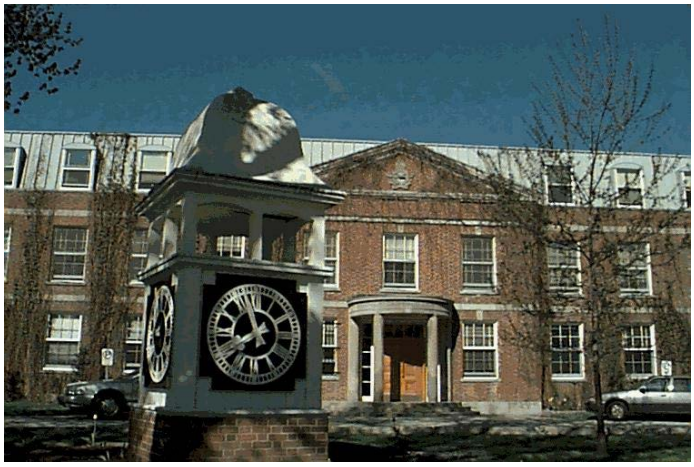
National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes



Cybersécurité au Canada : un changement de posture s'impose pour assurer la sécurité nationale

Major M.L.C. Belley

JCSP 40

Exercise *Solo Flight*

Disclaimer

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

PCEMI 40

Exercice *Solo Flight*

Avertissement

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

Canada

CANADIAN FORCES COLLEGE / COLLÈGE DES FORCES CANADIENNES

JCSP 40 / PCEMI 40

ESSAI SOLO FLIGHT

Cybersécurité au Canada : un changement de posture s'impose pour assurer la sécurité nationale

par maj M.L.C. Belley

12 mai 2014

Word Count: 5,868

Compte de mots : 5,868

« L'histoire nous enseigne qu'une civilisation, pour garder la maîtrise de son destin, doit se donner les moyens de sa sécurité. »

Jacques Chirac

INTRODUCTION

Cybercriminalité! La récente vulnérabilité logicielle appelée Heartbleed découverte dans la bibliothèque de cryptographie de l'outil OpenSSL[1] fait remonter à la surface une question de cybersécurité extrêmement pertinente. Ce type de faille, pouvant permettre à des internautes mal intentionnés d'exploiter les vulnérabilités d'un système prétendument capable de protéger, n'est pas à sous-estimer. Heartbleed, rendu public le 7 avril 2014, était en réalité actif depuis mars 2012. Environ 17 % des serveurs web dits sécurisés, soit approximativement un demi-million de serveurs, auraient été touchés par la faille au moment de la découverte[2]. Qualifiée de «dévastatrice» et reconnue comme l'une des menaces mondiales les plus importantes pour la sécurité en ligne, cette faille a eu un impact économique considérable pour le Canada. En plus d'affecter environ 900 citoyens par le vol de données personnelles, des pertes financières importantes ont été enregistrées en raison du délai inévitable que l'Agence du Revenu du Canada a accordé à la population en période de déclaration de revenus[3]. Est-ce que la stratégie canadienne de cybersécurité actuellement en vigueur est appropriée pour faire face à ce type de menace?

---

[1] *OpenSSL* est une boîte à outils de chiffrement comportant deux bibliothèques logicielle (libcrypto fournit les algorithmes cryptographiques et libssl implémente le protocole SSL) et une interface en ligne de commande (est une interface homme-machine dans laquelle la communication entre l'utilisateur et l'ordinateur s'effectue en mode texte).

[2] Wikipedia, « Heartbleed », consulté le 21 avril 2014, http://fr.wikipedia.org/wiki/Heartbleed.

[3] CBC, « Heartbleed bug may shut Revenue Canada website until the weekend », consulté le 6 mai 2014, http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742.

La thèse de cet essai propose que les cybermenaces actuelles et futures envers les infrastructures essentielles canadiennes représentent un danger concret pour la sécurité nationale. Toutefois, les recours juridiques et les lois actuelles sont imparfaites pour permettre au gouvernement de répondre à son mandat de protéger la nation contre les cybermenaces modernes. En effet, cet essai démontrera que la stratégie de cybersécurité impliquant les paliers gouvernementaux, le secteur privé et la population canadienne est défaillante. Le gouvernement fédéral doit modifier sa stratégie et adopter un plan d'action plus robuste pour assurer la cybersécurité au Canada. Il doit favoriser une approche globale plus efficace au niveau national et une représentation accrue sur la scène internationale dans l'optique de défendre plus adéquatement les intérêts nationaux.

Afin de prouver la validité de cette thèse, l'analyse sera divisée en deux parties. La première partie a pour objectif de conceptualiser la nature de la cybermenace. Pour ce faire, l'étude mettra l'accent sur la définition d'infrastructures essentielles et des menaces qui s'y rattachent. Par la suite, les différentes écoles de pensée seront analysées pour déterminer laquelle est la plus adaptée à la description de la réalité d'aujourd'hui. Cet examen des cybermenaces mettra en lumière son importance.

La deuxième partie étudiera l'efficacité de la stratégie canadienne pour faire face aux cybermenaces identifiées précédemment. Le rôle de la nation sur la scène internationale sera analysé à partir des failles constatées dans l'application des lois internationales. Ensuite, l'importance d'une approche globale pour faire face au défi de cybersécurité sera évaluée en regardant les obligations de trois acteurs clés : le gouvernement, le secteur privé et la population canadienne. Pour finir, une réflexion sur la pertinence d'adopter un plan d'action plus robuste misant sur la cyber-résilience sera faite.

Il est bon de mentionner que cet essai ne fait qu'une analyse rapide de la stratégie canadienne et qu'elle ne vise pas à faire des recommandations pour améliorer la situation. Les questions reliées à une telle recherche seraient trop nombreuses et dépasseraient largement l'étendue de ce travail.

LA CYBERMENACE

Définition de la cybersécurité

Les technologies informatiques sont utilisées dans de nombreux domaines comme, par exemple, la défense, l'énergie, l'industrie, l'administration et la finance. De plus en plus important dans nos vies, ce domaine est aussi de plus en plus complexe. Bien que l'utilisation des technologies soit apparue dans notre quotidien depuis très longtemps, c'est le niveau de connectivité qui complexifie la synergie dans le cyberespace[4]. Par conséquent, vient le besoin d'identifier les éléments vitaux à protéger appelé les infrastructures essentielles.

Le gouvernement du Canada définit les infrastructures essentielles comme étant « les processus, les systèmes, les installations, les technologies, les réseaux, les biens et les services qui sont essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et des Canadiennes, ainsi qu'au fonctionnement efficace du gouvernement[5] ». Ces infrastructures sont très souvent interreliées les unes aux autres et, deviennent ainsi très vulnérables aux attaques ciblées car la perturbation d'un secteur peut affecter l'ensemble du système. Comme les infrastructures essentielles reposent principalement sur des

---

[4]Jarno Limnell, « Le cyber change-t-il l'art de la guerre? », Sécurité globale, No 23 (2013/1), p. 34, http://www.cairn.info/revue-securite-globale-2013-1-page-33.htm.

[5]Sécurité Publique Canada, « Infrastructures essentielles », consulté le 5 mai 2014, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fra.aspx.

composantes d'information touchant le cyberespace, la cybersécurité devient donc nécessaire pour assurer la protection de la sécurité nationale. Compte tenu de l'interconnectivité de cette structure qui assure la sécurité, l'économie et la qualité de vie de la nation, il est possible d'avancer que « la perturbation de ces infrastructures essentielles pourrait se traduire en pertes de vie et en effets économiques néfastes, et pourrait considérablement ébranler la confiance du grand public[6] ».

Les infrastructures essentielles qui supportent le bon fonctionnement de la nation sont représentées selon dix secteurs spécifiques: la santé, l'alimentation, les finances, l'eau, les technologies de l'information et de la communication, la sécurité, l'énergie et services publics, le secteur manufacturier, le gouvernement et le transport[7]. Une caractéristique unique de ces secteurs est qu'ils détiennent un « element of mutual dependance [...] therefore be necessary to look at this view of critical infrastructure as a series of interacting systems, each with its own internal logic but playing in a complex field[8] ». En effet, on peut concevoir les impacts que pourrait avoir un secteur touché par une attaque ou une défaillance importante sur d'autres secteurs. Par exemple, les impacts qu'aurait une interruption des technologies de l'information et de la communication sur le réseau de la santé. Mais ces secteurs sont, non seulement, reliés les uns aux autres au sein de la nation, mais ils se retrouvent également très uni avec les structures américaines. Il est donc primordial de considérer le problème dans son ensemble en tant que système nord-américain plutôt que

---

[6] *Ibid.*

[7] *Ibid.*

[8] Andrew Graham, « Canada's Critical Infrastructure : When is safe enough safe enough? », Institute MacDonald-Laurier (2011), consulté le 02 mai 2014, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fra.aspx, p. 8.

purement canadien. « A glaring example of this [interconnection] was the power outage of 2005, when one failure in the United States put all of Ontario in the dark for a number of days[9] ». Tout comme pour la question de la sécurité des frontières qui fut particulièrement controversée après 9/11. Il est juste d'envisager que si nous ne semblons pas s'attaquer à la question de la cybermenace adéquatement, les États-Unis seraient portés à se dissocier de nous pour assurer la sécurité de leurs infrastructures essentielles par leurs propres moyens.

Afin de pouvoir définir ce que la cybersécurité implique, il est nécessaire de bien comprendre la nature des cybermenaces. Ces menaces gravitent autour de trois terminologies clés; cyberattaque, cyberguerre et cybercrime. La figure 1 démontre bien les différentes caractéristiques essentielles de chacun de ces trois termes.

	Type of cyber-action		
	Cyber-attack	*Cyber-crime*	*Cyber-warfare*
Involves only non–state actors		√	
Must be violation of criminal law, committed by means of a computer system		√	
Objective must be to undermine the function of a computer network	√		√
Must have a political or national security purpose	√		√
Effects must be equivalent to an "armed attack," or activity must occur in the context of armed conflict			√

Figure 1 – Caractéristiques essentielles des différentes actions cybernétiques
Source : Hathaway, *The Law of Cyber Attack*, p. 833.

Au niveau international, la validation du terme cyberattaque reste, sur le plan juridique, très controversé. Pour pallier cette problématique, certains experts suggèrent d'y

[9]Andrew Graham, « When is safe enough safe enough? », p. 8.

ajouter un élément relié à l'intention réelle à la base de l'action. Ainsi, une définition recommandée d'une cyberattaque pourrait se définir comme « any action taken to undermine the functions of a computer network for a political or national security purpose[10] ». Toutes autres cyberactions tombent dans la catégorie des cybercrimes.

Le Canada définit le terme cyberattaque plus largement. La *Stratégie de cybersécurité du Canada*, définit les cyberattaques comme « l'accès involontaire ou non autorisé à des renseignements électroniques et/ou des infrastructures électroniques ou matérielles utilisés pour traiter, communiquer ou entreposer cette information, ainsi que leur utilisation, leur manipulation, leur interruption ou leur destruction[11] ». Donc, une définition très large incluant toutes cyberopérations possibles pourvu que l'intention soit malveillante. De plus, le Canada attribue une catégorie à la nature de la cybermenace selon les motifs et intentions de l'agresseur : cyberespionnage et activités militaires parrainés par des états, utilisation d'internet par les terroristes et cybercriminalité[12].

En résumé, au niveau international, on essaie de plus en plus de faire une distinction entre cybercriminalité et cyberattaque alors qu'au Canada, le terme cyberattaque est vu au sens plus large validant le concept que les cyberattaques sont utilisées pour la conduite de cybercrimes. La Stratégie de cybersécurité du Canada définit le terme cybersécurité comme

---

[10]Oona Hathaway et coll., « The law of cyber attack », California Law Review 100, No 4 (2012), consulté le 07 mai 2014, http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf, p. 826.

[11]Ministère de la Sécurité publique, *Stratégie de cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité* (Ottawa : Groupe Communication Canada, 2010), p. 3.

[12]*Ibid.*, p. 5-6.

« le niveau d'intervention et les mesures d'atténuation nécessaires[13] » pour neutraliser la cyberattaque. Considérant que les infrastructures essentielles seront les plus susceptibles d'être ciblées dû à leur grande valeur pour la sécurité de la nation, il est possible de constater que la cybersécurité doit couvrir le spectre complet des opérations cybernétiques pour assurer la protection de cette structure critique.

Nature de la menace

Mais au-delà de la définition de cybersécurité, quelles sont les probabilités qu'une cybermenace affecte vraiment notre sécurité nationale? C'est en analysant les trois principales écoles de pensées que nous pourrons répondre à cette question : conservatrice, révolutionnaire et libérale.

L'école de pensée *conservatrice* avance, dans un premier temps, que le cyber espace ne représente pas un danger en soi. Thomas Rid consacre son œuvre complet à défendre cette position que la guerre cybernétique n'est pas une menace importante prétendant que la guerre dans le cyberespace est plus limitée qu'on peut le croire. C'est toutefois sa propre définition de différents types de cyber actions qui le pousse à poser une telle conclusion. Rid soutient que des menaces de toutes sortes remplissent effectivement le cyberespace, mais ne sous-entend pas pour autant le déclenchement d'une guerre. Présentant son objection à l'idéologie des alarmistes, il conclut en affirmant que : « there was no and there is no Hiroshima of cyber war. Based on a careful evaluation of the empirical record, based on technical detail and trends, and based on the conceptual analysis presented here, a future cyber-Hiroshima

[13] *Ibid.,* p. 3.

must be considered highly unlikely[14] ». Mais cette vision est quelque peu simpliste. Il est toutefois vrai de dire que « la cyberguerre n'a pas d'autonomie stratégique, elle ne peut exister par elle-même. [...] l'affirmation de Thomas Rid est donc juste: la cyberguerre n'aura pas lieu; mais la guerre traditionnelle, elle, est bien réelle et les cyberopérations peuvent être un de ses modes d'action[15] ». Par conséquent, il est primordial de garder en tête les impacts possibles d'une cyberattaque sur la sécurité nationale.

L'école de pensée *révolutionnaire*, quant à elle, suggère plutôt que le cyberespace est révolutionnaire dans son ensemble et surtout que la cyberguerre est inévitable. C'est du moins la philosophie de Richard Clarke, premier conseiller spécial pour la cybersécurité pour quatre présidents de la Maison Blanche, qui prône que la nouvelle menace de la guerre du futur est essentiellement reliée aux attaques menées dans le cyberespace, les menaces des armes nucléaires étant dépassées. Dans une entrevue donnée avec *The Economist* en 2012, il prédit la cyberguerre en 2013 comme inévitable. Il affirme que nous sommes à l'aube d'un pré 9-11 lorsqu'on parle de cyberguerre. Basé sur l'exemple du projet AURORA Idaho[16], il affirme que la perturbation, la destruction et les dommages sur les infrastructures critiques du pays auraient un impact considérable sur la sécurité nationale sont imminents[17]. Il voit les

---

[14]Thomas Rid, *Cyber war will not take place* (New York : Oxford University Press, 2013), p. 174.

[15]*Ibid.*, p. 306.

[16]En Mars 2007, des chercheurs de l'Idaho National Laboratory (INL) ont mené une expérience nommé le test Generator Aurora pour démontrer les conséquences d'une cyberattaque simulée sur un réseau d'alimentation (power network). Dans une vidéo diffusée par le U.S. Department of Homeland Security, une turbine de générateur, semblable à d'autres actuellement en usage aux États-Unis, est instruite par ordinateur de s'autodétruire. La turbine surchauffe et s'arrête de façon spectaculaire, après avoir reçu des commandes malveillantes à partir d'un pirate. Les chercheurs de l'INL enquêtaient sur les résultats possibles d'une cyberattaque dirigée contre une vulnérabilité qui, paraît-il, a depuis été corrigé.

[17]The Economist, « Interview with Richard A. Clarke: Cyber war in 2013 », visionné le 06 mai 2014, https://www.youtube.com/watch?v=6_ek8mugOUc.

représailles par l'action cybernétique et aucun autre moyen lorsque les États-Unis entreront dans le prochain conflit. Ce choix de l'attaquant lui permettra de s'en tirer sans conséquences dues au manque de préparation des États-Unis face à la menace. Dans une guerre conventionnelle entre les États-Unis et l'Iran, il y aura, selon lui, des éléments de cyberguerre qui affecteront directement la nation sur son propre territoire dû à la portée de l'arme[18]. Il ajoute que, selon l'Agence centrale de renseignement ou, en anglais, la Central Intelligence Agency, de 20 à 30 pays auraient des unités aptes à conduire la cyberguerre possédant une capacité offensive importante, incluant la Chine, la Russie, l'Israël, le Royaume-Uni, l'Allemagne et la Corée du Nord. Parce que la cyberguerre est peu coûteuse à mener, sa principale préoccupation est que le niveau de compétences pour mener de telles opérations se multiplie à un rythme impressionnant[19]. Vision très alarmiste, il présente toutefois une solution intéressante en raison de sa perception d'une politique de contrôle d'armes.

> When arms control works well, it reduces uncertainty, creating a more predictable security environment. By establishing some practices as illegal and some armament acquisition as a violation, arms control agreements can clarify what another nation's intentions might be. If a nation is willing to violate a clear agreement, there is less ambiguity about their policies. By prohibiting certain arms and practices, arms control can sometimes help nations to avoid expenditures that they might have been driven to only by fear that other nations were about to do the same. Agreed-upon international norms can be useful in gathering multilateral support against a nation that is an outlier[20].

---

[18]*Ibid.*

[19]*Ibid.*

[20]Richard A. Clarke et Robert K. Knake, *Cyber war: The next threat to national security and what to do about it* (New York : HarperCollins Publishers, 2010), p. 225.

Un contrôle du cyberespace selon les modalités du contrôle des armements conventionnels pourrait donc présenter des avantages importants dans l'effort de la normalisation de la malveillance humaine qui persiste à demeurer.

Il est possible de croire que la réalité se trouve entre ces deux écoles de pensée, qui est représenté par la perspective *libérale*. L'œuvre *Cyberspace and the State* défend bien la proposition que: « if cyberspace is not quite the hoped-for Garden of Eden, it is also not quite the pestilential swamp of the imagination of the cyber-alarmists[21] ». C'est une vision plus libérale qui défend une reconnaissance que l'environnement est effectivement en constante évolution, mais que toutefois, la présence et surtout l'influence parfois négative de l'être humain restent omniprésentes. C'est donc sans être pessimiste, mais plutôt en restant réaliste que l'on doit être préparé à toute éventualité d'une menace cybernétique. Dans son article *Cyber: la surprise n'est pas celle que l'on croit*, Olivier Kempf en fait bien la démonstration. En effet, il démontre avec doigté qu'un avènement se doit d'être surprenant selon la définition du concept de surprise stratégique[22] pour être considéré comme révolutionnaire et fondatrice d'un nouvel ordre stratégique. Or, le cyberespace ne satisfait pas ce critère car, paradoxalement, on en parle trop pour qu'elle soit une surprise[23].

> Le cyber est certes une révolution en soi, qui affecte en profondeur l'équilibre de l'humanité dans des proportions comparables à l'invention de l'imprimerie

---

[21]David J. Betz et Tim Stevens, *Cyberspace and the State : Toward a strategy for Cyber*-power (London : The International Institute for Strategic Studies, 2011), p. 129.

[22]La stratégie a deux dimensions : la grande stratégie (de l'ordre politique) et la stratégie militaire. La surprise stratégique imposera un changement de grande stratégie. D'autres changements moins importants modifieront seulement la stratégie militaire. Par exemple, les attentats du 11 septembre 2001 ou l'apparition de l'arme nucléaire ont amené la notion de « surprise stratégique ». Pour plus de précision, voir l'article d'Olivier Kempf, « Cyber : la surprise n'est pas celle que l'on croit ».

[23]Olivier Kempf, « Cyber : la surprise n'est pas celle que l'on croit », Revue Défense Nationale, No 767 (février 2014), p. 12.

> ou celle du moteur à explosion et de l'électricité. Toutefois, elle se produit à un rythme beaucoup plus élevé que ces précédentes révolutions technoanthropologiques. De ce point de vue, l'avènement du cyberespace constitue un bouleversement qui suscite de nombreux étonnements quant aux développements incessants qu'il produit. Pour autant, ces bouleversements n'amènent pas une «surprise stratégique[24].

L'être humain pouvant toutefois être imprévisible et malveillant, l'éventualité d'une cyberaction nuisible reste donc possible. Le coût d'une telle action étant possiblement trop important pour une nation, l'importance de demeurer vigilant et réaliste prend tout son sens. Même dans l'absence d'une surprise stratégique possible, il faut donc rester prudent et maintenir une veille efficace.

Réalité d'aujourd'hui

Dans un contexte où les théories reliées à la guerre irrégulière continuent à prendre de l'importance, les probabilités que le cyberespace soit exploité comme cinquième dimension sont grandissantes[25]. Dans ces conflits modernes, les acteurs étatiques et non étatiques exploitent de plus en plus tous les moyens pour conduire à bien leurs intentions en utilisant des armes traditionnelles sophistiquées mais également des tactiques et moyens plus irrégulières comme la criminalité ou même le terrorisme. Aujourd'hui, l'utilisation des cyberactions s'ajoute à cette liste et assiste à efficacement déstabiliser l'ordre existant.

Bien que l'utilisation des cyberattaques soit un outil parmi tant d'autres lors de conflits, la montée en flèche de son utilisation partout dans le monde s'explique selon quatre

---

[24]*Ibid.*, p. 14-15.

[25]Arnaud Coustillière, « La cyberdéfense : Un enjeu global et une priorité stratégique pour le ministère de la défense », Sécurité globale, No 1 (2013), p. 27-28.

caractéristiques : elle peut être peu coûteuse, simple dans le sens que des agresseurs ayant des connaissances limitées peuvent quand même imposer des coups importants, elle est efficace, mais surtout, elle représente un faible risque si délicatement planifié[26]. Elles représentent donc une bonne stratégie de contournement comme la guerre irrégulière. Les cyberattaques peuvent se rapprocher du concept de crime parfait. « Alors que des bombardements comportent plus de risques de déstabilisation d'une région et pourraient entraîner vraisemblablement un conflit avec l'adversaire, sur l'internet, c'est bien plus propre, intangible, voire invisible[27] ». Cette réalité aide à expliquer la monté en popularité de ces actions clandestines.

Si l'on regarde seulement les statistiques reliées à la cybercriminalité au Canada, on peut clairement constater une augmentation exponentielle de la menace. Le tableau 1, fourni par le Centre canadien de la statistique juridique de Statistique Canada, présente les données relatives aux crimes rapportés par les services de police au Canada incluant les cyberincidents.

Tableau 1 – Taux de cybercriminalité au Canada de 2008 à 2010 (en %)

	Total des crimes rapportés par les services de police	% relié à la cybercriminalité
2008	2360	14,6
2009	3334	18,9
2010	6626	24,9

Source: Statistique Canada, Centre canadien de la statistique juridique, demande d'accès à l'information numéro 619921.

[26]Ministère de la Sécurité publique, *Stratégie de cybersécurité du Canada*, p. 5.

[27]Ardavan Amir-Aslani, « Stuxnet vs Shamoom : La cyberguerre au Moyen-Orient », Sécurité globale, No 24 (2013/2), consulté le 26 avril 2014, http://www.cairn.info/revue-securite-globale-2013-2-page-9 htm, p. 10.

Malgré le fait que certains crimes sont possiblement non déclarés dans cette collecte de données, les chiffres démontrent quand même clairement une augmentation importante du taux de cybercriminalité passant de 14,6% sur 2360 crimes déclarés en 2008 à presque 25% des 6626 crimes déclarés en 2010. Ceci étant dit, il est possible de penser que plusieurs cyberincidents ne sont pas rapportés officiellement au système juridique en raison de la nature clandestine du crime discuté précédemment.

Alors que les théoriciens plus conventionnels affirment que la cyberguerre, au sens propre, n'est pas en ce moment une menace possible, l'histoire nous apporte à réaliser que l'impact des cyberactions ne devrait pas en être diminué pour autant. Dans un contexte de guerre conventionnelle, l'utilisation du cyberespace a bel et bien été prouvée. En combinaison avec d'autres outils plus conventionnels, les cyberattaques seront de plus en plus utilisées dans le futur. L'opération Orchard[28] en témoigne indéniablement. En effet, la combinaison habile d'une cyberattaque contre les systèmes de défense sol-air syriens et d'une attaque aérienne a permis à Israël, en octobre 2007, d'atteindre leur objectif de mission. C'est un programme de type Suter, un virus s'attaquant aux systèmes de défense

[28]L'opération Orchard est une opération militaire exécutée par l'armée de l'air d'Israël. Elle a bombardé et détruit, le 6 septembre 2007, un immeuble en Syrie, lequel abritait probablement des installations nucléaires à but militaire. La particularité de cette opération est que les forces israéliennes avaient perturbé, avant de lancer les frappes aériennes, les systèmes de défense sol-air de la Syrie par cyberattaques ciblées créant ainsi un corridor de protection pour leurs avions de chasse de pénétrer en territoire ennemi sans être vu. Une des opérations militaires combinant le cyberespace à l'application de la guerre conventionnelle les plus sophistiquée jusqu'à ce jour.

sol-air, qui a permis de perturber les capteurs du système leur permettant ainsi une couverture suffisante pour effectuer une attaque aérienne sur la Syrie[29].

Mais plus récemment, la cyberattaque a aussi été utilisée en isolation. C'est la découverte, en septembre 2010, du ver informatique Stuxnet[30] qui a contribué à faire évoluer cette dimension à un niveau jamais atteint dans le passé. Plusieurs rapports publiés attribuent ce logiciel malveillant à l'œuvre d'une alliance israélo-américaine ayant pour principal objectif d'infecter les systèmes des centrales nucléaires iraniennes de Natanz et de Bouchehr. Avec cette attaque ciblée qui confirme le passage du stade de la perturbation à celui de la destruction, on peut maintenant suggérer que, pour la cyberguerre, l'avenir est maintenant à nos portes[31].

LA STRATÉGIE CANADIENNE DE CYBERSÉCURITÉ

Maintenant que la définition de la menace a été faite, il est possible d'examiner l'efficacité de la stratégie canadienne de cybersécurité qui vise à assurer la sécurité nationale.

---

[29]Michel Baud, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », Politique étrangère, No 2 (été 2012), p. 310.

[30]Stuxnet, 2009-2010: A computer worm, dubbed Stuxnet, infected computers manufactured by Siemens and used in the Iranian nuclear programme. The worm is believed by experts to have been created by the United States military with assistance from Israel and scientists at Siemens. The effect of the worm in Iran was to cause centrifuges to turn far more rapidly than appropriate. In early 2011, officials in Israel and the US announced that Iran's nuclear programmes had been set back by 'several years.' The Stuxnet worm, however, affected computers in other countries as well, including India, Indonesia, and Russia. It is believed that 40 per cent of the computers affected were outside Iran. Stuxnet is said to be the 'first-known worm designed to target real-world infrastructure such as power stations, water plants and industrial units..

[31]James P. Farwell et Rafal Rohozinski, « Stuxnet and the Future of Cyber War », *Survival* 53:1 (2011), p. 23-40, https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf.

Rôle du Canada sur la scène internationale

Comme mentionnées plutôt dans ce travail, certaines notions dans le domaine restent très controversées et pour régler cette problématique, les états demeurent des joueurs clés. Oona Hathaway, professeur agrégé en droit international à l'université Yale Law School recommande que « the international community create a multilateral agreement. [...] it should offer a framework for more robust international cooperation in evidence collection and criminal prosecution of those participating in cross-national cyber-attacks[32] ».

Néanmoins, le manuel Tallinn, publié en mars 2013 par le NATO Cooperative Cyber Defence Centre of Excellence, représente un pas dans la bonne direction fournissant une interprétation du Droit international applicable aux conflits cybernétiques[33]. Toutefois, bien que ce manuel soit une avancée dans le domaine étant un ensemble de principes directeurs pour aider les nations à correctement interpréter les lois internationales, de nombreuses inconnues persistent[34].

Mais les défis non résolus ne manquent pas. Par exemple, une problématique extrêmement importante est celle de l'attribution. En effet, « a central problem for both the law enforcement and armed conflict approaches to cyber-security is determining the identity of the assailant[35] ». Comme les ordinateurs et systèmes informatiques ne sous-entendent pas

---

[32]Oona Hathaway, « The law of cyber attack », p.880.

[33]Youtube website, « CyCon 2012 – Michael Schmitt: Tallinn Manual Part 1 », visionné le 17 avril 2014, https://www.youtube.com/watch?v=wY3uEo-Itso.

[34]Arnaud Coustillière, « La cyberdéfense : Un enjeu global et une priorité stratégique pour le ministère de la défense », Sécurité globale, No 1 (2013), p. 30.

[35]Nathan Alexander Sales, « Regulating cyber-security », Northwestern University Law Review, Vol 107, No 4 (2013), p. 1524.

une notion d'appartenance à un individu précis comme pour une automobile par exemple, il est pratiquement impossible d'attribuer la responsabilité à un agresseur précis. La seule façon d'y parvenir effectivement est par l'utilisation de capacités de cyberespionnage que le Canada ne possède pas officiellement.

Un autre exemple est celui de la limite juridique affectant la sphère de recours pour les nations. En effet, les propriétés particulières du domaine cybernétique font en sorte que cette dimension ne respecte pas les frontières. À l'intérieur des frontières, les pays peuvent fixer des politiques et des lois qui sont souvent adéquates et facilement applicables pour répondre à la menace par exemple les lois en place au Canada pour légiférer la cyberpornographie impliquant des enfants. Le problème c'est lorsque l'on fait face à un agresseur en provenance d'un autre pays ce qui est souvent le cas avec les cyberattaques. Par exemple, si un attaquant en provenance de la Russie attaque le Canada, il n'existe aucun recours légal pour s'attaquer à la situation autre que par voie diplomatique. « A cyber investigation therefore typically involves multiple countries and requires tracing an evidentiary trail across international borders. This makes effective international cooperation essential to cyber crime investigations[36] ». Des traités ou des normes internationales sont donc requis pour pallier à ce type de problème et améliorer la sécurité de toutes les nations. Certains traités existent actuellement avec nos alliés les plus proches, mais une plus grande coopération internationale est nécessaire où le Canada se doit d'investir des efforts concrets pour le bien de la nation.

---

[36]Michael Vatis, « The Next Battlefield: The Reality of Virtual Threats », Harvard International Review, Vol 28, No 3 (automne 2006), consulté le 28 avril 2014, http://search.proquest.com/docview/59968204/6448448F4E4F41F9PQ/2?accountid=9867.

La politique américaine lancée en juillet 2011 avec Strategy for Operating in Cyberspace met l'accent sur quatre tactiques bien précises dont l'une d'elles est de favoriser une collaboration internationale. Les États-Unis avance qu'aucun état n'est capable, de par lui-même, de maintenir une défense efficace contre cette menace complexe qui ne se limite pas par les frontières et ainsi valorise une approche globale pour répondre à la problématique. « [A] cyber cooperation [will] develop collective self-defense and increase collective deterrence. [...] expanded and strengthened relationships [...] can maximize scarce cyber capabilities, mitigate risk, and create coalitions to deter malicious activities in cyberspace[37] ». Mais pour être admis à la table des grandes puissances lors de discussions sérieuses sur le sujet, encore faut-il être capable d'être vu comme contributeur utile. Toutefois, sans une capacité d'attaque ou d'espionnage de réseaux informatiques (Computer Network Espionnage & Computer Network Attack en anglais), le Canada peinera à se faire entendre.

À tout le moins, le Canada a grand intérêt à collaborer étroitement avec les Américains simplement en raison de l'interconnexion et interdépendance de leurs systèmes d'infrastructures essentielles mentionnés dans la première partie de cet essai. Considérant que « Canada's level of threat is directly linked to that of the United States, both in real and perceived terms[38] ». Une réalité représentant une opportunité pour le Canada de profiter d'un cyber parapluie des États-Unis dans le cadre d'une sécurité collective.

---

[37]Department of Defense, *Strategy for Operating in Cyberspace* (Washington, D.C.: Government Printing Office, juillet 2014, consulté le 03 mai 2014, http://www.defense.gov/news/d20110714cyber.pdf, p.10.

[38]Andrew Graham, « When is safe enough safe enough? », p. 17.

Approche globale nationale

Suite à l'analyse de la faiblesse de la stratégie canadienne d'un point de vue international, il est nécessaire d'approfondir l'examen d'une perspective d'efficacité globale au niveau national. Trois éléments essentiels sont proposés pour assurer l'efficacité d'une telle approche globale et seront évalués dans cette section soit : la dimension pangouvernementale, la collaboration avec l'industrie et le rôle de la population canadienne.

On peut facilement comprendre l'importance d'une approche pangouvernementale pour assurer la sécurité nationale d'un pays. L'article de Douglas Brook en fait bien la démonstration. De nos jours, un terme de plus en plus populaire est celui de la défense commune qui préconise l'idée suivante: « a whole of gouverment approach is suggested as a means for integrating and coordinating national security policies and programs[39] ». L'article fait référence au modèle canadien de l'approche pangouvernemental introduit il y a environ dix ans avec le Canada's Performance 2002 qui présentait une stratégie d'intégration entre les différents départements du gouvernement. La figure 2 démontre les rôles et responsabilités pour chacune des organisations clés du gouvernement fédéral.

[39]Douglas A. Brook, « Budgeting for national security : A whole of gouvernment perspective », J. of Public Budgeting, Accounting & Financial Management, Review 24, No 1 (printemps 2012), consulté le 27 avril 2014, http://search.proquest.com/docview/1019950248/fulltextPDF/E8F773E0ED144B5BPQ/1?accountid=9867, p. 32.

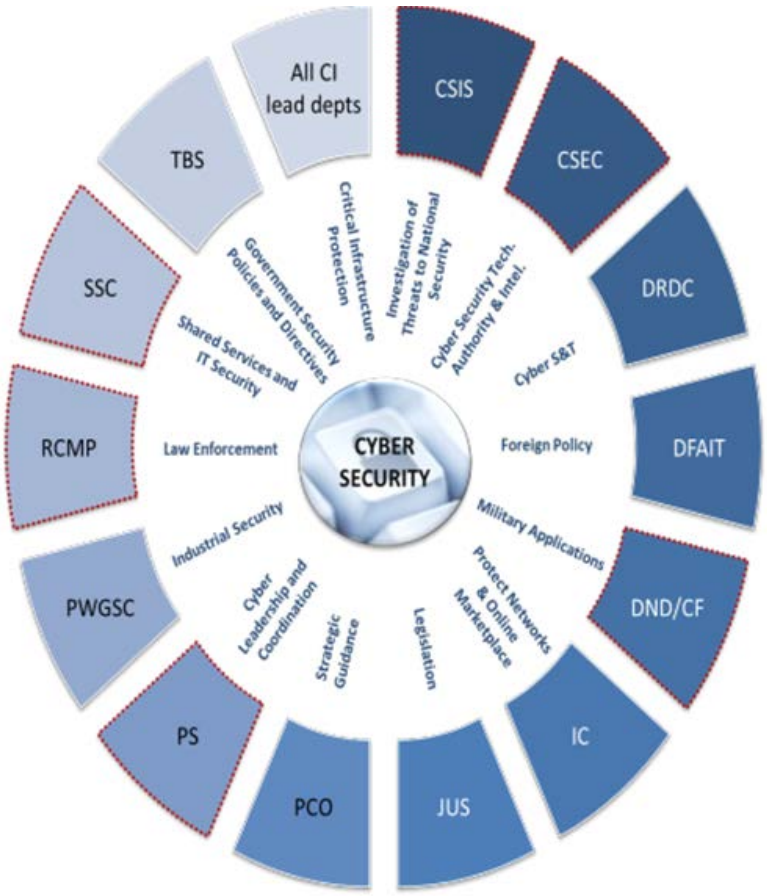


Figure 2 – Les rôles et responsabilités à l'égard de la cybersécurité
Source : Hawco, *Development of the CAF Cyber Capability*, Conférence GOFO, avec l'autorisation du conférencier.

Dans une telle approche globale, l'intégration des processus et la synchronisation des efforts sont essentielles. Or, il est clair que les efforts jusqu'à maintenant ont démontré certaines lacunes importantes de collaboration entre tous les intervenants impliqués et des problèmes d'intégration et synchronisation des efforts. Par exemple, Jim Robbins, président de la société d'ingénierie EWA-Canada, a indiqué lors d'une session du Comité sénatorial permanent sur la Sécurité nationale et de la défense en mai 2012 que plusieurs incidents majeurs n'étaient toujours pas rapportés parce que le Canada ne dispose pas un registre central pour consolider ce type d'information malgré la mise en place du Centre canadien de

réponse aux incidents cybernétiques (CCRIC). Il ajoute que le Canada est en fait le seul pays du G8 qui ne dispose pas d'un tel système capable de consolider les données de cyberincidents ce qui empêche la conduite d'une analyse rigoureuse nous permettant d'en tirer des leçons apprises essentielles[40]. Pourtant, la vocation première du CCRIC est de recueillir, analyser et diffuser l'information sur ce type d'opérations à tous les paliers gouvernementaux (fédéraux, provinciaux et territoriaux) et au secteur privé. Toutefois, le rapport du vérificateur général du Canada énonce bien que :

> 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 intervenants[41].

Cette enquête du vérificateur général du Canada, conduite en 2012, visait à évaluer si les efforts du gouvernement fédéral depuis la publication de son engagement à l'égard de la cybersécurité dans la *Politique de sécurité nationale* (2004), avec les autres paliers gouvernementaux et le secteur privé étaient adéquats pour la mise en œuvre de la stratégie contre les cybermenaces[42]. Trois conclusions majeures ressortent de ce rapport.

---

[40]Parlement du Canada, « Travaux parlementaires : Délibération du Comité sénatorial permanent de la Sécurité nationale et de la défense », consulté le 08 mai 2014, http://www.parl.gc.ca/content/sen/committee/411/SECD/06EVB-49519-f.HTM.

[41]Bureau du vérificateur général du Canada, *Rapport du vérificateur général du Canada à la Chambre des communes – Chapitre 3 : Protéger l'infrastructure canadienne essentielles contre les cybermenaces* (Ottawa : Groupe Communication Canada, 2012), p 2-3.

[42]*Ibid.*, p. 1.

Premièrement, le rapport souligne qu'entre 2001 et 2009, le gouvernement a fait peu de progrès pour coordonner et diriger le plan d'action envers l'établissement d'une protection de l'infrastructure essentielle du Canada contre les cybermenaces. Deuxièmement, le vérificateur général constate aussi que les réseaux sectoriels de l'infrastructure essentielle, qui sont des tribunes visant à favoriser les discussions sont inefficaces pour contribuer à l'établissement de partenariats solides au sein du gouvernement. Basé sur un principe de participation volontaire, lors de l'enquête, seulement cinq membres avaient apporté le sujet de cybersécurité lors d'une rencontre du comité. Et finalement, comme mentionnée plus tôt, l'enquête démontre que le CCRIC n'atteint pas les objectifs fixés par son mandat résultant, entre autres, d'une difficulté à partager l'information en temps opportun et l'absence d'une capacité de traiter l'information 24 heures sur 24, 7 jours du 7[43].

Malheureusement, on attribue ces problématiques de mise en œuvre de la stratégie de cybersécurité à un manque de ressources en personnel et financement nécessaires dans tout plan d'action robuste et efficace pour développer la capacité et à un manque d'imputabilité du gouvernement. De plus, on y associe un manque de connaissances dans le domaine, de l'inefficacité du traitement et partage d'information des incidents et de l'incapacité du gouvernement à faire pression sur les propriétaires et les exploitants d'infrastructures essentielles[44].

---

[43]Bureau du vérificateur général du Canada, *Rapport à la Chambre des communes*, p. 2, 15 et 18-20.

[44]Éric Cyr, « 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), consulté le 15 avril 2014, http://www.cfc.forces.gc.ca/259/290/299/286/Cyr.pdf#pagemode=thumbs, p. 19-20.

Le gouvernement fédéral se doit donc d'ajuster son plan d'action pour assurer la mise en œuvre de sa stratégie de cybersécurité. « Pour un gouvernement, aucune fonction ou obligation ne peut être plus importante que celle d'assurer la protection et la sécurité de ses citoyens[45] ». Ainsi, si la sécurité nationale repose sur les infrastructures essentielles comme indiqué dans la première partie, le gouvernement se trouve être le seul leader dans la mise en place d'un tel plan d'action. Étant le seul à pouvoir imposer des changements rigoureux au niveau de l'organisation, son implication active devient vitale.

Bien qu'il est facile de comprendre qu'une approche pangouvernementale soit importante pour affronter la menace cybernétique, il est aussi possible d'argumenter que la réalité dans lequel nous plonge le cyberespace est beaucoup plus complexe et demande donc une collaboration encore plus grande que celle limitée à une approche essentiellement pangouvernementale.

Dans cette approche globale proposée, l'industrie privée devient un joueur de premier plan au côté du gouvernement. James Farwell, expert en stratégie de la communication et de l'information et, anciennement consultant pour le Département de la défense américain, défend lui-même cette approche essentielle. Au Canada, il est estimé que 85% de toutes les infrastructures essentielles sont détenues et opérées par l'industrie, les provinces et les organismes non gouvermentales[46]. Mais, il est nécessaire de faire face à ce défi en pleine collaboration :

---

[45]Bureau du Conseil Privé, *Politique canadienne de sécurité nationale* (Ottawa : Groupe Communication Canada, 2010), consulté le 04 mai 2014, http://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf 7, p. vii.

[46]Andrew Graham, « When is safe enough safe enough? », p. 8.

> We need to move expeditiously but smartly to minimize cyber risks and vulnerabilities to critical infrastructure for both government and industry. To strengthen cyber security, we must remove legislative obstacles, develop partnerships between public and private interests, and expertly manage global [...] risks[47].

Le gouvernement devient un joueur clé pour assurer l'atteinte de la balance entre deux visions opposées: objectif ultime de la sécurité nationale qui motive le gouvernement face à l'ensemble des actions maximisant la marge de profit qui motive l'entreprise privée. La formulation d'une stratégie de cybersécurité plus robuste basée sur une collaboration accrue du domaine public et privé, dans une perspective d'approche globale, est donc la seule solution. On peut conclure qu'une modification de la législation est nécessaire si l'on veut prendre en considération certaine étude qui avance que « intelligence collection efforts can and should be provided - both classified and unclassified form (when possible) - to the private sector in order to help the owners and operators of the vast majority of America's information infrastructure better protect themselves[48] ».

Le partage d'information critique ne sera pourtant pas le seul défi de taille. Un engagement de toutes les parties de pair avec une confiance mutuelle sera un objectif difficile, mais nécessaire. « Gouverment programs intended for [...] critical infrastructure protection require collaboration engagement with private sector operators in order to be effective in accomplishing their intended goals[49] ».

---

[47]James P. Farwell, « Industry's Vital Role in National Cyber Security », Strategic Studies Quarterly (hiver 2012), consulté le 30 avril 2014, http://search.proquest.com/docview/1240323762/fulltextPDF/C24F76931E2848A1PQ/2?accountid=9867, p.34-35.

[48]James P. Farwell, « Industry's Vital Role in National Cyber Security », p. 17.

[49]Geoffrey T. Stewart, Ramesh Kolluru et Mark Smith, « Leveraging public-private partnerships to improve community resilience in times of disaster », International Journal of Physical (2009), consulté le 02

Le problème avec une telle approche est bien connu. Les entreprises sont de nature très réticente à l'idée de coopérer avec la concurrence pour des questions stratégiques de commerce. « Firms may be especially reluctant to share information with their competitors. If a firm discovers an effective way to defend its systems against a particular form of cyberintrusion, that information gives it a comparative advantage over rivals that may not be as adept at protecting their own networks[50] ». Il est encore plus important que le gouvernement fédéral intervient en tant que leader pour remédier à ce défi de taille.

Le citoyen est le troisième acteur clé dans une approche globale. En effet, la *Stratégie de cybersécurité du Canada* stipule bien que « les Canadiens et Canadiennes renforceront leur propre cybersécurité et celle de notre pays en général[51] ». Même si l'implication du citoyen dans la structure de protection des infrastructures essentielles est considérée comme indirecte, elle n'en est pas pour autant moins importante. Pourtant, une étude conduite par le Centre de recherche Pew aux États-Unis en janvier 2014 démontre qu'un Américain sur cinq est victime de cybercriminalité représentant une augmentation de 63% comparativement aux données de l'année précédente, des statistiques considérées similaires au Canada[52]. « Cybersecurity should not be an afterthought for the average citizen, but engrained within a nation's populace and deeply rooted in the citizens' day to day activities[53] ».

---

mai 2014, http://search.proquest.com/docview/232592275/fulltextPDF/9F41AC8D343B42F2PQ/1?accountid=9867, p. 350.

[50]Nathan Alexander Sales, « Regulating cyber-security », p. 1532.

[51]Ministère de la Sécurité publique, *Stratégie de cybersécurité du Canada*, p. 15.

[52]Pew Research Center, « Extremists, cyber-attacks top Americans' security threat list », consulté le 08 mai 2014, http://www.pewresearch.org/fact-tank/2014/01/02/americans-see-extremists-cyber-attacks-as-major-threats-to-the-u-s/.

[53]*Ibid.*

Le gouvernement détient une grande part de responsabilité pour assurer une éducation adéquate de la population canadienne. « To do so, stronger relationships between government and its citizens, as well as an improved education effort aimed at reinforcing cybersecurity are essential components required to strengthen the cybersecurity of critical infrastructure[54] ». Sans le soutien de la population dans cette lutte, il est difficile d'aspirer à une cybersécurité globale pour le Canada. L'importance de la communication avec la population pour les informer des risques reliés à la cybersécurité à travers des campagnes de sensibilisation reste une des méthodes les plus efficaces et une responsabilité importante du gouvernement fédéral.

Une approche plus active

À la lumière de l'évidence de l'évolution exponentielle des opérations dans le cyberespace, il devient encore plus important de prendre toutes les mesures nécessaires pour efficacement instaurer un système de protection pour assurer la sécurité nationale. Le Secrétaire adjoint de la Défense des États-Unis, William Lynn soutient aussi que « in this environment, a fortress mentality will not work. We cannot hide behind a Maginot line of firewalls. As I will describe shortly, our defenses must be active[55] ». Des cyberattaques de plus en plus sophistiquées et versatiles sont commises régulièrement à la fois sur les réseaux du gouvernement et du secteur privé dans le but de discréditer nos infrastructures essentielles ou perturber leur cohérence et efficacité. « New cyber security approaches must continually

---

[54]*Ibid.*

[55]U.S. Deputy Secretary of Defense Speech, William J. Lynn, III, « Remarks on Cyber at the Council on Foreign Relations – 30 septembre 2010 », consulté le 05 mai 2014, http://www.defense.gov/speeches/speech.aspx?speechid=1509.

be developed, tested and implemented to respond to new threat technologies and strategies[56] ».

Considérant que certaines cyberattaques seront inévitables dans le futur peu importe les mesures prises pour se protéger, il devient critique de s'assurer que notre système soit basée sur un principe de cyber-résilience, c'est-à-dire « a process linking a set of adaptive capabilities to a positive trajectory of functioning and adaptation after a disturbance[57] ». Développer une telle capacité est vital à la survie de la nation en cas de catastrophe. Le problème est bien entendu de trouver une balance ne pas se préparer adéquatement et en faire tout simplement trop. « The optimal level of cyber-intrusions is not zero, and the optimal level of cyber-security expenditures is not infinity. From an economic perspective, the goal is to achieve an efficient level of attacks, not to prevent all attacks. […] Cyber-security is a form of risk management, where risk is a function of three variables: vulnerabilities, threats, and consequences[58] ».

L'OTAN a déclaré lors du sommet de Lisbonne en 2010 que la cybersécurité est maintenant « au premier rang des nouveaux défis de sécurité que l'OTAN et sa nouvelle division défis de sécurité émergente devront relever dans les années à venir[59] ». Que ces attaques soient l'action d'un autre état ou d'un acteur non étatique, elles restent bel et bien réelles. Tout comme le reste des membres de l'alliance, le Canada se doit d'être prêt à faire

---

[56]Dan Dunkel, « The New Security Order », SDM Exclusive (juin 2010), consulté le 07 mai 2014, http://search.proquest.com/docview/501737492/fulltextPDF/657EEDBE9A14DBFPQ/1?accountid=9867, p. 48.

[57]Geoffrey T. Stewart, « Leveraging public-private partnerships », p. 349.

[58]Nathan Alexander Sales, « Regulating cyber-security », p 1511.

[59]Arnaud Coustillière, « La cyberdéfense : Un enjeu global et une priorité stratégique », p. 30.

face à ce type de menace d'ordre non conventionnel qui inclut l’agression cybernétique de gravité diverse.

CONCLUSION

En conclusion, l’examen de la stratégie canadienne pour la cybersécurité a été conduit dans cet essai et elle a été basée sur la comparaison de la cybermenace et des mesures en place pour protéger les infrastructures essentielles. En premier lieu, la nature de la cybermenace a été analysée en définissant le concept d’infrastructures essentielles et les cybermenaces qui s’y rattachent. En deuxième lieu, l’analyse de l’efficacité de la stratégie canadienne pour faire face à ces menaces a été faite en considérant le rôle de la nation sur la scène internationale ainsi que l’importance d’une approche globale au niveau national. Pour finir, une réflexion sur la pertinence d’adopter un plan d’action plus robuste misant sur la cyber-résilience a été présentée.

La définition de la cybersécurité était nécessaire afin d’évaluer la pertinence de la stratégie canadienne face aux nouvelles réalités imposées par le cyberespace. Les infrastructures essentielles sont au cœur de la sécurité nationale. La validation du concept de cyberattaque a permis de conclure que la cybersécurité du Canada ne peut être assurée que par la protection de ces structures vitales.

L’analyse des écoles de pensée sur la nature de la cybermenace a démontré que cette cinquième dimension n’est pas révolutionnaire en soi, mais qu’elle ne peut, pour autant, être totalement ignorée. Elle fait effectivement désormais partie intégrante des conflits modernes. De plus en plus populaire comme outil disponible pour faire la guerre parce qu’elle permet d’avoir un impact important et chirurgical sur l’adversaire tout en laissant peu de traces. Elle

présente des caractéristiques propres à elle-même. Des faits concrets, comme la hausse de la criminalité ou de cyberattaques comme celles utilisées lors de l'opération Orchard ou Stuxnet, ont été présentés pour prouver que les cyberattaques soient inévitablement vouées à augmenter dans le futur.

L'étude de la menace a permis de valider l'inefficacité de la stratégie canadienne. Au niveau international, les lois sont incomplètes et laisse en suspens de nombreuses questions non résolues que les états se doivent de régler. Au niveau des intérêts nationaux, le Canada se retrouve donc dans l'obligation d'être plus actif sur la scène internationale. Au niveau national, la stratégie canadienne présente des faiblesses nuisant à l'approche globale nécessaire à la mise en œuvre de la cybersécurité. Finalement, il a été défini que le plan d'action et la stratégie canadienne pour la cybersécurité se doivent d'être modifiés pour assurer une posture plus efficace assurant l'intégration des efforts de tous les acteurs clés.

Les arguments présentés dans ce travail ont permis de valider que les cybermenaces actuelles et futures envers les infrastructures essentielles canadiennes représentent un danger concret pour la sécurité nationale. Toutefois, les recours juridiques et lois actuelles sont incomplets pour permettre au gouvernement de répondre à son mandat de protéger la nation envers les cybermenaces modernes. En effet, la stratégie impliquant les paliers gouvernementaux, le secteur privé et la population canadienne est défaillante. Le gouvernement fédéral doit modifier sa stratégie et adopter un plan d'action plus robuste pour assurer la cybersécurité au Canada. Il doit favoriser une approche globale plus efficace au niveau national et une représentation accrue sur la scène internationale dans l'optique de défendre plus adéquatement les intérêts nationaux.

Somme toute, il demeure vrai que les problèmes complexes reliés à la cybersécurité exigent des solutions qui sont à la fois sophistiquées et cohérentes. Toutefois, pour définir ces solutions, il nous faut une image opérationnelle commune solidement fondée sur des données empiriques qui a malheureusement un prix. Il y aura sans aucun doute des choix à faire et seul le futur pourra nous certifier si nous avons sélectionné la stratégie gagnante…

BIBLIOGRAPHIE

Amir-Aslani, Ardavan. « Stuxnet vs Shamoon: La cyberguerre au Moyen-Orient » *extrait de Sécurité globale*, No 24 (2013/2), accédé le 26 avril 2014, http://www.cairn.info/revue-securite-globale-2013-2-page-9.htm, p. 9-14.

Baud, Michel. « La cyberguerre n'aura pas lieu, mais il faut s'y préparer » *extrait de Politique étrangère*, No 2, (été 2012), p. 305-316.

Betz, David J., et Tim Stevens. *Cyberspace and the State: Toward a strategy for Cyber-power*, London : The International Institute for Strategic Studies, 2011.

Brook, Douglas A. « Budgeting for national security: A whole of gouvernment perspective » *extrait de J. of Public Budgeting, Accounting & Financial Management*, Review 24, No 1 (printemps 2012), accédé le 27 avril 2014, http://search.proquest.com/docview/1019950248/fulltextPDF/E8F773E0ED144B5BPQ/1?accountid=9867, p. 32-57.

Canada. Bureau du Conseil Privé. *Politique canadienne de sécurité nationale*, Ottawa : Groupe Communication Canada, 2010, accédé le 04 mai 2014, http://publications.gc.ca/collections/Collection/CP22-77-2004F.pdf.

Canada. Bureau du vérificateur général du Canada. *Rapport du vérificateur général du Canada à la Chambre des communes - Chapitre 3: Protéger l'infrastructure canadienne essentielle contre les cybermenaces*, Ottawa : Groupe Communication Canada, 2012, accédé le 09 mai 2014, http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201210_03_f.pdf.

Canada. Ministère de la Sécurité publique. *Stratégie de cybersécurité du Canada: Renforcer le Canada et accroître sa prospérité*, Ottawa : Groupe Communication Canada, 2010, accédé le 22 avril 2014, http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fra.aspx.

Canada, Parlement du Canada. *Travaux parlementaires: Délibération du Comité sénatorial permanent de la Sécurité nationale et de la défense*, Ottawa : Groupe Communication Canada, 2010, accédé le 07 mai 2012, http://www.parl.gc.ca/content/sen/committee/411/SECD/06EVB-49519-f.HTM.

CBC. « Heartbleed bug may shut Revenue Canada website until weekend », accédé le 06 mai 2014, http://www.cbc.ca/news/business/heartbleed-bug-may-shut-revenue-canada-website-until-weekend-1.2603742.

Clarke, Richard A., et Robert K. Knake. *Cyber war: The next threat to national security and what to do about it*, New York : HarperCollins Publishers, 2010.

Coustillière, Arnaud. « La cyberdéfense: Un enjeu global et une priorité stratégique pour le ministère de la défense » *extrait de Sécurité globale*, No 1, (2013), p. 27-32.

Cyr, Éric. « 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), accédé le 15 avril 2014, http://www.cfc.forces.gc.ca/259/290/299/286/Cyr.pdf#pagemode=thumbs.

Dunkel, Dan. « The New Security Order » *extrait de SDM Exclusive* (juin 2010), accédé le 07 mai 2014, http://search.proquest.com/docview/501737492/fulltextPDF/657EEDBE9A14DBFPQ/1?accountid=9867, p. 44-50.

États-Unis, Department of Defense. *Strategy for Operating in Cyberspace*, Washington, D.C.: U.S. Government Printing Office, juillet 2011, accédé le 03 mai 2014, http://www.defense.gov/news/d20110714cyber.pdf.

Farwell, James P. « Industry's Vital Role in National Cyber Security » *extrait de Strategic Studies Quarterly* (hiver 2012), accédé le 30 avril 2014, http://search.proquest.com/docview/1240323762/fulltextPDF/C24F76931E2848A1PQ/2?accountid=9867, p. 10-41.

Farwell, James P., et Rafal Rohozinski. « Stuxnet and the Future of Cyber War », *extrait de Survival* 53:1, (2011), p. 23-40, https://www.cs.duke.edu/courses/common/compsci092/papers/cyberwar/stuxnet2.pdf.

Graham, Andrew. « Canada's Critical Infrastructure : When is safe enough safe enough? » *extrait de Institute MacDonald-Laurier*, (2011), accédé le 02 mai 2014, http://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf, p. 1-32.

Hathaway, Oona A., et coll. « The law of cyber attack » *extrait de California Law Review 100*, No. 4, (2012), accédé le 07 mai 2014, http://www.californialawreview.org/assets/pdfs/100-4/02-Hathaway.pdf, p. 817-885.

Hawco, Darren. « CAF Director General Cyber - Development of the CAF Cyber Capability », *Conférence GOFO*, Ottawa: Ont, 30 avril 2014, avec l'autorisation du conférencier.

Kempf, Olivier. « Cyber : la surprise n'est pas celle que l'on croit » *extrait de Revue Défense Nationale*, No 767 (février 2014), p. 9 - 15.

Limnell, Jarno. « Le cyber change-t-il l'art de la guerre? », *extrait de Sécurité globale*, No 23 (2013/1), p. 34, http://www.cairn.info/revue-securite-globale-2013-1-page-33.htm.

NATO, North Atlantic Treaty Organisation. « NATO 2020: Assured security; dynamic engagement », Brussels: Belgium, NATO Public Diplomacy Division, 17 may 2010, accédé le 03 mai 2014, http://www.nato.int/strategic-concept/expertsreport.pdf.

Pew Research Center. « Extremists, cyber-attacks top Americans' security threat list », accédé le 08 mai 2014, http://www.pewresearch.org/fact-tank/2014/01/02/americans-see-extremists-cyber-attacks-as-major-threats-to-the-u-s/.

Rid, Thomas. *Cyber war will not take place*, New York : Oxford University Press, 2013.

Sécurité Publique Canada, « Infrastructures essentielles », accédé le 05 mai 2014, http://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fra.aspx.

Sales, Nathan Alexander. « Regulating cyber-security » *extrait de Northwestern University Law Review*, Vol 107, No 4 (2013), p. 1503-1568.

Statistique Canada, Centre canadien de la statistique juridique. « Taux de cybercriminalité au Canada rapporté par les services de police (2008 - 2010) », demande d'accès à l'information numéro 619921, 06 mai 2014.

Stewart, Geoffrey T., Ramesh Kolluru et Mark Smith. « Leveraging public-private partnerships to improve community resilience in times of disaster » *extrait de International Journal of Physical* (2009), accédé le 02 mai 2014, http://search.proquest.com/docview/232592275/fulltextPDF/9F41AC8D343B42F2PQ/1?accountid=9867, p. 343-364.

The Economist. « Interview with Richard A. Clarke: Cyber war in 2013 », accédé le 06 mai 2014, https://www.youtube.com/watch?v=6_ek8mugOUc.

U.S. Deputy Secretary of Defense Speech, William J. Lynn, III. « Remarks on Cyber at the Council on Foreign Relations – 30 septembre 2010 » accédé le 05 mai 2014, http://www.defense.gov/speeches/speech.aspx?speechid=1509.

Vatis, Michael. « The next battlefield : The reality of virtual threats » *extrait de Harvard International Review*, Vol 28, No 3 (automne 2006), accédé le 28 avril 2014, http://search.proquest.com/docview/59968204/6448448F4E4F41F9PQ/2?accountid=9867.

Wikipedia. *Heartbleed*, 09 mai 2014, accédé le 21 avril 2014, http://fr.wikipedia.org/wiki/Heartbleed (accès le avril 23, 2014).

Youtube website. « CyCon 2012 – Michael Schmitt: Tallinn Manual Part 1 », accédé le 17 avril 2014, https://www.youtube.com/watch?v=wY3uEo-Itso.