

*Cyberconflits et règles d'engagement : perspective pour une orientation
politique canadienne*

*Cyberconflicts and Rules of Engagement: a Perspective for Canadian
Policy Orientations*

Jean-Christophe Boucher

(jean-christophe.boucher@hei.ulaval.ca)

&

Hugo Loiseau

(hugo.loiseau@hei.ulaval.ca)

Le tissage de la toile cybernétique représente sans aucun doute l'une des innovations les plus importantes de la fin du XX^e siècle. Cette toile modifia considérablement le quotidien des individus appartenant aux sociétés occidentales. De fait, la création de ce lieu public virtuel ainsi que la multiplication des « relations cybernétiques » entre les individus constituent une nouvelle donne dont les gouvernements doivent tenir compte. Manifestement, à l'instar du territoire national, la protection de cet environnement émergent apparaît de plus en plus fondamentale. Or, une conception pratique des cyberconflits fait cruellement défaut dans la littérature. Comment en effet l'État peut et doit agir dans ce nouveau contexte? En se basant sur les règles d'engagement régissant les conflits conventionnels, la tâche qui s'impose s'avère être double. D'une part, à partir de la littérature, ce texte élabore une revue des diverses formes de cyberconflits ainsi que de leurs distinctions et originalités par rapport aux problèmes de sécurité plus traditionnels. D'autre part, ce texte considère les ramifications légales et éthiques qui peuvent s'appliquer à ce problème de sécurité en émergence. Tout cela afin de construire une assise théorique à l'aide de laquelle le Canada pourra orienter sa politique de sécurité en la matière et de formuler des règles d'engagement appropriées à ses objectifs de défense.

The development of the World Wide Web certainly represents one of the most important innovations of the end of the twentieth century. The Web considerably modified the daily lives of individuals living in western societies. In fact, the creation of this virtual public domain and the multiplication of “cybernetic relations” between individuals constitute a new domain, which governments must acknowledge and take into account. The protection of this emerging environment will become as fundamental to states as their territory is. However, a practical understanding of cyberconflict lacks in the existing literature. In this new context, what are the actions that states must, and can, accomplish to protect this critical structure? In light of the rules of engagement that apply to conventional conflicts, we see our present task in two fold. On the one hand, by reviewing the extant literature on the subject, we elaborate an understanding of the multiple forms of cyberconflicts and their distinctiveness in comparison with more traditional security issues. Secondly, this text tries to discern the various legal and ethical ramifications of this emerging security threat. Our main goal is to develop a theoretical background upon which Canada could orient its security policy and formulate rules of engagement appropriate with its defence objectives.

Introduction

Sur le plan militaire, les dix dernières années ont été riches en profonds changements. Il suffit de penser à la révolution des les affaires militaires (RAM), aux opérations de maintien de la paix de troisième génération, à l'émergence du concept de sécurité humaine... Tous ces développements sont le reflet des nombreuses transformations survenues dans l'espace international au cours de cette période. La réalité change et les théories doivent expliquer et rendre compte de ces évolutions.

Parmi ces changements, un problème émerge avec de plus en plus d'ampleur. Il s'agit de la sécurité face aux menaces en provenance du cyberspace. Les gouvernements et les législateurs prennent davantage conscience de cet important problème souterrain qui est plus difficilement discernable face à d'autres menaces plus traditionnelles à la sécurité. En somme, forcés de réagir car vulnérables, les gouvernements doivent trouver, ou à tout le moins proposer, des solutions afin de contrer cette nouvelle forme de menace. Cela soulève plusieurs questions d'ordre éthique, juridique et politique mais aussi des questions d'ordre militaire auxquelles ce texte entend répondre. Se questionner et réfléchir sur les cyberconflits est d'autant plus criant que, actuellement, la menace semble sous-évaluée. Pourtant, celle-ci est belle et bien présente. D'ailleurs, la dernière cyberattaque rapportée le 24 octobre 2002 est considérée comme majeure par les spécialistes. En fait, le vide juridique existant présentement en ce qui concerne le cyberspace laisse une incroyable marge de manœuvre aux cyberpirates. Ce texte se penchera sur la réponse que doivent donner les gouvernements et les forces armées, en termes de règles d'engagement, dans

l'éventualité d'une attaque informatique en provenance du cyberspace.

Dans un premier temps, nous tenterons de fournir un aperçu général de la littérature sur les cyberconflits et les problèmes de sécurité qu'ils engendrent. Dans un deuxième temps, nous chercherons à considérer l'applicabilité du cadre analytique des règles d'engagement aux menaces cybernétiques. En quelque sorte nous désirons explorer la validité théorique d'une telle entreprise afin d'édifier une compréhension initiale de la possibilité d'une politique canadienne orientée vers ce sujet.

Revue de littérature

Toute revue de littérature portant sur les cyberconflits et sur le cyberspace doit faire face à deux difficultés. D'une part, la littérature sur le sujet devient rapidement obsolète face aux progrès qu'enregistre l'industrie des hautes technologies. Il est donc difficile de prendre un certain recul face aux événements et aux avancées technologiques qui, parfois, bouleversent les plus solides analyses. Les gouvernements se retrouvent aussi dans cette situation puisque leurs législations et plans d'action sont toujours décalées par rapport à la réalité. D'autre part, à cette difficulté s'ajoute la nouveauté du sujet et le caractère multiforme des cyberconflits. Ceux-ci touchent à la fois à la protection des infrastructures civiles et militaires, à la protection des renseignements, à la diffusion à grande échelle de savoirs normalement prohibés (fabrication de bombes, techniques de piratage informatique, secret d'État...), à la sécurité économique, à la sécurité publique et, surtout, à la sécurité nationale. De surcroît, les cyberconflits font l'objet de recherches peu définies et surtout mal expliquées. Cet objet mêle guerre de l'information, cyberspace, nouvelles technologies des communications, cyberterrorisme... dans un ensemble confus. En définitive, pour toutes ces raisons, tout propos sur la littérature traitant des dilemmes de sécurité associés au cyberspace doit inévitablement faire des choix qui laissent dans l'ombre des analyses intéressantes mais désuètes ou des études trop éloignées du cœur du problème.

Pour circonvier à ces deux difficultés, cette revue de littérature se concentrera sur les conséquences de la prise en compte du cyberspace sur la sécurité nationale et les politiques de défense. Il faut également tenir compte que la littérature sur les cyberconflits, quoique encore clairsemée, louvoie entre plusieurs courants: positiviste, alarmiste, à la limite de la science fiction, largement normative et descriptive... dont les apports se situent à différents degrés d'importance.

Le premier constat qui peut être fait est que les cyberconflits et leur existence même sont directement liés à la technologie et aux développements technologiques et informatiques. D'ailleurs, pour Michel Wautelet, les technologies de l'information ne sont pas exclusivement au domaine militaire mais bien universelles puisque n'importe qui peut se les procurer. Cette facilité d'utilisation annonce une véritable prolifération des armes technologiques. La distribution de la puissance dans l'espace international est remodelée par les nouvelles technologies et l'information (NTI) et le différentiel de puissance s'accroît ainsi entre les États puissants et les autres en même temps que s'accroît la vulnérabilité des États puissants. D'ailleurs, l'utilisation des NTI augmente la capacité de faire des dégâts par des États, des groupes ou des individus au but malveillant. Gansler, corroborant ces propos, est à clair à ce sujet : « Cyberspace tends to level the playing field between the entities in that space and offers attackers many high-value, low-risk targets. [...] Unlike physical break-ins, Internet attacks are easy. » L'utilisation et le développement des NTI constituent donc les principales bases au déploiement des cyberconflits et des guerres électroniques.

Wautelet définit les cyberconflits comme l'utilisation «de toutes les ressources du cyberespace pour détruire des éléments essentiels de la société de l'adversaire.». Donc un cyberconflit peut engendrer des problèmes et des dégâts économiques colossaux, des dégâts matériels, des dégâts informatiques et, conséquence de tout cela, des pertes de vie humaine majoritairement civile. La particularité des cyberconflits est qu'ils ne détruisent rien de physiquement réel mais leurs conséquences entraînent des destructions massives car de plus en plus, les États industrialisés ont développé une dépendance face aux réseaux informatiques pour ce qui est de la sécurité publique, de la sécurité économique et surtout de la sécurité nationale.

Or, Wautelet fait une nette distinction entre la guerre électronique et les cyberconflits. La première se définit comme «l'utilisation de toutes les techniques électroniques ainsi que le chiffrement et le décryptage assisté par ordinateur» afin de mener à terme un conflit. La guerre électronique fait donc usage des technologies intelligentes appliquées aux armes et aux ordinateurs ainsi qu'à tout ce qui entoure la guerre c'est-à-dire les communications, le renseignement, l'observation et les infrastructures pour déployer ces réseaux. L'exemple de la guerre du Golfe comme une des premières guerres électroniques est sans doute le plus cité dans la littérature. En somme, la guerre électronique et son déploiement (le débordement) dans le cyberespace n'est qu'une incidence dans le but ultime du conflit : la victoire traditionnelle par la neutralisation des moyens de défense et d'attaque de l'ennemi.

Les cyberconflits sont de toute évidence des conflits se déroulant dans le cyberespace. Il apparaît donc essentiel de définir ce nouveau lieu de combat. Martin Libicki, une sommité en ce qui concerne les questions entourant le cyberespace et la guerre de

l'information, propose une typologie éclairant le présent débat. D'emblée, il affirme que la guerre de l'information prise comme une technique indépendante pour faire la guerre est un concept assez faible. En réalité, cette notion prend tout son sens lorsqu'on lui distingue des sous-catégories beaucoup plus opérationnelles à la fois pour les chercheurs et les militaires en général. Ainsi, Libicki décrit sept types ou sous-types de guerre de l'information lui servant de base pour le reste de son analyse. Le dernier de ces types concerne les cyberconflits et, selon sa perspective, ce type de conflit demeure encore entre la science-fiction et la réalité. Cet auteur juge leurs occurrences fort improbables.

Toutefois, la problématique est de savoir comment faire la guerre dans le cyberspace puisque cela est possible même si improbable. Un document du Pentagone classe les cyberconflits dans la catégories des opérations d'information (IO) qu'il définit comme « action taken to affect adversary information and information systems while defending one's own information and information systems. » À l'instar du Pentagone, le Ministère de la défense nationale du Canada classe également les cyberconflits dans la catégorie des opérations d'information tel que le mentionne un document du SCRS. Celui-ci considère les opérations d'information comme étant issue du concept de la guerre de l'information c'est-à-dire « les opérations physiques et informatiques menées par des forces militaires en temps de conflit et d'avant-conflit en vue de compromettre l'acheminement et la viabilité des informations et leurs propres systèmes. »

Néanmoins, selon Clemmons et Brown, cette définition est insuffisante pour englober la réalité des cyberconflits et la façon de combattre dans le cyberspace. Pour eux, il faudrait plutôt concevoir ce concept comme : « nonkinetic, offensive actions taken to achieve information superiority by affecting enemy information-based process, information systems and computer-based networks. » Cette définition limiterait la portée de la doctrine du Pentagone en situation de cyberattaque et de cyberconflits. Cependant, les auteurs ne proposent pas de véritables procédures ou règles d'engagement en cas de cyberconflits. En dernière analyse, leur évaluation des cyberconflits et du cyberspace demeure dans le courant de pensée central en terme de théorie et de stratégie militaire.

Il nous apparaît nécessaire de s'attarder aux conséquences de la présence du cyberspace autant dans l'ordre international que dans le quotidien des individus. Wautelet, sans le dire expressément, affirme qu'il existe deux grands paradoxes sous-jacents au cyberspace et, par voie de conséquence, à l'occurrence des cyberconflits. D'une part, le cyberspace est à la fois un lieu et un enjeu de conflit. C'est un lieu de conflit car le cyberspace est ouvert à tous et accessible avec peu de connaissances et peu de moyens. Cette qualité intrinsèque au cyberspace favorise l'augmentation constante du nombre de ses utilisateurs et plus il y a d'utilisateurs plus les possibilités de conflits entre eux sont grandes. D'autant plus que comme le dit Wautelet «il n'y a aucune uniformité culturelle, légale, éthique, politique dans le cyberspace.». C'est aussi un enjeu puisque que le

cyberespace s'est au départ développé de manière anarchique et les considérations de sécurité n'étaient point envisagées à l'origine. Les gouvernements et les organisations internationales ont pris du retard en terme de législation et de contrôle face à ce développement même si de grands secteurs de la société : économique, industriel, militaire ont créé de puissants liens de dépendance envers cet espace. Enfin, il faut aussi ajouter que le cyberespace est complémentaire et englobant la triade traditionnelle (terre-air-mer) de déploiement des conflits. Ce qui fait en sorte que le contrôle de cet espace de combat devient primordial durant toutes les phases d'un conflit. Cette situation pousse donc les responsables politiques et militaires à se questionner sur l'impact du cyberespace sur la paix et la sécurité dans le monde.

D'autre part, le cyberespace est à la fois menace et menacé. Il est simultanément arme et cible. Il est source d'insécurité car il est difficilement compréhensible pour le commun des mortels du fait qu'il est hautement abstrait. C'est un nouvel espace de combat qui n'a pas de frontières clairement définies et qui ne relève pas exclusivement des forces militaires ni uniquement du domaine d'application des lois comme l'affirme Donald A. La Carte. En fait, les conflits dans le cyberespace sont globaux puisqu'ils englobent tous les autres espaces et transcendent autant les sphères civiles et militaires que les lois nationales et le droit international. Cette affirmation est d'autant plus vraie que toutes les possibilités du cyberespace n'ont pas encore été ni explorées ni définies. Si bien qu'il est encore difficile de déterminer la différence entre un crime et attaque dans le cyberespace. De plus, le cyberespace est propice au développement et à la prolifération de nouveaux types d'armes : les bombes logiques, les virus informatiques... ainsi qu'à des tactiques plus traditionnelles telles que la manipulation de l'information ou la guerre psychologique. Tout en étant menaçant, le cyberespace est menacé. Il est menacé car il contient de nombreuses failles de sécurité à tous ses niveaux. L'exemple le plus frappant est sans doute la vulnérabilité des infrastructures et des composantes logicielles qui soutiennent et donnent vie au cyberespace.

Ceci étant dit, une question demeure toujours à débattre : la menace en provenance du cyberespace est-elle réelle? Deux écoles de pensée s'affrontent sur cette question. La première affirme que la menace est belle et bien réelle et que les attaques en provenance du cyberespace doublent à tous les ans et que la vulnérabilité des infrastructures du cyberespace incite les esprits malveillants à se servir de cet espace pour attaquer. La seconde école de pensée croit que les enjeux associés à l'utilisation du cyberespace sont tellement grand que le marché par lui-même règlera les failles de sécurité et que les institutions et les entreprises qui ne se protègent pas périront. En somme, ils pensent que la menace provenant du cyberespace sera étouffée par les actions des gouvernements et des entreprises qui ne veulent pas que le système économique, ou une partie de celui-ci, s'effondre et entraîne dans sa chute des conséquences incalculables.

Sans résoudre ce débat, les penseurs militaires apportent souvent de bonnes analyses quant au phénomène du cyberspace. Henry et Peartree offrent un aperçu général du lien qu'il est possible de tracer entre l'évolution des théories militaires et la guerre de l'information (information warfare ou IW). Ils tentent de démontrer que les nouvelles technologies ont historiquement une influence limitée sur les conflits. Selon eux, les changements technologiques influençant les conflits ont un impact éphémère. Ils appliquent cette idée aux nouvelles possibilités sur le champ de bataille qu'offrent les technologies de l'information. De prime abord, ils mettent en garde les lecteurs que les nouvelles technologies ont souvent été surestimées et ont conduit les états-majors et les théoriciens dans l'erreur ce qui a entraîné de maigres résultats autant sur le champ de bataille que dans les théories militaires. Ils enchaînent ensuite sur la principale contribution à la guerre qu'apportent les nouvelles technologies de l'information : la supériorité de l'information. Selon un scénario extrême, celle-ci permettrait non seulement de donner en temps réel des informations globales sur le champ de bataille mais aussi de manipuler, d'exploiter et de neutraliser les systèmes d'information ennemis.

Toutefois, selon Henry et Peartree, il est inutile de jouer au technoprophète pour être capable de comprendre les impacts futurs des nouvelles technologies de l'information sur les théories et le déroulement de la guerre. S'appuyant sur l'exemple de la théorie de la supériorité aérienne de Giulio Douhet qui s'est révélée inexacte, ils ressortent trois problèmes qui empêchent de prévoir correctement l'impact des nouvelles technologies de l'information : 1) la rapidité des changements technologiques, 2) la nature de l'information et des technologies qui lui sont adjacentes qui brouillent la distinction entre civil et militaire et 3) l'incertitude entourant la guerre de l'information en tant que telle.

Les propos de Henry et Peartree contrastent grandement face aux idées de Bunker qui affirme que la pensée militaire et stratégique traditionnelle est incorrecte. Cette pensée traditionnelle suppose le déroulement d'un conflit armé dans une logique où prévalent quatre dimensions (x, y, z et t). Pour Bunker, le champ de bataille futur se composera d'une cinquième dimension qu'il appelle le cyberspace. Il dénonce que seules les variables stratégiques, technologiques et militaires soient considérées dans la révolution des affaires militaires. Il se produit selon Bunker des changements socio-politiques fondamentaux qui vont transformer la nature de la guerre. Il appuie cette idée sur l'importance grandissante du cyberspace dans le déroulement des combats. Celle-ci se situe dans la compression des limites physiques et temporelles des quatre dimensions traditionnelles déjà mentionnées. Tout d'abord, l'utilisation du cyberspace pour faire la guerre diminue la distance entre l'arme et la cible entre le soldat et l'ennemi. Le cyberspace a un effet de « spatial contraction [that] takes two military objects that are far away from one another and brings them closer. » Ensuite, le cyberspace possède les mêmes vertus en ce qui a trait à la dimension temporelle (t) puisqu'il agit aussi comme un réducteur de temps entre la prise en compte d'un risque ou d'une menace et l'action militaire visant à éliminer ce risque ou cette

menace. Enfin, l'auteur prévoit que la dimension défensive des combats basée sur la structure physique des objets (le blindage par exemple) devra être réévaluée à la lumière de la nature post-mécanique d'une guerre dans la cinquième dimension. Il mentionne l'exemple de l'utilisation de l'énergie électromagnétique comme arme de futurs combats.

Toutefois, avant d'en arriver à des scénarios de science-fiction tel que Bunker les conçoit, il faut considérer la dimension éminemment politique du cyberspace. Dans son livre *La géopolitique d'Internet*, Solveig Godeluck affirme que les États régulateurs sont très peu présents dans le cyberspace puisque l'exercice du pouvoir s'effectue sur un territoire stable. Or, ce type de territoire n'existe pas dans le cyberspace. Bien entendu, ces États peuvent débrancher le réseau physique sur leur territoire national mais comme le cyberspace s'est construit selon une logique de duplication des informations et de décentralisation, ces États n'ont que très peu d'emprise régulatrice sur le contenu du réseau. En fait, selon elle, les compétences juridiques des États se chevauchent et s'enchevêtrent dans l'espace virtuel qu'est le cyberspace ce qui complique la régulation de cet espace. Dit plus simplement, les données transmises sur Internet ne s'arrêtent pas aux frontières. Cela s'explique par le fait que le cyberspace n'est pas un territoire aux frontières nationales réellement définies. Certains, tel Gansler, pensent que le cyberspace n'a pas de frontière tout simplement. En fait, les véritables régulateurs du cyberspace sont les internautes et les marchands (qu'elle désigne aussi sous le nom de technopouvoir). Ces deux groupes constituent en quelque sorte des défricheurs du cyberspace car ils forgent au fur et à mesure de leurs expériences la réalité que l'on nomme cyberspace. Ils en délimitent les possibilités et de cette manière viennent à réguler et à autoréguler cet espace. En somme, selon elle, nous sommes très loin de voir apparaître une organisation internationale chargée de réguler le réseau Internet.

Cette brève revue de littérature sur les cyberconflits et le cyberspace permet de conclure deux choses. Tout d'abord, il existe très peu d'études qui discutent véritablement de ce que devraient être les règles d'engagement d'une force armée nationale dans le cadre d'un cyberconflit. À tout le moins, les auteurs et les différents rapports gouvernementaux débattent de la nature et de l'ampleur de la réponse à donner en cas de cyberattaques. Considérant qu'il a été impossible de tout lire sur le sujet et que certains documents sont confidentiels, il est possible d'affirmer que très peu d'ouvrages mentionnent explicitement quelles devraient être les règles d'engagement précises en cas de cyberconflits. La question demeure donc entièrement ouverte et cela apporte de nombreux problèmes sur le plan opérationnel pour les forces armées. En outre, les opinions sont partagées devant la menace que pose le cyberspace. Les opinions sont tout autant partagées quant à déterminer qui doit s'occuper des cyberattaques en terme de juridictions civiles et militaires. La question n'est pas banale car il faut déterminer quelle institution est la plus apte à faire face aux cyberattaques : la police ou les forces armées et quelles seront les règles d'engagement prévalant? Face à ces faits, il est impératif de poser de bonnes

questions afin d'obtenir des réponses pertinentes et de mieux conceptualiser le cyberspace et les cyberconflits pour mieux les comprendre.

Règles d'engagement et cyberconflits

La problématique des règles d'engagement (RE) dans les cyberconflits se présente avec une acuité grandissante. En effet, loin de prononcer un jugement fataliste sur la possibilité des secteurs publics et privés de se prémunir complètement des attaques cybernétiques, nous croyons néanmoins qu'une telle démarche en vue d'augmenter la sécurité informatique doit être nécessairement accompagnée d'un plan d'action en vue de répondre aux éventuels assauts cybernétiques. À l'évidence, cette menace est croissante. D'une part, la faiblesse des réseaux informatiques canadiens augmente du fait de la multiplication du nombre de réseaux et d'utilisateurs internet, de la dépendance croissante des gouvernements, des institutions, des entreprises, des groupes et des individus à l'égard des communications informatisées et des technologies de l'information et de l'interopérabilité grandissante des systèmes informatiques gouvernementaux et internationaux. D'autre part, accentuant cette faiblesse, la probabilité d'une attaque cybernétique est ascendante en raison de la croissance trop rapide des technologies informatiques (tant au niveau des logiciels que des infrastructures), du coût relativement abordable des équipements nécessaires pour perpétrer ces attaques et de la grande accessibilité des techniques de cyberattaques. À la lumière de ces deux phénomènes, la question demeurant est à savoir comment le Canada doit et peut réagir face aux attaques cybernétiques?

Notre ambition est donc, à ce stade de notre réflexion, d'élaborer des principes d'action à l'aide desquelles le gouvernement canadien peut formuler sa politique en regard aux cyberconflits. Cette prédétermination de normes pratiques devrait servir plusieurs objectifs dont éviter l'improvisation et les risques de fomentation d'une crise internationale, d'établir une cohérence et une stabilité à l'action canadienne et, finalement, de promouvoir une réponse rapide et efficace de la part des autorités canadiennes face aux dangers associés aux cyberconflits. Or, il ne semble pas évident à première vue que l'introduction du concept de règles d'engagement puisse être applicable au cas particulier des cyberconflits. Par conséquent, dans une large mesure, les RE nous servent ici de modèle analytique. En tant qu'instrument de réflexion, nous ne considérons pas les RE comme étant la seule avenue possible pour élaborer des principes d'action lors des cyberconflits. Toutefois, les RE nous apparaissent comme un cadre approprié en vue de penser l'action canadienne en regard aux problèmes cybernétiques. Or, selon les Ordres et règlements des Forces canadiennes, les règles d'engagement se définissent comme : « Les RE constituent la façon dont les commandants militaires contrôlent l'utilisation de la force par leurs subalternes. » Autrement dit, les règles d'engagements sont un ensemble de normes ou de principes d'action définie préalablement en vue de l'utilisation efficace et proportionnée de la force. Appliqué au cyberconflit, les règles d'engagement seraient une détermination

péremptoire d'un code de conduite servant à encadrer la réponse canadienne à une attaque cybernétique d'une source étrangère.

La première interrogation est à savoir si l'emploi de mesures cybernétiques peut se prévaloir du concept de la force? Manifestement, au sens restreint du terme, on pourrait associer la force à des considérations d'ordre physique. Dans ce cas précis, il nous semblerait futile d'argumenter qu'une cyberréponse puisse se concevoir comme une application de la force. Néanmoins, au sens large du terme où la force est comprise comme une mesure ayant pour objectif essentiel d'imposer une volonté, l'utilisation du cyberspace à des fins illicites semblent prendre la forme d'un moyen en vue d'une finalité.

Ceci étant dit, il nous apparaît pertinent de considérer la question du domaine de compétence de l'action canadienne en cas de cyberconflits. Or, l'action de l'État canadien a deux champs d'application particuliers : soit au niveau national ou au niveau international. Ces deux niveaux nous amènent à réfléchir à deux scénarios envisageables qui influent nécessairement sur les actions du gouvernement. Premièrement, une attaque cybernétique est fomentée par une source domestique (un citoyen canadien, une entreprise ou une organisation canadienne) sur des cibles canadiennes. Ce scénario relève, à notre avis, du domaine interne de l'action canadienne et, par conséquent, la question demeure dans une large mesure du domaine criminel. Ainsi, l'action du gouvernement canadien est encadrée par un ensemble de mesures législatives nationales à cet effet. En ce sens, le concept des RE n'est guère adéquat pour structurer un débat qui relève plutôt de la sphère juridique canadienne. Par contre, si nous transposons notre réflexion au plan international, nous pouvons penser à une cyberattaque perpétrée par une source étrangère sur des objectifs canadiens. Si nous acceptons qu'une cyberréponse constitue en soi une utilisation de la force, il faut avouer qu'une attaque cybernétique d'une source étrangère constitue une action internationale et, donc, encadrée par un système juridique international auquel le Canada adhère. Or, dans l'ordre international, deux conditions permettent l'utilisation légitime de la force : en temps de guerre et dans le cadre restreint prévu par la Charte des Nations Unies. Pour l'essentiel, l'emploi de la force en temps de guerre demeure régit par le droit de la guerre enchâssée dans les diverses Conventions de Genève et leurs protocoles.

En regard aux dispositifs prévus par la Charte des Nations Unies, l'article 39 stipule clairement que le Conseil de sécurité est habilité à reconnaître toutes formes de « menaces à la paix, menace contre la paix, d'une rupture de la paix ou d'un acte d'agression. » Il faut remarquer ici le caractère suffisamment souple définissant les mesures à l'intérieur desquelles

le Conseil de sécurité peut identifier une source de « menace » et, par extension, élaborer des résolutions à cet effet. En théorie, et nonobstant l'énorme difficulté d'établir un consensus politique au sein du Conseil de sécurité, nous pourrions aisément admettre que cet organe pourrait identifier les attaques cybernétiques comme une « menace » à la paix. Ainsi, en vertu des articles 41 ou 42, une cyberréponse pourrait être envisageable sous l'égide des Nations Unies. En somme, la problématique des règles d'engagement serait considérée à l'intérieur du cadre restreint des résolutions et des objectifs définis par un mandat onusien.

En dernière analyse, la question demeurant est celle de l'utilisation des moyens cybernétiques en réponse à une attaque du même type dans la mesure où nous ne sommes pas dans un état de guerre et où il n'y pas de résolutions du Conseil de sécurité. Le cas échéant, il nous semble pertinent de faire valoir l'article 51 de la Charte des Nations Unies qui affirme le droit de tout État de recourir à la force dans l'intérêt de sa légitime défense. Le litige apparaît distinctement dans l'idée selon laquelle une attaque cybernétique puisse constituer une « agression armée » selon les termes de l'article. Or, dans la mesure où une cyberattaque était effectivement interprétée en tant qu'acte d'agression, la victime pourrait justifier une riposte analogue comme étant de l'ordre de la légitime défense en vertu des dispositions de l'article 51. Cependant, si la provocation n'est pas envisagée comme une « agression armée », alors il nous apparaît fort probable qu'une réponse similaire ne serait pas, elle-même, jugée comme une « agression armée ». Autrement dit, en raison du vide juridique en ce qui a trait aux cyberconflits, seule l'utilisation d'une réponse identique s'avère licite en regard du droit international.

En conclusion, nous avons donc établi un premier élément de réponse à notre interrogation initiale à savoir quelle devraient être l'action canadienne dans l'éventualité d'un cyberconflit. Nous sommes d'avis que le Canada pourrait, juridiquement parlant, utiliser les moyens associés au cyberspace afin de répondre à une menace extérieure affectant des objectifs canadiens et, par extension, cette interprétation permet l'élaboration d'une politique canadienne définissant les règles d'engagement dans le cadre d'un cyberconflit.

Jean-Christophe Boucher est étudiant à la maîtrise à l'Institut québécois des hautes études internationales de l'Université Laval et chercheur pour la Chaire de recherche du Canada sur la sécurité internationale. **Hugo Loiseau** est candidat au doctorat au Département de science politique de l'Université Laval et chercheur pour le Centre d'études interaméricaines (CEI). Les deux auteurs travaillent également à l'Institut québécois des hautes études internationales (IQHEI). Ils tiennent à remercier M. Dany Deschênes et le Lieutenant-colonel Richard Garon pour leurs précieux renseignements.

« Cyberattaque avortée », *Le Devoir*, jeudi 24 octobre 2002, p.B5.

Les statistiques produites par le Carnegie Mellon Software Engineering Institute

(www.cert.org/stats/cert_stats.html) démontrent bien la progression du nombre de cyberattaques depuis 1998.

Le dernier plan d'action du gouvernement américain sur la cybersécurité, intitulé *The National Strategy to Secure Cyberspace* a été décrié dès le lendemain de sa publication par plusieurs intervenants de différents milieux. Lire : <http://news.com.com/2100-1023-956353.html?tag=bplst> et

[1023-958545.html?tag=fg_lede](http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf) . Le plan d'action est disponible : <http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf> .

Le rapport du Service canadien du renseignement de sécurité circonscrit très bien la problématique concernant les cyberconflits. Voir Service canadien du renseignement de sécurité. « Opérations d'information », *Perspectives*, Rapport n 2001/11, 6 mai 2002, www.csis-scrs.gc.ca/fra/misdocs/200111_f.html .

Lire à titre d'exemple : GOMPERT, David C. «National Security in the Information Age», *Naval War College Review*, vol. 51, n°4, automne 1998, pp. 22-41.

Plusieurs auteurs n'hésitent pas à brandir la menace d'un Pearl Harbor électronique face aux nombreuses failles de sécurité dans le cyberspace.

BUNKER, Robert J. « Higher-dimensional warfighting », *Military Review*, Vol. 79, N.5, sept/oct 1999, pp.53-62.

GANSLER, Jacques S. « Protecting Cyberspace » dans BINNENDIJK, Hans (dir.), *Transforming America's Military*, Washington DC, National Defense University Press, 2002, pp.331-344.

WAUTELET, Michel. *Les cyberconflits, Internet, autoroutes de l'information et cyberspace : quelles menaces?*, Bruxelles, Éditions GRIP, 1998, p. 45-46.

GANSLER, Jacques S., *op cit.*, p.335.

WAUTELET, Michel, *op cit.*, p. 48.

Ibid., p. 53.

LIBICKI, Martin C. «What Is Information Warfare?» dans GONGORA, Thierry et RIEKHOFF, Harald von (dir.). *Toward a Revolution in Military Affairs? Defense and Security at the Dawn of the Twenty-First Century*, Westport, Greenwood Press, 2000, pp. 37-60.

Department of Defense, Joint Pub. 3-13, *Joint Doctrine for Information Operations*, 9 octobre 1998, GL-7.

Service canadien du renseignement de sécurité, *loc cit.*

CLEMMONS, Byard, Q. et BROWN, Gary D., « Cyberwarfare : Ways, warriors and weapons of mass destruction », *Military Review*, Vol. 79, n.5, sept/oct 1999, pp.35-45.

WAUTELET, Michel. *op cit.*, p. 85.

GANSLER, Jacques S., *op cit.*, p.332.

WAUTELET, Michel. *op cit.*, p. 71.

RATTRAY, Greg, *Strategic Warfare in Cyberspace*, Cambridge Mass., The MIT Press, 2001, p.1.

LA CARTE, Donald A. «La guerre asymétrique et l'utilisation des forces spéciales dans l'application des lois en Amérique du nord», *Revue militaire canadienne*, vol. 2, n°4, hiver 2001-2002, p. 25.

Idem.

GANSLER, Jacques S., *op cit.*, p.331.

WAUTELET, Michel. *op cit.*, pp. 87-88.

HENRY, R. et PEARTREE C.E. «Military theory and information warfare», *Parameters: Journal of the US Army War College*, vol. 38, n°3, automne 1998, pp. 121-125.

BUNKER, Robert J. *op cit.*, pp.53-62.

Idem.

GODELUCK, Solveig, *La géopolitique d'Internet*, Paris, Éditions La Découverte, 2002, pp.7-11.

GANSLER, Jacques S., *op cit.*, p.335.

GODELUCK, Solveig, *op cit.*, p.223-231.

Selon James Adams : « quelques 30 000 sites web publient des outils de piratage. » dans « Virtual Defense », *Foreign Affairs*, Vol. 80, No. 30, may/juin 2001, p.101. En outre, selon le *National Institute of Standards and Technology*, les pirates placent de 30 à 40 nouveaux outils sur leurs sites web chaque mois.