events/cybersecurity-summit

National Communications System. Supervisory Control and Data Acquisition (SCADA) Systems, Arlington, VA : Office of the Manager National Communications System, 2004.

NORAD. « **NORAD, USNORTHCOM Joint Cyber Center stands up** », accédé le 7 avril 2014, http://www.norad.mil/Newsroom/tabid/3170/Article/1738/norad-usnorthcom-joint-cyber-center-stands-up.aspx

Nye, Joseph S. « Power and National Security in Cyberspace », extrait de *America's Cyber Future : Security and Prosperity in the Informationoreign Age*, vol. 2, Washington, DC : Center for a New American Security, 2011.

OTAN. « L'OTAN et la cyberdéfense », accédé le 7 avril 2014, http://www.nato.int/cps/fr/natolive/topics_78170.htm

———. « NATO 2020 : Assured Security; Dynamic Engagement », accédé le 7 avril 2014, http://www.nato.int/strategic-concept/expertsreport.pdf

Parent, J.A.J. « North American Aerospace Defense Command », conférence, Collège des Forces canadiennes, Toronto, ON, 28 janvier 2014, avec l'autorisation du conférencier.

Penney, Jon. « Time to Get Transparent about Cyber Security », extrait de *InfoWar Monitor*, 29 juillet 2011, accédé le 22 avril 2014, http://www.infowar-monitor.net/2011/07/time-to-get-transparent-about-cyber-security/

Perez, Celestino. « A Practical Guide to Design : A Way To Think About It, and a Way to Do it », extrait de *Military Review* (mars - avril 2011), p. 44.

Petraeus, David. « Multi-National Force-Iraq Commander's Counterinsurgency Guidance », extrait de *Military Review* Special Edition, Couterinsurgency Reader II (août 2008), p. 211.

Porteus, Holly. *The Stuxnet Worm : Just Another Computer Attack or a Game Changer?*, Ottawa : Library of Parliement, 2010.

Reveron, Derek S. *Cyberspace and National Security : Threats, Opportunities, and Power in a Virtual World*, Washington, D.C. : Georgetown University Press, 2012.

Rial, Nerea. « NATO targets hacktivists in new cyberwar directive », extrait de *New Europe Online*, accédé le 7 avril 2014, http://www.neurope.eu/article/nato-targets-hacktivists-new-cyberwar-directive

Royaume-Uni. Ministère de la Défense du Royaume-Uni. « Defence Cyber Operations Group », diapo 10, accédé le 22 avril 2014, http://www.google.ca/url?sa=t&rct=j&q=defence%20cyber%20operations%20group&source=web&cd=2&ved=0CDoQFjAB&url=http%3A%2F%2Fwww.science.mod.uk%2Fcontrols%2Fgetpdf.pdf%3F606&ei=JQ_zUJHMBqbc2QWo-oCwBA&usg=AFQjCNHy4kB9a-T6IlEVKybfV_HxZHHnDA&bvm=bv.1357700187,d.b2I

———. Ministère de la Défense du Royaume-Uni. « hc 106 Defence and Cyber-security, Session 2012-13 », 18 April 2012 (prepared 9 May 2012), accédé le 22 avril 2014, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/writev/106/m01a.htm

Schmidt, Eric, et Jared Cohen. *The New Digital Age*, New York : Knopf, 2013.

Schmitt, Michael N. « International Law in Cyberspace : The Koh Speech and Tallinn Manual Juxtaposed », extrait de *Harvard International Law Journal*, Vol. 54 (décembre 2012), p. 14, accédé le 7 avril 2014, https://www.usnwc.edu/getattachment/5067e23e-b849-4f60-a9f7-63e5238d4f6f/HILJ-Online_54_Schmitt.aspx

Singer, Peter, et Allan Friedman. *Cybersecurity and Cyberwar : What everyone needs to know*, New York : Oxford University Press, 2014.

Smith, Rupert. *The Utility of Force : The Art of War in the Modern World*, London:Penguin Books, 2005.

U.S.-Canada Power System Outage Task Force. « Final Report on the August 14, 2003 Blackout in the United States and Canada : Cause and Recommendations », accédé le 4 février 2014, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf

The White House. « Foreign Policy / Cybersecurity », accédé le 28 janvier 2014, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

———. « The White House Blog », accédé le 28 janvier 2014, http://www.whitehouse.gov/blog/author/Howard%20A.%20Schmidt
Tohn, David Tohn. « The FP Survey : The Internet », extrait de *Foreign Policy*, no. 188 (septembre-octobre 2011), p. 116.

Ventre, Daniel. *La guerre de l'information*, Paris : Lavoisier, 2007.

Wass de Czege, Huba. « Systemic Operational Design : Learning and Adapting in Complex Missions », extrait de *Military Review* (janvier – février 2009), p. 2.

Walkling, J.C. « Considerations : Canadian Forces' Efforts In The Electromagnetic Spectrum And Cyber Operating Environment », travail rédigé dans le cadre du Programme de commandement et d'état-major interarmées, Collège des Forces canadiennes, 2013.

Wark, Wesley. « Cyber-Agression and its Discontents », extrait de *Global Brief* (Fall 2012), p. 35-36.

Yale Law School. « Arms race in Cyberspace? », *Rebekka Bonner's blog* (blogue), accédé le 5 février 2014, http://www.yaleisp.org/2011/05/arms-race-in-cyberspace

ZDNet. « South Korea army, university to start cyberdefense major », accédé le 5 février 2014, http://www.zdnet.com/south-korea-army-university-to-start-cyberdefense-major-2062300991/

Zweibelson, Ben. « Seven Design Theory Considerations : An Approach to Ill-Structured Problems », extrait de *Military Review* (novembre- décembre 2012), p. 81.