National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

LA MENACE CYBER EST-ELLE VRAIMENT MENAÇANTE?

Maj J.Y.A. Côté

JCSP 42

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 42

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 42 – PCEMI 42
2015 – 2016

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

LA MENACE CYBER EST-ELLE VRAIMENT MENAÇANTE?

Maj J.Y.A. Côté

Word Count: 6318

Compte de mots: 6318

LA MENACE CYBER EST-ELLE VRAIMENT MENAÇANTE?

INTRODUCTION

Même si les états actuels n'ont pas connu de conflit mondial interétatique depuis maintenant près de 60 ans, le monde bouillonne de conflits. Par leur nouvelle nature, ces conflits apportent un niveau de complexité supplémentaire. Ce niveau de complexité additionnel peut être expliqué par Andy et Heidy Toffler, frère et sœur publiés de réputation mondiale qui conseillent les compagnies et gouvernements à propos des changements au niveau économique, technologique et social, en utilisant leur *théorie des trois vagues* telle qu'illustrée à la figure 1.

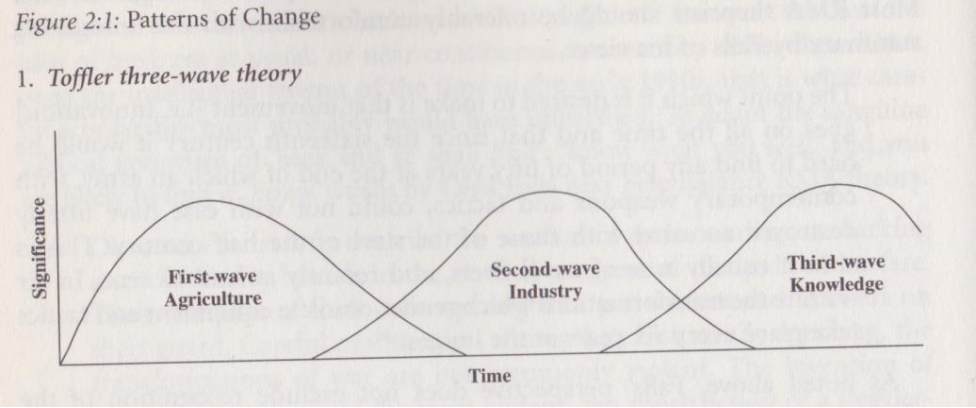

Figure 1 – La théorie des trois vagues des Toffler

Source : Gray, *Strategy for Chaos : Revolution in Military Affairs and the Evidence of History*, p. 54.

Cette théorie situe l'époque actuelle dans l'ère de l'information. Cette nouvelle ère s'est également caractérisée par l'avènement d'un nouveau domaine de guerre[1], le cyberespace. Ce nouveau domaine est tout aussi important que la terre, la mer, l'air ou l'espace[2]. Daniel Ventre, ingénieur français au centre national de la recherche scientifique considéré comme étant un des

[1] Paul J. Springer, *Cyber Warfare: A Reference Handbook* (Santa Barbara, CA : ABC-CLIO, 2015), p. 61.

[2] Thomas Rid, « Cyberwar Will Not Take Place », *Journal of Strategic Studies* 35, n^0 1 (février 2012), p. 6, http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939.

meilleurs spécialistes français en matière de cyberguerre, démontre bien, à la figure 2, l'interaction de ce nouveau domaine avec les domaines de guerre traditionnel.

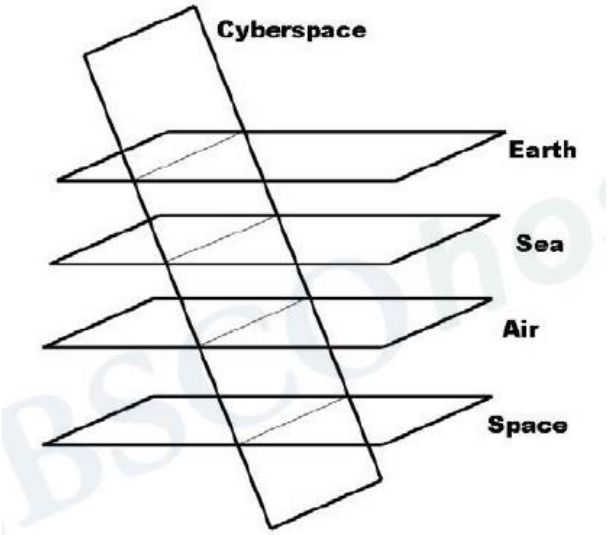

Figure 2 – Le cyberespace
Source : Ventre, *Cyberwar and Information Warfare*, p. 162.

Le cyberespace est unique et il interagit avec tous les autres domaines de guerre. Dans ces débuts, la menace du cyberespace pouvait mener à craindre un *Pearl Harbor digital*[3]. Mais maintenant que le cyberespace est mieux compris, quelles sont les vraies menaces qui émanent de ce nouveau domaine de guerre? Mais plus pertinemment, quelles sont les menaces actuelles du cyberespace envers les intérêts canadiens? Cet essai prouvera que la menace cyber est seulement une menace de niveau moyen face aux intérêts canadiens. La méthodologie utilisée sera simple. Après avoir défini les intérêts canadiens, la menace sera définie en analysant les acteurs potentiels pouvant devenir un des *quatre chevaliers de la cyberagression*[4] : le cyberterrorisme, le cybercrime, le cyberespionnage et la cyberguerre. Les acteurs pouvant perpétrer ces agressions sont : les terroristes, les criminelles, les pirates informatiques et les états.

---

[3] Gabriel Wiemann, « *Cyberterrorism : How Real Is the Threat?* », Special Report 119 (Washington, D. C. : United States Institute of Peace, 2004), p. 2, http://www.usip.org/sites/default/files/sr119.pdf.

[4] Wesley Wark, « Cyber-Aggression and Its Discontents », *Global Brief*, 4 octobre 2012, p. 1, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

Étant donné que la Chine est perçue par plusieurs comme étant la pire menace cyber envers les États-Unis[5], l'analyse d'un état se limitera à l'analyse de la Chine. Pour quantifier le risque de ces acteurs potentiels, la définition de Lior Tabansky, un expert en politique de sécurité cyber, sera utilisée. Tabansky défini la menace comme : « étant un produit de la probabilité qu'un événement se produise et l'analyse de dommages [potentiels qui ont] causés l'événement[6]. » [trad. libre] En plus de la probabilité et de la gravité, le nombre d'intérêts canadiens menacés influencera également le niveau de la menace. Donc, la première section définira les intérêts canadiens. La deuxième section analysera la menace des cyberterroristes, des cybercriminels et des pirates informatiques. La troisième section définira la stratégie chinoise et analysera la menace du cyberespionnage et de la cyberguerre chinoise. Finalement, la comparaison de toutes ces menaces permettra de prouver la thèse.

SECTION 1 – LES INTÉRÊTS CANADIENS

L'analyse de la menace cyber serait obsolète si elle n'était pas mise en relation avec des intérêts. Donc cette section définira, sans ordre particulier, les quatre intérêts canadiens dans le cyberespace qui peuvent être déduits des politiques de sécurité canadienne ainsi que de la littérature à cet effet. Le premier est la sécurité de l'économie canadienne et l'importance de la coopération avec le secteur privé. Le deuxième est la sécurité nationale incluant la sécurité des systèmes informatiques et la sécurité des infrastructures essentielles. Le troisième est la sécurité des Canadiens par le respect de leur vie privée et la responsabilité du gouvernement envers les Canadiens. Finalement, le quatrième est la crédibilité du Canada envers leurs alliés, tout particulièrement les États-Unis et *North American Aerospace Defense Command* (NORAD).

---

[5] Magnus Hjortdal, « China's use of cyber warfare: Espionage meets strategic deterrence », *Journal of Strategic Security* 4, n^0 2 (été 2011), p. 2.

[6] Lior Tabansky, « Basic Concepts in Cyber Warfare », *Military and Strategic Affairs* 3, n^0 1 (mai 2011), p. 86

La sécurité de l'économie

Il semble trivial d'accepter le fait que la sécurité de l'économie canadienne est essentielle à la prospérité et le bien-être des Canadiens. Cependant, lorsqu'on constate que le « Canada est un marché économique et que la prospérité économique canadienne repose fondamentalement sur un réseau ouvert et sécuritaire de communication global[7] », il est évident que la sécurité de l'économie au sein du cyberespace est d'intérêt canadien. En outre, Angela Gendron, une membre senior réputée au sein du *Centre canadien de recherche sur le renseignement et la sécurité* de l'Université de Carleton à Ottawa, et Martin Rudner, un docteur réputé fondateur de ce même centre, affirment qu'en 2011, 20% du produit intérieur brut du Canada était les institutions de finances et les banques. Ce plus gros segment de l'économie canadienne dépend des réseaux informatiques et de télécommunications[8]. Si les réseaux informatiques et les télécommunications canadiennes ne peuvent être sécurisés, l'économie en souffrira directement et compromettra la prospérité, la richesse et le bien-être des Canadiens[9]. Avec cette récente statistique, il ne fait plus de doute que la sécurité de l'économie canadienne est un intérêt canadien dans le cyberespace.

Cependant, la sécurité de l'économie canadienne ne peut être sécurisée correctement si le gouvernement ne porte pas une attention particulière aux secteurs privés et institutions non gouvernementaux. Ces derniers peuvent être des cibles faciles dans le cyberespace. La *Stratégie de Cybersécurité* en fait clairement mention : « [l]e milieu universitaire, les organismes non gouvernementaux et le secteur privé du Canada doivent unir leurs efforts à ceux du

---

[7] Ron Deibert, *Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace* (Calgary : Canadian Defense & Foreign Affairs Institute, 2012), p. 1.

[8] Angela Gendron et Martin Rudner, *Assessing Cyber Threats to Canadian Infrastructure* (Ottawa : Canadian Security Intelligence Service, 2012), p. 16.

[9] Vytautas Butrimas, « National Security and International Policy Challenges in a Post Stuxnet World », *Lithuanian Annual Strategic Review* 12, n^0 1 (2014), p. 30.

gouvernement pour assurer la sécurité des cybersytèmes au pays[10]. » Cette sécurité à une liaison directe avec la prospérité du pays. Il suffit de constater l'opinion de Daniel T. Kuehl, un docteur publié de la *National Defense University*, à Fort McNair en Virginie, qui mentionne que « le secteur public est inséparable du gouvernement et du militaire dans le cyberespace[11] » afin de confirmer l'importance de cette coopération. Si cette coopération n'a pas lieu ou n'est pas efficace, elle peut contribuer à la fermeture de compagnie canadienne, comme dans le cas de *Nortel*[12], qui affecte négativement l'économie canadienne. Bref, la sécurité de l'économie canadienne, incluant la coopération efficace avec le secteur public, est sans aucun doute un intérêt canadien important dans le cyberespace.

La sécurité nationale

Dans le cyberespace, la sécurité nationale peut être souvent menacée. Pour assurer sa sécurité nationale, le Canada doit assurer la sécurité des réseaux informatiques et assurer la sécurité des infrastructures essentielles. Il est certain que la sécurité informatique passe essentiellement par la « cybersécurité des systèmes du gouvernement fédéral[13] » comme il est clairement énoncé dans la *Politique canadienne de sécurité nationale*. Heureusement que la *Stratégie de cybersécurité du Canada* ne peut être plus claire : « la Stratégie permettra de protéger l'intégrité des systèmes gouvernementaux et des actifs essentiels à notre pays.[14] » Donc il est clair que la sécurité des cybersystèmes canadiens est bien comprise afin d'assurer la sécurité nationale.

---

[10] Sécurité publique Canada, *Stratégie de la cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité* (Ottawa : Sécurité Publique Canada, 2010), p. 8.

[11] Daniel T. Kuehl, « From Cyberspace to Cyberpower: Defining the Problem », *Cyberpower and national security* (Washington D. C. : National Defense University Press, 2009), p. 14.

[12] Deibert, *Distributed Security as Cyber Strategy*, p. 2.

[13] Bureau du Conseil Privé, *Protéger une société ouverte : la politique canadienne de sécurité nationale* (Ottawa : Bureau du Conseil Privé, 2004), p. 23.

[14] Sécurité publique Canada, *Stratégie de la cybersécurité du Canada*, p. 16.

D'un autre côté, la sécurité nationale ne peut être maintenue sans assurer la sécurité des infrastructures critiques. Dans son analyse de la politique de cybersécurité canadienne, Ventre mentionne qu'une préoccupation majeure du gouvernement fédéral canadien pour la sécurité nationale est la sécurité des infrastructures critiques[15]. C'est sans surprise qu'il est possible de retrouver explicitement une *Stratégie nationale sur les infrastructures essentielles*[16] ainsi que son plan d'action détaillé[17] afin d'assurer cette sécurité. Jacques J. M. Shore, un avocat d'une firme réputée à Ottawa et qui possède une vaste expérience dans le secteur public, tout particulièrement dans le domaine de la sécurité nationale, mentionne même que le système de justice canadien pourrait justifier le devoir de protéger les infrastructures essentielles[18]. Donc, il est évident de constater qu'en protégeant les systèmes gouvernementaux et les infrastructures essentielles, la sécurité nationale est un intérêt pour le Canada dans le cyberespace.

La sécurité des Canadiens

Dans le monde actuel, la population des pays développés dépend du cyberespace[19], même si la sécurité de leurs données privées ainsi que leur identité ne sont pas des acquis. Certes, « les familles canadiennes veulent que leur vie privée, identité et bien-être soient à l'abri des prédateurs en ligne[20]. » Le gouvernement reconnaît bien ce besoin en établissant un de ces trois piliers de la *Stratégie de la cybersécurité du Canada* comme étant « Aider les Canadiens à se protéger en ligne[21] ». En outre, dans son *Plan d'action 2010-2015 de la Stratégie de*

---

[15] Daniel Ventre, *Cyber Conflict: Competing National Perspectives* (Croydon : ISTE Ltd, 2012), p. 2.

[16] Sécurité publique Canada, *Stratégie nationale sur les infrastructures essentielles* (Ottawa : Sécurité publique Canada, 2009).

[17] Sécurité publique Canada, *Plan d'action sur les infrastructures essentielles : 2014-2017* (Ottawa : Sécurité publique Canada, 2014).

[18] Jacques J. M. Shore, « An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security », *International Journal of Intelligence and CouterInterlligence* 28, n^0 2 (2015), p. 241.

[19] Deibert, *Distributed Security as Cyber Strategy*, p. 4.

[20] Sécurité publique Canada, *Stratégie de la cybersécurité du Canada*, p. 14.

[21] *Ibid*., p. 7.

cybersécurité du Canada, le gouvernement énonce qu'il « considère prioritaire la protection des renseignements privés des Canadiens en ligne[22]. » Même que la *Gendarmerie royale du Canada* se fait donner un objectif clair afin de développer une stratégie contre la fraude et le vol d'identité dans le cyberespace[23]. Le gouvernement possède une certaine responsabilité envers ses citoyens afin de les protéger. Shore la décrit comme étant le développement d'un cadre législatif pour protéger les données et les informations sensibles du vol digital[24]. Bref, il est clair que la sécurité des Canadiens dans le cyberespace est un intérêt canadien très important.

La crédibilité du Canada envers ses alliés

L'aspect international et la relation avec les alliés au sein du cyberespace semblent seulement être effleurés[25] dans la *Stratégie de la cybersécurité du Canada.* Victor Platt, un récent diplômé de l'Université de Toronto qui est maintenant un consultant senior dans le domaine du risque cyber, conclue ainsi : « la stratégie ne couvre pas la diplomatie internationale et les impératifs politiques requis pour la cybersécurité[26]. » [trad. libre] Sauf que la *Politique canadienne de sécurité nationale* est très directe. Son deuxième intérêt fondamental en matière de sécurité est de s'assurer que « le Canada n'est pas une source pour des menaces visant leurs alliés[27]. » Ceci s'applique également au cyberespace. Même si la stratégie manque à cet égard, la réalité est sans équivoque, « les membres de l'*Organisation du traité d'Atlantique Nord*, notamment les États-Unis et la Grande-Bretagne, sont en train de bâtir leurs capacités de

---

[22] Sécurité publique Canada, *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada* (Ottawa : Sécurité publique Canada, 2013), p. 5.

[23] *Ibid*., p. 12.

[24] Shore, « An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security », *International Journal of Intelligence and CouterInterlligence*, p. 3.

[25] Sécurité publique Canada, *Stratégie de la cybersécurité du Canada*, p. 3.

[26] Victor Platt, « Still the fire-proof house? An analysis of Canada's cyber security strategy », *International Journal* 67, n^{0} 1 (hivers 2011-12), p. 167.

[27] Bureau du Conseil Privé, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, p. vii.

cyberguerre[28]. » [trad. libre]. Même la conscience du cyberespace au niveau de l'*Organisation des Nations Unies* est en train de se bâtir[29]. Donc il est évident de constater qu'il est dans l'intérêt canadien de bâtir une cybercapacité fiable afin de maintenir sa crédibilité au niveau de ces alliés.

Dans un même ordre d'idée, au-delà de ces alliances plus larges, le Canada se doit de démontrer un très grand intérêt envers sa crédibilité avec les États-Unis, incluant son engagement avec NORAD. La proximité avec les États-Unis est critique pour le Canada. Les États-Unis ont créé en 2010 *United State Cyber Command*[30], un commandement opérationnel dédié à cyber. Matthew G. Devost et Neal A. Pollard, du Terrorism Research Center, recommandent même de développer un centre d'opérations cyber au sein du NORAD[31]. Les États-Unis sont un joueur clé dans le cyberespace et ils y investissent beaucoup de ressources. Le Canada se doit de démontrer un intérêt considérable envers le cyber afin de maintenir sa crédibilité avec les États-Unis. Deibert le mentionne : « la politique étrangère du Canada dans le cyberespace devrait inclure une composante de sensibilisation avec les plus importants pays pour la future gouvernance du cyberespace[32]. » [trad. libre] Il ne fait aucun doute que l'alliance la plus importante pour le Canada est avec les États-Unis, tant au niveau militaire qu'au niveau économique. Même une partie de l'infrastructure essentielle du Canada, telle que l'électricité[33], est liée aux États-Unis.

---

[28] Steve Ranger, « NATO updates cyber defense policy as digital attacks become a standard part of conflict », *ZDNet*, 30 juin 2014, p. 4, http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

[29] Platt, « Still the fire-proof house? An analysis of Canada's cyber security strategy », *International Journal*, p. 162

[30] Bachmann, Sascha-Dominik Oliver Vladimir, « Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management », extrait de *Amicus Curiae* 88 (2012), p. 26.

[31] Matthew G. Devost et Neal A. Pollard, *Taking Cyberterrorism Seriously: Failing to Adapt to Emerging Threats Could Have Dire Consequences* (Burke, VA : Terrorism Research Center, Inc., 2002), p. 2.

[32] Deibert, *Distributed Security as Cyber Strategy*, p. 23.

[33] Gendron et Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 14.

Donc, c'est sans équivoque que la crédibilité du Canada auprès de ses alliés, tout particulièrement les États-Unis, est un intérêt canadien dans le cyberespace.

Dans cette section, les intérêts canadiens par rapport au cyberespace ont été définis. Les quatre intérêts sont : la sécurité de l'économie qui inclue la coopération avec le secteur privé, la sécurité nationale qui inclue la sécurité des réseaux informatiques et la sécurité des infrastructures essentielles, la sécurité des Canadiens et finalement la crédibilité du Canada envers ces alliés, tout particulièrement les États-Unis. Maintenant, il est possible de commencer l'analyse de la menace cyber envers les intérêts canadiens.

SECTION 2 – LA MENACE DES TERRORISTES, DES CRIMINELS ET DES PIRATES INFORMATIQUES

Cette section définira séquentiellement le niveau de la menace des terroristes, des criminelles et des pirates informatiques. Il sera démontré que le niveau de la menace terroriste est de faible à moyenne, la menace criminelle est faible et la menace des pirates informatiques est moyenne. Chaque type de menace sera premièrement défini face aux intérêts canadiens pour ensuite être quantifié en évaluant la probabilité et la gravité.

Les cyberterroristes

Lorsqu'on pense au cyberterrorisme, on pense immédiatement à une cyberattaque qui paralyse le pays. Cependant l'utilisation quotidienne et fréquente du cyberespace par les organisations terroristes est tout autre. Les terroristes utilisent majoritairement le cyberespace pour communiquer entre eux, obtenir leur financement, faire de la propagande, effectuer leur recrutement et exécuter du cyberespionnage. C'est ainsi que Derek Reveron, docteur publié affilié de la faculté à *Harvard Kennedy School* et professeur au *Naval War College*, décrit l'utilisation commune du cyberespace par les terroristes[34]. Cependant, la communication et le

financement n'attaquent aucunement les intérêts canadiens. Même si la propagande, le recrutement et le cyberespionnage menacent la sécurité des Canadiens, ces actions sont qualifiées de simples « graffitis[35] » par James A. Lewis, un vice-président senior au *Center for Strategic & International Studies*. Cette qualification démontre que même s'ils touchent à un des intérêts canadiens, la gravité de ces actions est faible. Même si le Major Charvat, un officier britannique avec une vaste expérience cyber au sein de l'OTAN, affirme qu'il serait possible par la propagande de créer un mouvement de panique réel en falsifiant un site officiel du gouvernement[36], il rajoute également que ceci est possible, mais peu probable, étant donné que d'autres sites ou formes de médias contrediraient le site falsifié[37]. Donc, il est très peu probable que la propagande ait une gravité élevée. D'un autre côté, la probabilité de la propagande, le recrutement et le cyberespionnage est élevée, car elle se produit quotidiennement. Les terroristes actuels sont déjà en train de le faire. Cependant, même si cela se produit actuellement, la gravité mineure de ce type de menace terroriste permet de quantifier la menace comme étant mineure face aux intérêts canadiens.

En ce qui concerne la cyberattaque terroriste, si jamais elle se concrétise, elle pourrait menacer tous les intérêts canadiens, car les cibles sont « l'énergie, la finance, le militaire, le transport ainsi que d'autres services humains essentiels[38]. » [trad. libre] Une attaque sur l'infrastructure électrique aurait un impact direct sur l'économie, la sécurité nationale et la sécurité de chaque Canadien affecté par la panne électrique. En plus, la crédibilité envers les

---

[34] Dereck S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D. C. : Goergetown University Press, 2012), p. 62.

[35] James Andrew Lewis, *Assessing the risks of cyber terrorism, cyber war and other cyber threats* (Washington, D. C. : Center for Strategic & International Studies, 2002), p. 8.

[36] Christian Czosseck et Kenneth Geers, *The Virtual Battlefield: Perspectives on Cyber Warfare*, Volume 3 (Amsterdam : IOS Press, 2009), p. 83.

[37] *Ibid*.

[38] Sean Collins et Stephen McCombie, « Stuxnet: the emergence of a new cyber weapon and its implications », *Journal of Policing, Intelligence and Counter Terrorism* 7, n^0 1 (2012), p 89.

États-Unis serait affectée, car eux aussi ressentiraient les effets de cette panne. Même si cela semble définir la gravité comme étant élevé, Fred Schreider, un consultant *Geneva Center for Democratic Control of Armed Forces*, qualifie les cyberattaques comme étant dérangeantes et non destructives[39]. Et ceci prend tout son sens lorsque les plans de redondances qui sont normalement en places avec les infrastructures essentielles[40] sont considérés, les dommages d'une telle attaque seront limités et ne persisteront pas longtemps. Donc, ceci étant pris pour compte, la gravité peut être définie à moyenne.

Pour ce qui est de la probabilité d'une telle cyberattaque terroriste, il est à noter qu'aucune attaque de ce genre ne s'est jamais produite[41]. Vytautas Butrimas, conseiller en chef pour la cybersécurité du Ministère de la Défense nationale lithuanienne, explique cette absence d'attaque par le fait que « jusqu'à maintenant [les terroristes] manquent de compétences, d'intérêts et de capacités à déployer une arme cyber complexe[42]. » [trad. libre] Donc, il leur est actuellement impossible de faire une telle attaque. Même s'il y a un certain consensus sur ces faits, la majorité de la littérature laisse sous-entendre que si elle est vraiment une menace, la cyberattaque terroriste peut être une menace future[43]. Cependant des spéculations futures ne permettent pas d'évaluer la menace actuelle qui est acceptée comme étant faible. Il reste toujours ceux, comme Gendron et Rudner, qui sont convaincus de la possibilité d'une telle cyberattaque terroriste de grande envergure, en la qualifiant « d'arme asymétrique parfaite, peu coûteuse et

---

[39] Fred Schreier, *On Cyberwarfare*, DCAF Horizon 2015 Working Paper n^0 7 (Genève : DCAF, 2012), p. 28.

[40] Wiemann, « *Cyberterrorism : How Real Is the Threat?* », p. 10, http://www.usip.org/sites/default/files/sr119.pdf.

[41] Adam P. Liff, « Cyberwar: A new 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War », *The Journal of Strategic Studies* 35, n^0 3 (juin 2012), p. 423.

[42] Butrimas, « National Security and International Policy Challenges in a Post Stuxnet World », *Lithuanian Annual Strategic Review*, p. 13.

[43] Wark, « Cyber-Aggression and Its Discontents », *Global Brief*, p. 2, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

non attribuable[44]. » Cependant, il faut prendre en considération que leur rapport était pour le *Service canadien du renseignement de sécurité,* et que les organisations gouvernementales vont parfois gonfler la menace afin de pouvoir justifier leur budget[45]. Bref, même si une cyberattaque terroriste pourrait devenir réelle dans le futur, ceci est présentement très peu probable. Donc, avec une gravité moyenne et une probabilité faible qui menace tous les intérêts canadiens, la menace d'une cyberattaque terroriste est moyenne.

Basé sur l'analyse précédente de la menace cyberterroriste, il est possible de constater que la propagande, le recrutement et l'espionnage impactent principalement la sécurité des Canadiens. Donc, la menace est faible pour ce type d'attaque. Pour ce qui est de la cyberattaque terroriste, même si elle menace tous les intérêts canadiens, la menace a été quantifiée de moyenne. Bref, la menace englobant tout le cyberterroriste envers les intérêts canadiens est classifiée de faible à moyenne.

Les cybercriminels

Le monde criminel est par nature, motivé par l'argent. Dans le cyberespace, ceci n'est pas différent, leurs activités auront toutes un but lucratif. La *Stratégie de la cybersécurité du Canada* définit leur activité au sein du cyberespace comme étant les mêmes « activités traditionnelles, comme le vol d'identité, le blanchiment d'argent et l'extorsion[46]. » Ils volent des données personnelles, telles des cartes de crédit valides, afin de pouvoir les revendre. Les industries paient des rançons aux cybercriminelles[47] pour des secrets industriels, des formules pharmaceutiques volées[48], etc. Il est clair que deux intérêts canadiens majoritairement menacés :

---

[44] Gendron et Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 26.
[45] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. i.
[46] Sécurité publique Canada, *Stratégie de la cybersécurité du Canada*, p. 6.
[47] Nir Kshetri, « Pattern of global cyber war and crime: A conceptual framework », *Journal of International Management* 11, n^{0} 4 (2005), p. 557.
[48] Reveron, *Cyberspace and National Security*, p. 64.

la sécurité de l'économie et la sécurité des Canadiens. Il serait possible d'extrapoler et d'affirmer que les cybercriminels pourraient s'attaquer à la sécurité nationale ainsi qu'à la crédibilité du Canada envers ces alliés. Cependant, ceci serait peut-être du suicide, car une emphase nationale ou des conventions internationales pourraient limiter le cybercrime[49]. C'est pourquoi le cybercrime menace seulement la sécurité de l'économie et la sécurité des Canadiens.

Le cybercrime est omniprésent. Il se produit tous les jours. L'*International Cyber Security Protection Alliance (ICPSA)*, une firme internationale réputée en cybercriminalité, a produit un rapport sur le cybercrime canadien et rapporte que : « [d]e manière générale, le cybercrime est assez répandu dans les entreprises canadiennes, 69% d'entre elles ayant signalé une attaque quelconque au cours d'une période de douze mois[50]. » Et ceci ne prend même pas en compte les vols d'identité et d'informations privées. Donc, il est évident de conclure que la probabilité du cybercrime est élevée. Cependant, la gravité n'est pas ce que l'on pourrait penser. Même si Keith Alexander, le directeur de la *National Security Agency*, a qualifié le cyberespionnage industriel comme étant « le plus grand transfert de richesses dans l'histoire[51] » [trad. libre], il faut mettre le tout en contexte. Les pertes en chiffre peuvent sembler faramineuses, mais dans l'économie mondiale, Butrimas qualifie cette perte « d'erreur d'arrondissement dans une économie de 14 billions[52]. » [trad. libre] Même l'ICPSA rapporte que le cybercrime n'est pas trop grave et que les dommages ne sont pas importants[53]. Bref, la gravité peut être quantifiée à faible. Donc, même si elle possède une probabilité élevée, sa faible gravité

---

[49] Joseph S. Nye Jr., « *Cyber power* » (Cambridge, MA : Belfer Center for Science and International Affairs, 2010), p.17.

[50] International Cyber Security Protection Alliance, *Rapport d'enquête sur le cybercrime au Canada* (Chesham : ICSPA, 2013), p. 7.

[51] Keith Alexandre, s.l.n.d. cité dans Wark, « Cyber-Aggression and Its Discontents », *Global Brief*, p. 1, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

[52] Butrimas, « National Security and International Policy Challenges in a Post Stuxnet World », *Lithuanian Annual Strategic Review*, p. 30.

[53] ICSPA, *Rapport d'enquête sur le cybercrime au Canada*, p. 7, 9.

qui ne menace que deux intérêts canadiens, soit la sécurité de l'économie et des Canadiens, il est possible de conclure que la menace de la cybercriminalité envers les intérêts canadiens est faible.

Les pirates informatiques

Dans le cyberespace il existe également les pirates informatiques. Parfois ils travaillent en solo, parfois ils travaillent en groupe, mais tous représentent une menace dans le cyberespace. Leurs activités sont variées. Ils peuvent : effectuer du vol d'identité[54], exécuter du cyberespionnage tant au niveau industriel qu'au niveau gouvernemental[55], produire des logiciels malveillants, conduire des cyberattaques afin de défendre leurs idéologies ou protester contre une cause, comme il est survenu pour Google[56] quelques fois dans le passé. Avec toutes ces activités, tous les intérêts canadiens se retrouvent menacés. La sécurité de l'économie est menacée par le cyberespionnage industriel[57]. La sécurité nationale est menacée par le cyberespionnage et les cyberattaques qui perturbent les réseaux[58] des infrastructures essentielles. La sécurité des Canadiens est menacée par le vol d'identité et d'informations personnelles qui peut être fait par l'exploitation des réseaux sociaux, tel que démontré par l'expérience *Robin Sage*[59]. Finalement la crédibilité du Canada avec ces alliés pourrait être menacée si des pirates informatiques exécutent une cyberattaque sur une infrastructure essentielle qui touche également aux États-Unis afin de protester contre les deux pays. Bref, aucun des intérêts canadiens n'est à l'abri des pirates informatiques.

---

[54] Gendron et Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 33.

[55] Kenneth Geers, « The cyber threat to national critical infrastructures: Beyond theory », *Information Security Journal: A Global Perspective* 18, n^0 1 (2009), p. 2.

[56] Paul J. Springer, *Cyber Warfare: A Reference Handbook* (Santa Barbara, CA : ABC-CLIO, 2015), p. 158-159.

[57] John J. Tkacik, *Trojan Dragon: China's Cyber Threat*, Executive Summary Backgrounder n^0 2106 (Washington, D. C. : The Heritage Foundation, 2008), p. i, http://s3.amazonaws.com/thf_media/2008/pdf/bg2106es.pdf.

[58] Martin Libicki, *Cyberdeterrence and Cyberwar* (Washington, D. C. : RAND, 2009), p. 41-42, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

[59] Paulo Shakarian, Jana Shakarian et Andrew Ruef, *Introduction to cyber-warfare: A multidisciplinary approach* (Waltham, MA : Elsevier, Inc., 2013), p. 173.

D'un côté, l'analyse de la menace révèle que la probabilité des pirates informatiques envers les intérêts canadiens est élevée. Les pirates informatiques utilisent le cyberespace en continu. Kenneth Geers, docteur publié et ambassadeur du centre cyber de l'OTAN en Estonie, explique très clairement que les cyberattaques sont communes[60]. Selon la firme de cybersécurité McAfee, les pirates informatiques pourraient produire jusqu'à 60 000 logiciels malveillants chaque jour. D'un autre côté la probabilité semble faible. Il est important de considérer la réalité : « il n'existe aucun rapport énonçant que les communications internes au Pentagone ont déjà été piratées[61]. » [trad. libre] En y considérant la gravité, lorsque la probabilité est faible, des groupes tels qu'*Anonymous* ont démontré qu'ils sont capables de causer des dommages considérables lorsqu'ils unissent leurs efforts[62]. Cependant, lorsque la probabilité est élevée, Reveron mentionne que les pirates informatiques ne sont qu'une nuisance et qu'ils sont une faible menace dans le cyberespace[63]. Bref, la corrélation pour évaluer la menace est comme suit. Lorsque la probabilité est faible, la gravité des activités malfaisantes des pirates informatiques est élevée. Lorsque la probabilité est élevée, la gravité des activités malfaisantes des pirates informatiques est faible. Donc, tout en restant conservateur, il est possible de conclure que la menace des pirates informatiques envers tous les intérêts canadiens est moyenne.

La section deux a démontré que les cyberterroristes sont une menace évaluée de faible à moyenne. Les cybercriminels sont une menace faible. Finalement, les pirates informatiques sont une menace moyenne pour les intérêts canadiens dans le cyberespace. Maintenant, la Chine sera utilisée afin de compléter une analyse de la menace d'un état envers les intérêts canadiens.

---

[60] Geers, « The cyber threat to national critical infrastructures », *Information Security Journal: A Global Perspective*, p. 5.
[61] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. 10.
[62] Gendron et Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 33-34.
[63] Reveron, *Cyberspace and National Security*, p. 58.

SECTION 3 – LA MENACE D'UN ÉTAT : LA CHINE

La Chine est reconnue pour être très active dans le cyberespace. Depuis plus d'une décennie, les activités hostiles chinoises dans le cyberespace ont augmenté[64]. C'est pour cette raison que cette section évaluera la menace chinoise envers les intérêts canadiens dans le cyberespace ce qui équivaut à évaluer la menace d'un état envers ces mêmes intérêts. Il sera démontré que le cyberespionnage et la cyberguerre chinois représentent chacun une menace moyenne dans le cyberespace envers les intérêts canadiens. Pour ce faire, la stratégie chinoise dans le cyberespace sera premièrement définie, ensuite la menace sera séparément évaluée pour le cyberespionnage et la cyberguerre chinoise. Encore une fois, chaque type de menace sera premièrement défini face aux intérêts canadiens pour ensuite être quantifié en évaluant la probabilité et la gravité.

La stratégie chinoise

Avant de pouvoir évaluer la menace chinoise, il est important de comprendre les grandes lignes de leur stratégie cyber qui gravite autour de la domination du flot de l'information. Dans un rapport pour la *US-China Economic and Security Review Commission*, la définition du but de la guerre de l'information chinoise est de « contrôler le flot de l'information ennemi et de maintenir la dominance dans le champ de bataille[65]. » [trad. libre] En fait, le rapport mentionne également que : « l'établissement de la domination de l'information sur un ennemi est une des plus hautes priorités opérationnelles[66]. » [trad. libre] Dans un même ordre d'idée, Ventre mentionne que l'objectif chinois est clair : « être capable de gagner des guerres conduites par

---

[64] *Ibid.*, p. 200.

[65] The US-China Economic and Security Review Commission, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation* (McLean, VA : Northrop Grumann Corporation Information Systems Sector, 2009), p. 6.

[66] *Ibid.*, p. 7.

l'information (guerre de l'information) d'ici la moitié du XXI[e] siècle[67]. » Et pour lui, la guerre de l'information est « la guerre où l'informatique est utilisée pour obtenir ou détruire des renseignements[68]. » Afin d'atteindre cet objectif, la stratégie militaire chinoise, appelée l'*Information Network Electronic Warfare (INEW)*[69], groupe et intègre ensemble tous les éléments militaires cyber. Cette intégration permet d'exécuter du cyberespionnage et une cyberguerre efficace afin de contrôler le flot de l'information. Cependant, même si la Chine a parfois de la difficulté à « contrôler le flot de l'information en essayant d'accommoder les pressions publiques pour un certain niveau de transparence et de responsabilité[70] », il devient tout de même apparent que le cyberespionnage et la cyberguerre occupent une place de choix dans la stratégie cyber chinoise afin de dominer ce flot de l'information.

Également, la Chine, qui a longtemps eu une stratégie basée sur une *défense active*, a réalisé que pour obtenir la supériorité de l'information, elle devra appliquer une *offensive active*. Ventre explique ce changement comme un « concept de légitime défense et d'attaques préemptives[71]. » Paulo Shakarian, docteur publié et assistant-professeur à l'Arizona State University, aidé de sa sœur Jana et de Andrew Ruef, décrit explicitement le passage de la stratégie Chinoise à *l'offensive active*[72]. Cette stratégie permet de prendre et garder l'initiative dans le cyberespace. En outre, même si cette stratégie plus agressive risque que la nation soit accusée d'espionnage, elle peut devenir un bénéfice au niveau de la dissuasion des autres états en

[67] Daniel Ventre, *Cyberguerre et la guerre de l'information : stratégies, règles, enjeux* (Paris : Lavoisier, 2010), p. 288.
[68] Daniel Ventre, *La guerre de l'information* (Paris : Lavoisier, 2007), p. 82-83.
[69] The US-China Economic and Security Review Commission, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, p. 14.
[70] Reveron, *Cyberspace and National Security*, p. 191.
[71] Ventre, *La guerre de l'information*, p. 83.
[72] Shakarian, Shakarian et Ruef, *Introduction to cyber-warfare*, p. 117.

démontrant les capacités cyber chinoises[73]. Donc, ceci explique pourquoi la Chine paraît si active dans le cyberespace au niveau du cyberespionnage.

Dans un même ordre d'idée, la Chine prend une approche intégrée à tous les niveaux dans le cyberespace. C'est ce que Ventre appelle la *guerre du peuple*[74], tout le monde y participe. Plus précisément, Wark décrit « l'émergence de ce complexe militaire-cyber chinois incluant un sombre partenariat entre les militaires chinois, le secteur académique chinois et les groupes privés organisés[75]. » [trad. libre] Ces groupes privés organisés ont été les pirates informatiques, cependant la Chine découvre rapidement que ces derniers ne sont pas compatibles avec l'*INEW*. Le commandement et contrôle, le ciblage de précision et l'effet de surprise sont difficiles à maintenir avec des pirates informatiques au sein de l'*INEW*[76]. C'est pour cette raison que « l'expansion de la loi antipiratage informatique chinoise, jumelée avec une série d'arrestations de haut profile et des sentences sévères pour le crime du piratage informatique[77] » [trad. libre] ont permis de ralentir l'utilisation des pirates informatiques à la *guerre du peuple* chinoise. Malgré tout, « plusieurs pirates informatiques réémergent en tant que membres légitimes des firmes de consultant en sécurité ou des académies[78] » [trad. libre], ce qui permet à la Chine de bénéficier de leur expertise. La Chine est plus encline à utiliser l'expertise de ces firmes commerciales[79]. Bref, avec sa *guerre du peuple* et son approche intégrée, la Chine démontre la capacité d'accéder à un bassin d'expertise qui permet d'accomplir des activités hautement complexes dans le cyberespace.

---

[73] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. 4.

[74] Ventre, *La guerre de l'information*, p. 77.

[75] Wark, « Cyber-Aggression and Its Discontents », *Global Brief*, p. 3, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

[76] Shakarian, Shakarian et Ruef, *Introduction to cyber-warfare*, p. 122.

[77] The US-China Economic and Security Review Commission, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, p. 39.

[78] Shakarian, Shakarian et Ruef, *Introduction to cyber-warfare*, p. 152.

[79] Dennis F. Poindexter, *The Chinese Information War: Espionage, Cyberwar, Communication Control and Related Threats to United States Interests* (Jefferson, NC : McFarland & Company, Inc., 2013), p. 65.

Bref, la Chine de par sa stratégie et son approche intégrée peut faire du cyberespionnage, et potentiellement une cyberguerre, de grande complexité. Cependant, certains détails méritent d'être énoncés afin de bien comprendre la manière dont la Chine mettra en application cette stratégie. Tel que rapporté par Ventre, le livre blanc de 2004 est très explicite :

> La Chine y réaffirme le caractère strictement pacifique de ses efforts de développement. Elle souhaite construire une société prospère, dans la paix. La Chine n'aura jamais d'ambitions expansionnistes et ne recherchera jamais un pouvoir hégémonique (par référence aux États-Unis évidemment). Sa politique de défense nationale est strictement défensive et protège la souveraineté nationale. Il ne peut y avoir de modernisation et de croissance économique sans un pays assuré de sa sécurité. Les développements de la défense nationale et de l'économie sont ainsi liés et doivent être coordonnés[80].

Même si le livre blanc date de quelques années, il reste tout de même valide. La Chine n'est pas expansionniste, donc il ne sera pas logique selon leur stratégie de lancer une attaque, dans le cyberespace ou non, contre le Canada sans raison valide. De plus, l'économie est cruciale pour la Chine. Donc attaquer l'économie d'un autre pays aura également des impacts sur l'économie de la Chine étant donné qu'elle possède des liens commerciaux pratiquement avec tous les pays. Cependant, il faut nuancer sa politique strictement défensive énoncée dans le livre blanc par l'*offensive active* selon laquelle la Chine a agi au cours de ces dernières années. Cela permet de conclure que l'accent sur le cyberespionnage, à la place de la cyberguerre, permet à la Chine de respecter son livre blanc et son *offensive active*. En fait Shakarian affirme que le cyberespionnage est directement dans la stratégie chinoise[81]. Donc, la stratégie chinoise démontre une capacité de faire des activités d'une grande complexité dans le cyberespace et, même si la Chine optera probablement plus pour le cyberespionnage, elle sera prête à faire la cyberguerre si nécessaire.

---

[80] Ventre, *La guerre de l'information*, p. 86.
[81] Shakarian, Shakarian et Ruef, *Introduction to cyber-warfare*, p. 114.

Le cyberespionnage chinois

L'histoire démontre que la Chine est extrêmement active au niveau du cyberespionnage. Comme l'économie est très importante pour la Chine, elle n'hésitera pas à « espionner pour obtenir un avantage économique[82]. » Gendron et Rudner mentionnent que le cyberespionnage industriel est réel au Canada[83] et étant donné que la Chine est très active à ce niveau, il est normal de conclure qu'elle menace la sécurité économique du Canada. La Chine est également très active au niveau du cyberespionnage de cible militaire. Même si le tout ne peut lui être officiellement attribué, une « supposition éclairé[84] » [trad. libre] permet de déduire que la Chine était derrière l'affaire Ghosnet, ce qui lui a permis d'infiltrer le réseau de la *Recherche et développement pour la défense du Canada*[85]. Également, elle a apparemment réussi à infiltrer le programme du *Joint Strike Figther*[86], lui donnant ainsi accès à une large quantité de données sur cette plateforme de dernier cri. Il ne fait aucun doute que la Chine, par son espionnage sur des entités militaires[87], menace la sécurité nationale, mais également la crédibilité canadienne envers ses alliés, car si le Canada ne peut protéger ces réseaux informatiques militaires, ses alliés se verront forcés de restreindre les échanges d'informations. Au niveau de la protection des Canadiens, la Chine a peu d'intérêt et de bénéfice à s'attarder à des données privées d'individu au niveau du cyberespionnage. Reveron résume très bien la situation : « la liste des activités de cyberexploitation s'apparentant à être originaire de la Chine est longue, et les cibles sont un

[82] Department of Justice, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: First Time Criminal Charges Are Filed Against Known State Actors for Hacking* (Washington, D. C. : Office of the Public Affairs, 19 mai 2014), p. 1, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[83] Gendron et Rudner, *Assessing Cyber Threats to Canadian Infrastructure*, p. 27.

[84] Poindexter, *The Chinese Information War*, p. 89.

[85] Greg Weston, « Foreign hackers attack Canadian government: Computer systems at 3 key departments penetrated », CBC News, 17 février 2011, http://www.cbc.ca/news/politics/foreign-hackers-attack-canadian-government-1.982618.

[86] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. 4.

[87] Platt, « Still the fire-proof house? An analysis of Canada's cyber security strategy », *International Journal*, p. 160.

mixte des départements gouvernementaux et du secteur privé.[88] » C'est pour cette raison que trois des intérêts canadiens, la sécurité de l'économie, la sécurité nationale et la crédibilité canadienne envers ses alliés sont menacés par le cyberespionnage chinois.

La probabilité du cyberespionnage chinois est moyenne. Même si la Chine est très active dans le cyberespace, le Canada n'est pas la seule et la principale nation ciblée. Le Canada a déjà été une cible par le passé, mais les États-Unis sont probablement une cible plus attrayante, et c'est pour cette raison que John Tkacik, un membre senior du *International Assessment and Strategy Center*, recommande à des organisations gouvernementales américaines de définir la Chine comme la menace numéro un d'espionnage[89]. Au niveau de la gravité, de par son immense expertise et ses succès, il est possible de penser que la Chine peut occasionner de grands dommages par son cyberespionnage. Cependant, deux facteurs doivent être considérés. Premièrement, tel qu'avancé par Magnus Hjortdal, chef de section dans le ministère des Affaires étrangères du Danemark, il est possible que la menace chinoise est peut-être gonflée par les États-Unis[90]. En outre, basé sur son analyse de la crise du Xinjiang, Ventre énonce que « le système chinois de contrôle et de régulation du cyberespace ne soit moins efficace, structuré, coordonné qu'on ne l'imagine[91]. » Donc, avec ces considérations, la gravité peut être logiquement attribuée comme étant moyenne. Avec une probabilité moyenne et une gravité moyenne, la menace du cyberespionnage chinois envers les trois intérêts canadiens est moyenne.

La cyberguerre chinoise

La possibilité d'une cyberguerre prend souvent différentes significations. Cependant, la Chine n'attaquerait sûrement pas l'économie canadienne. Comme mentionne Geers, il est peu

---

[88] Reveron, *Cyberspace and National Security*, p. 201.

[89] Tkacik, *Trojan Dragon: China's Cyber Threat*, p. ii, http://s3.amazonaws.com/thf_media/2008/pdf/bg2106es.pdf.

[90] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. 12.

[91] Ventre, *Cyberguerre et la guerre de l'information*, p. 293.

probable qu'une nation attaque le système économique d'une autre nation étant donné que tout est interconnecté[92]. Basé sur sa stratégie, ceci est encore plus vrai pour la Chine. Il en est de même pour la sécurité des Canadiens, la Chine ne s'attarderait pas à attaquer des données privées alors qu'elle fait la cyberguerre à un état. Au niveau de la sécurité nationale et la crédibilité du Canada envers ces alliés, la cyberguerre chinoise peut définitivement être une menace. Cependant, cette menace ne devrait pas prendre la forme d'une attaque uniquement dans le cyberespace. Ventre mentionne que même si la cyberguerre correspond à la stratégie chinoise, elle possède « une petite valeur stratégique et une faible capacité de faire des dommages réels[93]. » [trad. libre] Cependant, elle pourrait prendre la forme d'une attaque massive sur l'infrastructure critique ou sur les systèmes de commandement et contrôle afin de supporter une opération militaire conventionnelle. Burtimas mentionne que la vraie menace d'une nation est l'attaque des infrastructures critiques[94]. Également, Geers mentionne que les nations doivent envisager à faire face à des cyberattaques pour supporter des opérations[95]. Les cyberattaques agissent comme un multiplicateur de force incroyable lorsqu'ils supportent directement une opération. Elle pourrait paralyser temporairement un ennemi[96]. Ce type de cyberattaque limité, selon Wark, est plus probable, car il « devance l'établissement des lois des conflits armés et est libre de la doctrine militaire[97]. » [trad. libre] Bref, la cyberguerre chinoise menace la sécurité nationale et la crédibilité du Canada envers ces alliés.

---

[92] Geers, « The cyber threat to national critical infrastructures », *Information Security Journal: A Global Perspective*, p. 5.

[93] Daniel Ventre, « Cyberconflict: Stakes of Power », *Cyberwar and Information Warfare* (London : Wiley-ISTE, 2011), p. 151.

[94] Butrimas, « National Security and International Policy Challenges in a Post Stuxnet World », *Lithuanian Annual Strategic Review*, p. 30.

[95] Geers, « The cyber threat to national critical infrastructures », *Information Security Journal: A Global Perspective*, p. 4.

[96] Hjortdal, « China's use of cyber warfare », *Journal of Strategic Security*, p. 3.

[97] Wark, « Cyber-Aggression and Its Discontents », *Global Brief*, p. 2, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

La probabilité d'une cyberguerre avec la Chine est peu probable. Autant pour la cyberattaque massive se limitant au cyberespace que pour la cyberattaque qui supporte les opérations. La raison est simple, le cyberespace est en constant changement[98]. Les mises à jour constantes des configurations réseaux, des antivirus, etc. occasionnent un défi autant pour l'attaquant que pour le défenseur. Ceci explique peut-être pourquoi une cyberattaque massive se limitant au cyberespace n'a jamais été observée[99]. Pour ce qui est de la cyberguerre limitée, c.-à-d. en support aux opérations militaires, ce n'est pas la cyberguerre qui est peu probable, mais bien l'opération militaire en tant que telle. Comme mentionne Reveron :

> Heureusement, le scénario le plus dangereux est très peu probable. De bonnes relations entre les grandes puissances capables de conduire des attaques cyber et conventionnelles simultanées sont renforcées par une bonne vieille dissuasion nucléaire. De la même manière, les infrastructures cyber et physiques nous rendent vulnérables à ce scénario, n'importe quel état qui attaquerait devrait avoir accès à sa propre capacité de ses infrastructures pour être capable d'exécuter un effort cyber majeur. Ces capacités cyber et la force cinétique utilisées lors d'une attaque sont également des cibles potentielles, au même titre que le restant des infrastructures essentielles de l'attaquant. Donc, c'est très peu probable qu'un état fera une telle attaque parce qu'il a également beaucoup à perdre[100]. [trad. libre]

Ceci explique clairement que la cyberguerre est peu probable. Même si la dissuasion nucléaire ne peut s'appliquer directement au Canada, la proximité avec les États-Unis permet de bénéficier de leur dissuasion.

Au niveau de la gravité, il est certain qu'un état comme la Chine, avec une force intégrée capable d'opération complexe dans le cyberespace, peut causer de grands dommages initiaux et ce, même plus grands qu'une cyberattaque terroriste. Cependant, avec la nature non permanente des cyberattaques, la gravité pourrait en être mitigée. Lewis mentionne clairement que « les cyberattaques sont, à moins qu'elle ne soit accompagnée par une attaque physique simultanée qui

---

[98] Geers, « The cyber threat to national critical infrastructures », *Information Security Journal: A Global Perspective*, p. 3.

[99] Andrew Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Washington D. C. : CSBA, 2012), p. v.

[100] Reveron, Cyberspace and National Security, p. 62.

occasionne des dommages physiques, de courte durée et inefficace[101]. » En plus, elle fonctionnerait qu'une seule fois[102]. Donc, étant donné que seulement deux des quatre intérêts canadiens sont menacés, il est possible de déduire que la gravité est de moyenne à élever. Avec une gravité moyenne à élever et une probabilité faible, la menace de la cyberguerre chinoise envers la sécurité nationale et la crédibilité du Canada envers ces alliés est moyenne.

La section trois a démontré que trois des quatre intérêts canadiens sont menacés par la Chine dans le cyberespace. Il s'agit de la sécurité de l'économie, la sécurité nationale et la crédibilité canadienne envers ses alliés. Cependant, même si l'analyse s'est basée sur la stratégie chinoise et elle a cernée les activités du cyberespace de la Chine, cette analyse peut être valide pour n'importe quel autre état, car la Chine est un des acteurs, sinon l'acteur le plus important dans le cyberespace. Donc, le cyberespionnage et la cyberguerre d'un état occasionnent chacun une menace moyenne envers les intérêts canadiens. En revue finale, en comparant toutes les menaces du cyberespace face aux intérêts canadiens, le niveau de menace le plus élevé provient des pirates informatiques, du cyberespionnage et de la cyberguerre chinoise qui sont tous de niveau moyen. Cela permet de prouver que la menace cyber est seulement une menace de niveau moyen face aux intérêts canadiens.

CONCLUSION

Cet essai a analysé la vraie menace dans le cyberespace. Tous les acteurs potentiels du cyberespace ont été analysés afin de quantifier la menace qu'ils représentent face aux intérêts canadiens. Pour ce faire les intérêts canadiens ont tout d'abord été définis. Le premier est la sécurité de l'économie où la sécurité dans le cyberespace et la coopération avec le secteur privé

---

[101] Lewis, Assessing the risks of cyber terrorism, cyber war and other cyber threats, p. 11.

[102] Geers, « The cyber threat to national critical infrastructures », *Information Security Journal: A Global Perspective*, p. 3.

est essentielle pour une économie nationale prospère. Le deuxième est la sécurité nationale qui inclue la cybersécurité des réseaux informatiques et des infrastructures essentielles qui sont cruciales afin d'assurer la sécurité du pays. La troisième est la sécurité des Canadiens qui sont des cibles pour certains acteurs dans le cyberespace, mais le gouvernement possède une certaine responsabilité de les protéger. Finalement, il y a la crédibilité du Canada envers ses alliés, surtout les États-Unis, qui tous accordent une importance grandissante à la sécurité dans le cyberespace et le Canada doit faire de même afin d'entretenir ses bonnes relations. Par la suite, les différentes menaces ont été évaluées et quantifiées. La menace cyberterroriste est de faible à moyenne car même si les cyberterroristes peuvent causer beaucoup de dommages à tous les intérêts canadiens, il y a très peu de chance que cela se produise. La menace cybercriminelle est faible, car leur omniprésence est mitigée par leur accent sur leurs bénéfices monétaires qui affectent peu une nation entière. La menace des pirates informatiques est moyenne. Même s'ils sont omniprésents, leurs dommages sont limités et une attaque majeure de leur part affectant substantiellement une nation a peu de chance de se produire. Finalement la Chine a été analysée afin d'évaluer la menace d'un état dans le cyberespace. L'analyse de la stratégie chinoise a permis de constater qu'avec son *offensive active*, sa *guerre du peuple* et une approche intégrée, la Chine a la capacité de conduire des activités complexes de cyberespionnage et cyberguerre dans le cyberespace. La menace du cyberespionnage d'un état est moyenne car même si la Chine est active au niveau du cyberespionnage, elle n'est peut-être pas si supérieure qu'on le pense. Finalement, la menace de la cyberguerre d'un état est moyenne, car les dommages initiaux étant potentiellement dévastateurs sont mitigés par une employabilité limitée en soutien aux opérations conventionnelles et une faible probabilité d'occurrence. Après l'analyse de toutes les menaces, les pires menaces sont de niveau moyen. Ce qui démontre que la menace cyber est seulement une

menace de niveau moyen face aux intérêts canadiens. Donc, même si le Canada est menacé, la nation n'est pas en péril dans le cyberespace. Cependant, si la situation mondiale dégénère pour se retrouver dans un conflit mondial interétatique, les pires scénarios à faible probabilité deviendront réalité. Le cyberespace deviendrait un champ de bataille impitoyable qui pourrait avoir des conséquences désastreuses pour plusieurs pays.

BIBLIOGRAPHIE

Ahamad, Mustaque, Dave Amster, Michael Barrett, Tom Cross, George Heron, Don Jackson, Jeff King, Wenke Lee, Ryan Naraine, Gunter Ollmann, Jon Ramsey, Howard A. Smith et Patrick Traynor. « *Emerging cyber threats report for 2009* », Atlanta, GA : Goergia Tech Information Security Center, 2008.

Bachmann, Sascha-Dominik Oliver Vladimir. « Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management », extrait de *Amicus Curiae* 88 (2012), p. 24-27.

Butrimas, Vytautas. « National Security and International Policy Challenges in a Post Stuxnet World », extrait de *Lithuanian Annual Strategic Review* 12, n^0 1 (2014), p. 11-31.

Canada. Bureau du Conseil Privé. *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Ottawa : Bureau du Conseil Privé, 2004.

Canada. Bureau du vérificateur général du Canada. Chapitre 3, « Protecting Canadian Critical Infrastructure Against Cyber Threats », extrait de *Report of the Auditor General of Canada to the House of Commons*, Ottawa : Travaux publics et Services gouvernementaux Canada, 2012.

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

Canada. Sécurité publique Canada. *Plan d'action sur les infrastructures essentielles : 2014-2017*, Ottawa : Sécurité publique Canada, 2014.

Canada. Sécurité publique Canada. *Stratégie de la cybersécurité du Canada : Renforcer le Canada et accroître sa prospérité*, Ottawa : Sécurité publique Canada, 2010.

Canada. Sécurité publique Canada. *Stratégie nationale sur les infrastructures essentielles*, Ottawa : Sécurité publique Canada, 2009.

Cavelty, Myriam Dunn. « Cyber-Terror - Looming Threat of Phantom Menace? The Framing of the US Cyber-Threat Debate », extrait de *Journal of Information Technology & Politics* 4, n^0 1 (2007), p. 19-36.

Collins, Sean, et Stephen McCombie. « Stuxnet: the emergence of a new cyber weapon and its implications », extrait de *Journal of Policing, Intelligence and Counter Terrorism* 7, n^0 1 (2012), p. 80-91.

Czosseck, Christian, et Kenneth Geers. *The Virtual Battlefield: Perspectives on Cyber Warfare*, Volume 3, Amsterdam : IOS Press, 2009.

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

Devost, Matthew G., et Neal A. Pollard. T*aking Cyberterrorism Seriously: Failing to Adapt to Emerging Threats Could Have Dire Consequences,* Burke, VA : Terrorism Research Center, Inc., 2002.

États-Unis. Department of Justice. *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage: First Time Criminal Charges Are Filed Against Known State Actors for Hacking*, Washington, D. C. : Office of the Public Affairs, 19 mai 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

Geers, Kenneth. « The cyber threat to national critical infrastructures: Beyond theory », extrait de *Information Security Journal: A Global Perspective* 18, n^0 1 (2009), p 1-7.

Gendron, Angela, et Martin Rudner. *Assessing Cyber Threats to Canadian Infrastructure,* Ottawa : Canadian Security Intelligence Service, 2012.

Gray, Colin S. *Strategy for Chaos : Revolution in Military Affairs and the Evidence of History*, London : Frank Cass, 2002.

Greitzer, Frank L., Andrew P. Moore, Dawn M. Cappelli, Dee H. Andrews, Lynn A. Carroll et Thomas D. Hull. « Combating the insider cyber threat », extrait de *Security & Privacy, IEEE* 6, n^0 1 (2008), p. 61-64.

Hjortdal, Magnus. « China's use of cyber warfare: Espionage meets strategic deterrence », extrait de *Journal of Strategic Security* 4, n^0 2 (été 2011), p. 1-24.

International Cyber Security Protection Alliance. *Rapport d'enquête sur le cybercrime au Canada*, Chesham : ICSPA, 2013.

Janczewski, Lech J., et Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*, Hersey, PA : IGI Global, 2008.

Krepinevich, Andrew. *Cyber Warfare: A "Nuclear Option"?*, Washington D. C. : CSBA, 2012.

Kshetri, Nir. « Pattern of global cyber war and crime: A conceptual framework », extrait de *Journal of International Management* 11, n^0 4 (2005), p. 541-562.

Kuehl, Daniel T. Chapitre 2, « From Cyberspace to Cyberpower: Defining the Problem », extrait de *Cyberpower and national security*, Washington D. C. : National Defense University Press, 2009.

Lewis, James Andrew. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*, Washington, D. C. : Center for Strategic & International Studies, 2002.

Libicki, Martin. *Cyberdeterrence and Cyberwar*, Washington, D. C. : RAND, 2009, http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Liff, Adam P. « *Cyberwar:* A new 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War », extrait de *The Journal of Strategic Studies* 35, n^0 3 (juin 2012), p. 401-428.

Nye Jr., Joseph S. « *Cyber power* », Cambridge, MA : Belfer Center for Science and International Affairs, 2010.

Platt, Victor. « Still the fire-proof house? An analysis of Canada's cyber security strategy », extrait de *International Journal* 67, n^0 1 (hivers 2011-12), p. 155-167.

Poindexter, Dennis F. *The Chinese Information War: Espionage, Cyberwar, Communication Control and Related Threats to United States Interests*, Jefferson, NC : McFarland & Company, Inc., 2013.

Ranger, Steve. « Hostile state-sponsored hackers breached government network », extrait de *ZDNet*, 17 juin 2014, http://www.zdnet.com/article/hostile-state-sponsored-hackers-breached-government-network/.

Ranger, Steve. « Inside the secret digital arms race: Facing the threat of a global cyberwar », extrait de *TechRepublic*, 16 avril 2006, http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/.

Ranger, Steve. « NATO updates cyber defence policy as digital attacks become a standard part of conflict », extrait de *ZDNet*, 30 juin 2014, http://www.zdnet.com/article/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict/.

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

Rid, Thomas, et Peter McBurney. « Cyber-weapons », extrait de *The RUSI Journal* 157, n^0 1 (2012), p. 6-13.

Rid, Thomas. « Cyberwar Will Not Take Place », extrait de Journal of Strategic Studies 35, n^0 1 (février 2012), p. 5-35, http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939.

Schreier, Fred. On Cyberwarfare, DCAF Horizon 2015 Working Paper n^0 7, Genève : DCAF, 2012.

Shakarian, Paulo, Jana Shakarian, et Andrew Ruef. *Introduction to cyber-warfare: A multidisciplinary approach*, Waltham, MA : Elsevier, Inc., 2013.

Shakarian, Paulo. « Stuxnet: cyberwar revolution in military affairs », extrait de *Small Wars Journal* (2011), http://www.dtic.mil/dtic/tr/fulltext/u2/a546439.pdf.

Shore, Jacques J. M. « An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security », extrait de *International Journal of Intelligence and CouterInterlligence* 28, n^0 2 (2015), p. 236-251.

Springer, Paul J. *Cyber Warfare: A Reference Handbook*, Santa Barbara, CA : ABC-CLIO, 2015.

Suciu, Peter. « Why cyber warfare is so attractive to small nations », extrait de *Fortune*, 21 décembre 2014, http://fortune.com/2014/12/21/why-cyber-warfare-is-so-attractive-to-small-nations/.

Tabansky, Lior. « Basic Concepts in Cyber Warfare », extrait de *Military and Strategic Affairs* 3, n^0 1 (mai 2011), p. 75-92.

The US-China Economic and Security Review Commission. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, McLean, VA : Northrop Grumann Corporation Information Systems Sector, 2009.

Theohary, Catherine A., et John W. Rollins. « *Cyberwarfare and Cyberterrorism: In Brief* », Washington, D. C. : Congressional Research Service, 2015, https://fas.org/sgp/crs/natsec/R43955.pdf.

Tkacik, John J. Trojan Dragon: China's Cyber Threat, Executive Summary Backgrounder n^0 2106, Washington, D. C. : The Heritage Foundation, 2008, http://s3.amazonaws.com/thf_media/2008/pdf/bg2106es.pdf.

Trevino, Cassandra M., Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, et Jason Frye. « *Cyber threat metrics* », Albuquerque, NM : Sandia National Laboratories, 2012.

Ventre, Daniel. Chapitre 4, « Cyberconflict: Stakes of Power », extrait de *Cyberwar and Information Warfare*, London : Wiley-ISTE, 2011.

Ventre, Daniel. *Cyber Conflict: Competing National Perspectives*, Croydon : ISTE Ltd, 2012.

Ventre, Daniel. *Cyberguerre et la guerre de l'information : stratégies, règles, enjeux*, Paris : Lavoisier, 2010.

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

Wark, Wesley. « Cyber-Aggression and Its Discontents », extrait de *Global Brief*, 4 octobre 2012, http://globalbrief.ca/blog/2012/10/04/cyber-aggression-and-its-discontents/.

Wiemann, Gabriel. « *Cyberterrorism : How Real Is the Threat?* », Special Report 119, Washington, D. C. : United States Institute of Peace, 2004, http://www.usip.org/sites/default/files/sr119.pdf.