

## **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)

et

**Hugo Loiseau<sup>1</sup>**

(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<sup>e</sup> siècle. Cette toile a considérablement modifié le quotidien des individus dans les 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 actuelle. Comment, en effet, l'État peut-il et doit-il agir dans ce nouveau contexte ? Si l'on se base sur les règles d'engagement qui régissent les conflits conventionnels, la tâche qui s'impose s'avère double. Ce texte, d'une part, présente une revue des diverses formes de cyberconflits que l'on retrouve dans la littérature, ainsi que ce qui les distingue des problèmes de sécurité plus traditionnels ; d'autre part, il analyse les ramifications légales et éthiques qui peuvent s'appliquer à ce problème de sécurité en émergence. Nous tenterons ainsi de construire une assise théorique à l'aide de laquelle le Canada pourra orienter sa politique de sécurité en la matière et 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.

Sur le plan militaire, les 10 dernières années ont été riches en changements profonds : il suffit par exemple de penser à la révolution dans les affaires militaires (RAM), aux opérations de maintien de la paix de troisième génération ou encore à l'émergence du concept de sécurité humaine. Tout cela est le reflet des nombreuses transformations survenues dans l'espace international au cours de cette période. La réalité change, les théories doivent rendre compte de ces évolutions et les expliquer.

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 cyberespace. Les gouvernements et les législateurs prennent davantage conscience de cet important problème souterrain qui est plus difficilement discernable que les 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. La nécessité de se questionner et de réfléchir sur les cyberconflicts est d'autant plus criante que, actuellement, la menace semble sous-évaluée. Pourtant, celle-ci est belle et bien présente. D'ailleurs, la cyberattaque rapportée le 24 octobre 2002, une des dernières à ce jour, a été considérée comme majeure par les spécialistes<sup>2</sup>. En fait, le vide juridique qui existe présentement en ce qui concerne le cyberespace laisse une incroyable marge de manœuvre aux cyberpirates<sup>3</sup>. Ce texte se penchera sur la réponse que devront donner les gouvernements et les forces armées, en termes de règles d'engagement, face à une éventuelle attaque informatique en provenance du cyberespace.

Dans un premier temps, nous tenterons de fournir un aperçu général de la littérature sur les cyberconflicts 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'établir une politique canadienne en cette matière.

## Revue de littérature

Quiconque veut faire une revue de la littérature portant sur les cyberconflits et sur le cyberspace fait face à deux difficultés. D'une part, la littérature sur le sujet devient rapidement obsolète devant les progrès rapides 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 décalés par rapport à la réalité<sup>4</sup>. D'autre part, à cette difficulté s'ajoute la nouveauté du sujet et le caractère multiforme des cyberconflits. Ceux-ci touchent à la fois la protection des infrastructures civiles et militaires, la protection des renseignements, la diffusion à grande échelle de savoirs normalement secrets (fabrication de bombes, techniques de piratage informatique, secrets d'État...), la sécurité économique, la sécurité publique et, surtout, la sécurité nationale<sup>5</sup>. De surcroît, les cyberconflits font l'objet de recherches mal définies et, surtout, mal expliquées : elles mêlent guerre de l'information, cyberspace, nouvelles technologies des communications, cyberterrorisme, etc., dans un ensemble confus. Pour toutes ces raisons, traiter des dilemmes de sécurité associés au cyberspace nécessite inévitablement de faire des choix qui laissent dans l'ombre des analyses intéressantes mais désuètes ou des études trop éloignées du cœur du problème.

Pour pallier ces deux difficultés, nous nous concentrerons ici sur les conséquences de la prise en compte du cyberspace par rapport à la sécurité nationale et aux politiques de défense. Nous tiendrons également compte du fait que la littérature sur les cyberconflits, même encore clairsemée, louvoie parmi plusieurs courants – positiviste<sup>6</sup>, alarmiste<sup>7</sup>, à la limite de la science-fiction<sup>8</sup> ou encore largement normatif et descriptif<sup>9</sup> –, dont l'importance varie.

Le premier constat qui peut être fait est que les cyberconflits et leur existence même sont directement liés à la technologie et aux progrès technologiques et informatiques. Comme l'affirme Michel Wautelet, les technologies de l'information ne sont pas réservées au domaine militaire mais sont universelles, puisque n'importe qui peut se les procurer. Cette facilité d'utilisation annonce une véritable prolifération des armes technologiques<sup>10</sup>. La distribution de la puissance dans l'espace international est remodelée par les nouvelles technologies de l'information (NTI), et le différentiel de puissance s'accroît ainsi entre les États puissants et les autres, en même temps qu'augmente la vulnérabilité des premiers. L'utilisation des NTI accroît la capacité d'États, de groupes ou d'individus ayant des intentions hostiles de passer à l'action. Gansler, corroborant ces propos, est 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<sup>11</sup> ». L'utilisation et le développement des NTI constituent donc les principales bases du déploiement des cyberconflits et des guerres électroniques.

Wautelet définit les cyberconflits comme étant l'utilisation « de toutes les ressources du cyberspace pour détruire des éléments essentiels de la société de l'adversaire<sup>12</sup> ». Il faut remarquer ici que l'auteur ne limite pas sa définition à des considérations de mesures ou de proportionnalité. Ainsi, une certaine confusion se dévoile entre les concepts de « cyberattaques » et de « cyberconflits ». En effet, à la lumière de la caractérisation sus-mentionnée, comment représenter la distinction importante entre les cyberattaques, qui se veulent être des événements singuliers, déliés d'un contexte interactionnel, et les cyberconflits qui, justement, exigent un échange de cyberattaques entre deux ou plusieurs antagonistes? Malheureusement, la lecture de Wautelet ne nous permet pas de fournir une explication satisfaisante à cette interrogation.<sup>13</sup>

Malgré cette difficulté conceptuelle majeure, il n'en demeure pas moins que la représentation de Wautelet a l'avantage de spécifier la finalité du conflit, soit « [...] détruire des éléments essentiels de la société de l'adversaire ». À notre avis, deux propositions émanent de cette spécification. D'abord, la précision de l'activité, soit «détruire », circonscrit les cyberconflits au-delà du simple espionnage informatique ou encore aux intrusions bénignes. Ensuite, cette « destruction » doit cibler les « éléments essentiels de la société ». Ainsi, un cyberconflit ne tient pas compte des attaques cybernétiques perpétrées contre des systèmes non-critiques, peu importe la nuisance qu'elles représentent pour nos ordinateurs personnels. Cependant, il apparaît clairement à la lumière de cette définition que les cyberconflits peuvent engendrer des problèmes économiques colossaux, causer des dommages matériels ou informatiques et, par conséquent, entraîner des pertes de vies humaines, plus particulièrement dans la population civile. La particularité des cyberconflits est que, en tant que tels, ils ne détruisent rien sur le plan physique ou matériel ; cependant, leurs conséquences entraînent des dommages importants, car les États industrialisés sont de plus en plus dépendants des réseaux informatiques pour ce qui est de la sécurité publique, de la sécurité économique et surtout de la sécurité nationale.

Wautelet fait une 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<sup>14</sup> » dans le but de sortir vainqueur d'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 nécessaires pour déployer ces réseaux. La guerre du Golfe, en tant que l'une des premières guerres électroniques, est sans doute l'exemple le plus cité dans la littérature. En somme, la guerre électronique et son déploiement (le débordement) dans le cyberspace n'est qu'un outil, utilisé dans un conflit traditionnel, pour neutraliser les moyens de défense et d'attaque de l'ennemi, et ainsi parvenir à la victoire.

Les cyberconflits sont des conflits qui se déroulent dans le cyberspace : il apparaît donc essentiel de définir ce nouveau lieu de combat. Martin Libicki, une sommité en ce qui concerne les questions entourant le cyberspace et la guerre de l'information, propose une typologie qui éclaire cette question. D'emblée, il affirme que la guerre de l'information, considérée comme une technique indépendante pour faire la guerre, est un concept assez faible. En réalité, cette notion prend tout son sens lorsqu'on distingue les sous-catégories qu'elle comporte, et qui sont beaucoup plus opérationnelles à la fois pour les chercheurs et les militaires. Ainsi, Libicki décrit sept types ou sous-types de guerre de l'information qui servent de base au reste de son analyse<sup>15</sup>. Le dernier de ces types concerne les cyberconflits et, selon sa perspective, c'est un type de conflit qui se situe encore entre la science-fiction et la réalité ; il juge ses occurrences fort improbables.

Toutefois, si la guerre dans le cyberspace est improbable, elle reste possible. Alors la question qu'on doit se poser est la suivante : comment se fait cette guerre ? Un document du Pentagone classe les cyberconflits dans la catégorie des opérations d'information (IO), qu'il définit ainsi : « action taken to affect adversary information and information systems while defending one's own information and information systems<sup>16</sup> ». 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 Service canadien du renseignement de sécurité (SCRS). Celui-ci considère les opérations d'information comme étant issues 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<sup>17</sup> ».

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 parler de « nonkinetic, offensive actions taken to achieve information superiority by affecting enemy information-

based process, information systems and computer-based networks<sup>18</sup> ». Cette définition limiterait la portée de la doctrine du Pentagone en situation de cyberattaques et de cyberconflits.<sup>19</sup> 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 termes de théorie et de stratégie militaire. De fait, aucun consensus définitionnel et doctrinal n'a été établi à partir duquel nous pourrions considérer la création d'un régime international en matière de cyberconflits.

Conséquemment, il nous apparaît nécessaire de nous 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 du cyberspace favorise l'augmentation constante du nombre de ses utilisateurs ; or, 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<sup>20</sup> ». C'est aussi un enjeu, puisque, au départ, le cyberspace s'est développé de manière anarchique et sans que les considérations de sécurité ne soient prises en compte<sup>21</sup>. Les gouvernements et les organisations internationales ont pris du retard en termes 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<sup>22</sup>. Enfin, il faut ajouter que le cyberspace est en quelque sorte un complément de la triade traditionnelle terre-air-mer de déploiement des conflits, qu'en même temps il englobe. Le contrôle de cet espace de combat devient donc primordial durant toutes les phases d'un conflit. Cette situation pousse donc les responsables politiques et militaires à se questionner sur l'impact du cyberspace sur la paix et la sécurité dans le monde.

Par ailleurs, le cyberspace est à la fois menaçant et menacé ; il est simultanément arme et cible<sup>23</sup>. 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<sup>24</sup>. En fait, les conflits dans le cyberspace 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. Cela est d'autant plus vrai que toutes les

possibilités du cyberspace n'ont pas encore été explorées ni définies, si bien qu'il est encore difficile de déterminer la différence entre un crime et une attaque dans le cyberspace<sup>25</sup>. De plus, le cyberspace est propice au développement et à la prolifération de nouveaux types d'armes – les bombes logiques, les virus informatiques, par exemple –, ainsi qu'à des tactiques plus traditionnelles telles que la manipulation de l'information ou la guerre psychologique. Tout en étant menaçant, le cyberspace est également menacé, car il comporte de nombreuses failles de sécurité à tous les niveaux. L'exemple le plus frappant est sans doute la vulnérabilité des infrastructures et des composantes logicielles qui le supportent et permettent son existence<sup>26</sup>.

Cela étant dit, une question demeure toujours à débattre : la menace qui vient du cyberspace est-elle réelle ? Deux écoles de pensée s'affrontent sur cette question. La première affirme que la menace est bel et bien réelle, que les attaques doublent tous les ans et que la vulnérabilité des infrastructures du cyberspace 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 cyberspace sont tellement grands que, de lui-même, le marché réglera les failles de sécurité, et que les institutions et les entreprises qui ne se protègent pas périront. En somme, selon ce point de vue, la menace qui vient du cyberspace 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, provoquant dans sa chute des conséquences incalculables<sup>27</sup>.

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 qui influencent les conflits ont un impact éphémère, et cela s'applique aux nouvelles possibilités qu'offrent les technologies de l'information sur le champ de bataille. De prime abord, ils affirment que les nouvelles technologies ont souvent été surestimées et ont conduit les états-majors et les théoriciens à commettre des erreurs, 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<sup>28</sup>.

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 soulignent 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 et 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 avec les 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 comportera une cinquième dimension, qu'il appelle le cyberspace. L'auteur dénonce le fait que seules les variables stratégiques, technologiques et militaires sont considérées dans la révolution des affaires militaires. Selon lui, des changements sociopolitiques fondamentaux vont transformer la nature de la guerre, et il appuie cette idée sur l'importance grandissante du cyberspace – due à la compression des limites physiques et temporelles des quatre dimensions traditionnelles – dans le déroulement des combats. 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 produit un effet de « spatial contraction [that] takes two military objects that are far away from one another and brings them closer<sup>29</sup> ». 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, Bunker 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<sup>30</sup>.

Toutefois, avant d'en arriver à des scénarios de science-fiction tels 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, les compétences juridiques des États se chevauchent et s'enchevêtrent dans l'espace virtuel qu'est le cyberspace, ce qui complique en la régulation. Autrement dit, 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<sup>31</sup> ; certains, tel Gansler, pensent que le cyberspace n'a tout simplement pas de frontière<sup>32</sup>. En fait, les véritables régulateurs du cyberspace sont les internautes et les marchands (les « technopouvoirs »). 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, en viennent à le réguler. En somme, nous sommes très loin de voir apparaître une organisation internationale chargée de réguler le réseau Internet<sup>33</sup>.

Cette brève revue de la littérature sur les cyberconflits et le cyberspace permet de conclure deux choses. Premièrement, 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. Les auteurs et les différents rapports gouvernementaux débattent simplement 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 nous 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. Deuxièmement, 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 termes de compétences 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 qui prévaudront ? 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 afin de 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 contre 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 pour répondre aux éventuels assauts cybernétiques. À l'évidence,

cette menace est croissante. D'une part, la faiblesse des réseaux informatiques canadiens augmente, du fait que le nombre de réseaux et d'utilisateurs se multiplie, que la dépendance des gouvernements, des institutions, des entreprises, des groupes et des individus à l'égard des communications informatisées et des technologies de l'information croît, et que l'interopérabilité des systèmes informatiques gouvernementaux et internationaux est de plus en plus grande. D'autre part – et cela accentue cette faiblesse –, la probabilité d'une attaque cybernétique augmente, en raison de la croissance trop rapide des technologies informatiques (tant sur le plan 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<sup>34</sup>. À la lumière de ces deux phénomènes, la question qui demeure est de 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 desquels le gouvernement canadien peut formuler sa politique en regard des cyberconflits. L'établissement de normes pratiques devrait servir plusieurs objectifs : éviter l'improvisation et les risques de provoquer une crise internationale, donner une cohérence et une stabilité à l'action canadienne et, finalement, permettre 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 le 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.

Nous ne considérons pas les RE, en tant qu'instrument de réflexion, comme étant la seule avenue possible pour élaborer des principes d'action lors de cyberconflits. Toutefois, les RE nous apparaissent comme un cadre approprié en vue de penser l'action canadienne en regard des problèmes cybernétiques. Or, selon les Ordres et règlement des Forces canadiennes, les règles d'engagement se définissent ainsi : « Les RE constituent la façon dont les commandants militaires contrôlent l'utilisation de la force par leurs subalternes. » Autrement dit, les règles d'engagement sont un ensemble de normes ou de principes d'action définis en vue de l'utilisation efficace et proportionnée de la force. Appliqués aux cyberconflits, les règles d'engagement seraient la détermination péremptoire d'un code de conduite servant à encadrer la réponse canadienne à une attaque cybernétique.

La première interrogation est donc la suivante : l'utilisation de mesures cybernétiques peut-elle être associée au concept de la force ? Manifestement, on pourrait associer la force, le terme étant pris dans un sens restreint, à des considérations d'ordre physique. Dans ce cas précis, il nous semblerait futile d'argumenter qu'une cyberattaque puisse se concevoir comme une application de la force. En

théorie, aucune force physique n'est appliquée lors de cyberattaques. Cependant, si l'on prend le terme dans un sens plus large, c'est-à-dire si la force est comprise comme une mesure ayant pour objectif essentiel d'imposer une volonté, l'utilisation du cyberspace<sup>35</sup> à des fins illicites et guerrières peut alors prendre la forme d'un moyen en vue d'une finalité. En regard à cette idée, une cyberattaque est l'application d'un moyen, en l'occurrence cybernétique, dans le but explicite de détruire ou contrôler les capacités cybernétiques d'autrui et ainsi imposer une supériorité cybernétique sur celui-ci. En dernière analyse, nous pouvons à juste titre reprendre la définition proposée par Clemmons et Brown, selon laquelle un cyberconflit met en jeu « nonkinetic, offensive actions taken to achieve information superiority by affecting enemy information-based process, information systems and computer-based network. »<sup>36</sup>

Cela 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 : au niveau national et au niveau international. Cela nous amène à réfléchir à deux scénarios envisageables influant nécessairement sur les actions du gouvernement. Dans le premier cas, si nous considérons une attaque cybernétique provenant d'une source intérieure (un citoyen canadien, une entreprise ou une organisation canadienne) et visant des cibles canadiennes, le scénario relève alors, à notre avis, du domaine interne de l'action canadienne, et, par conséquent, la question demeure dans une large mesure du domaine criminel. L'action du gouvernement canadien est encadrée par un ensemble de mesures législatives nationales à cet effet. En ce sens, le concept de RE n'est guère adéquat pour structurer un débat qui relève plutôt de la sphère juridique canadienne.

Par contre, dans le deuxième cas, si nous transposons notre réflexion au plan international – une cyberattaque perpétrée par une source étrangère et visant des objectifs canadiens – une attaque cybernétique d'une source étrangère constitue alors une action internationale et, donc, encadrée par un système juridique international auquel le Canada adhère. Effectivement, dans la mesure où nous acceptons qu'une cyberattaque représente une utilisation de la force, toute action étrangère ayant pour cible des infrastructures essentielles canadiennes<sup>37</sup> représente une menace extérieure pouvant justifier une « réponse » canadienne. 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 régi par le droit de la guerre enchâssé dans les diverses Conventions de Genève et leurs protocoles. Cependant, l'utilisation du

droit de la guerre à des fins cybernétiques soulève un écueil majeur que nous ne saurions minimiser. En effet, en vertu de la Convention de Genève, toutes actions contre des non combattants sont formellement prohibées. Conséquemment, l'utilisation des attaques cybernétiques en temps de guerre doit nécessairement tenir compte des effets insidieux que celles-ci peuvent avoir sur les populations civiles. Par exemple, une attaque cybernétique contre les systèmes financiers ou les infrastructures électriques d'un État, même en temps de guerre, soulèvent des interrogations importantes puisqu'elle affecterait indûment les non-combatants.

Comme le reconnaît d'ailleurs Richard A. Clarke, responsable américain du bureau pour la sécurité du cyberspace, la problématique de l'utilisation des armes cybernétiques en temps de conflit est analogue au dilemme de l'emploi des armes nucléaires quelques décennies précédentes.<sup>38</sup> En effet, la plupart des États ont maintenant la capacité informatique officielle et officieuse<sup>39</sup> de mener des offensives cybernétiques, mais les questions à savoir quand et comment utiliser ces compétences font défauts. Ainsi, nonobstant l'ensemble des mécanismes légaux entourant l'usage de la force en temps de guerre, il n'en demeure pas moins qu'une certaine adaptation des conventions internationales aux réalités des cyberconflits semble nécessaire du fait de l'ambiguïté de la nature exacte (militaire ou civile) des infrastructures informatiques des États.

En regard des 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 contre la paix, d'une rupture de la paix ou d'un acte d'agression et fait des recommandations ou décide quelles mesures seront prises conformément aux Articles 41 et 42 pour maintenir ou rétablir la paix et la sécurité internationales »<sup>40</sup>. Il faut remarquer ici le caractère suffisamment souple des critères que le Conseil de sécurité se donne pour établir une source de « menace » et, par extension, pour 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 considérer les attaques cybernétiques comme une « menace » à la paix. Ainsi, en vertu des articles 41 (en ce qui a trait aux mesures n'impliquant pas l'usage de la force) ou 42 (pour les mesures impliquant l'utilisation de la force), 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 définitive, la question demeurant est celle de l'utilisation des moyens cybernétiques en réponse à une attaque du même type dans le cas où il n'y a pas d'état de guerre ni 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. L'esprit de l'article 51 parle de lui-même : « Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies serait l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales [...] »<sup>41</sup>. Inexorablement, la problématique repose sur la question à savoir si une cyberattaque constitue ou non une agression armée au sens de l'article 51.

Or, dans la mesure où une cyberattaque est effectivement interprétée comme un acte d'agression en regard du droit international, la victime peut alors justifier une riposte (cybernétique ou conventionnelle) comme étant de l'ordre de la légitime défense. Certains États, notamment la Russie, ont déjà affirmé officiellement que toutes attaques cybernétiques contre ses infrastructures militaires seraient considérées comme un acte d'agression pouvant justifier l'emploi de la force conventionnelle.<sup>42</sup> Loin de vouloir argumenter en faveur de cette alternative qui semble, pour l'essentielle, ne pas correspondre au principe de proportionnalité comprise dans les Conventions de Genève sur le droit de la guerre, il est évident qu'une cyberréponse de la même nature que la cyberattaque concorde à l'esprit des dispositions de l'article 51 de la Charte des Nations Unies. Dans l'éventualité où une attaque cybernétique n'est **pas** interprétée comme une agression armée pouvant justifier l'usage de la force; il nous apparaît fort probable qu'une réponse utilisant les mêmes moyens cybernétiques ne serait pas jugée comme une « agression armée ». Effectivement, si la communauté internationale, en fonction du droit international, ne reconnaissait pas les cyberattaques comme étant des « agressions armées » au sens de l'article 51, alors comment qualifier la même cyberattaque (à titre de cyberréponse) comme une « agression armée »?

Naturellement comme il en va de tout nouveau développement en droit international, beaucoup dépend de la façon dont les États et les institutions internationales agissent et réagissent devant les diverses situations particulières. Donc, en raison du vide juridique du droit international en ce qui a trait aux cyberconflits, ainsi que la relative ambivalence des politiques extérieures de plusieurs pays en la matière<sup>43</sup>, la détermination de la politique canadienne dans l'éventualité d'une cyberattaque doit suivre la voie de la prudence. Suivant ceci, et à la lumière des considérations explicitées précédemment, nous sommes d'avis que le Canada pourrait, juridiquement parlant, utiliser les moyens associés au cyberspace afin de répondre à une menace extérieure visant des objectifs canadiens et, par conséquent, rendre claire sa politique face aux cyberconflits afin d'éliminer toutes ambiguïtés sur sa

volonté à protéger ses infrastructures critiques des influences extérieures. Malheureusement, à notre connaissance, le Canada n'a pas explicité publiquement des règles d'engagement dans l'éventualité des cyberconflits. Ce faisant, l'action canadienne en ce qui a trait aux cyberattaques demeure, pour l'essentielle, dans un état d'ajustement conjecturé. Manifestement, une telle attitude pourrait se révéler dommageables pour le Canada dans la mesure où elle porte le flanc à l'improvisation et, donc, au péril d'engendrer indûment une crise internationale. Des règles d'engagement claires et précises de la part des autorités canadiennes pourraient prévenir une telle possibilité.

Malgré le caractère foncièrement critique de notre propos sur la politique canadienne à ce sujet, il faut reconnaître la justesse de certaines mesures prises par le gouvernement canadien depuis quelques années. Notamment, le 5 février 2001, le gouvernement Chrétien fonda le Bureau de protection des infrastructures essentielles et de la protection civile (BPIEPC), sous tutelle du Ministère de la Défense nationale, ayant la responsabilité « [...] d'améliorer la sûreté et la sécurité de l'environnement matériel et cybernétique des Canadiennes et de Canadiens. »<sup>44</sup> Pour ce faire, le BPIEPC propose de favoriser un partenariat avec tous les secteurs associés, de proche ou de loin, aux infrastructures essentielles, soit les autres ministères et instances bureaucratiques, le secteur privé, les provinces, les territoires, les municipalités et les acteurs internationaux. De surcroît, il collabore également avec ses différents partenaires gouvernementaux en matière de sécurité dans le cadre des objectifs proposés par le document de la collectivité canadienne de la sécurité et du renseignement<sup>45</sup>

Toutefois, cette obsession à la collaboration tout azimut laisse le BPIEPC tributaire de la bonne volonté de ses multiples partenaires. Par exemple, le BPIEPC veut « favoriser » le dialogue entre les entreprises privées et instances publiques pour la cybersécurité. Vœux pieux s'il en est un puisqu'il y a une dichotomie flagrante entre le désir d'assurer le maximum de sécurité possible et la nécessité de protéger la confidentialité de l'information des sociétés privées.<sup>46</sup> En outre, le BPIEPC n'est pas la seule organisation à laquelle échoie la responsabilité de la sécurité des infrastructures cybernétiques du Canada. Au BPIEPC doivent s'ajouter la Gendarmerie Royale du Canada, le Service canadien du renseignement de sécurité, divers organismes du Ministère de la Défense nationale, dont les Forces armées canadiennes et le Centre de la sécurité des télécommunications, etc... Inexorablement, cette variété dans la sécurité cybernétique au pays fait du BPIEPC une seule voie parmi la chorale, ce qui entrave sa capacité à réellement promouvoir la sécurité cybernétique des infrastructures essentielles canadiennes et gêne la possibilité de formuler des règles d'engagement cohérentes.

En définitive, la relative absence d'une compréhension **politique** des cyberconflits est l'élément qui nous apparaît le plus inquiétant de la situation canadienne.<sup>47</sup> Effectivement, les présents efforts afin de protéger ses infrastructures essentielles mettent l'accent sur l'amélioration des capacités « techniques » des systèmes informatiques. À notre avis, cette initiative doit être accompagnée d'un dialogue normatif sur les différentes alternatives politiques disponibles. Seule une volonté politique ferme et cohérente, jumelée à une expertise technique, peut préparer le Canada aux multiples défis et dangers posés par les cyberconflits. De plus, corollaire à cette recommandation, il serait souhaitable pour le Canada d'encourager et de participer activement à tout dialogue international cherchant à normaliser les actions étatiques dans le cyberspace.

48

- 
1. **Jean-Christophe Boucher** est étudiant à la maîtrise à l'Institut québécois des hautes études internationales (IQHEI) 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'IQHEI. Ils tiennent à remercier l'Institut de la Conférence des Associations de la Défense et, plus personnellement, M. Alain Pellerin et M. Kyle Christensen qui offrent aux étudiants gradués une occasion inestimable de faire valoir leurs idées. En outre, les auteurs ont bénéficié des conseils, critiques et commentaires de nombreuses personnes, dont M. Dany Deschênes, le Major Richard Garon et le réviseur anonyme. Finalement, les auteurs désirent remercier leurs mentors respectifs, M. Jean-Sébastien Rioux et M. Gordon Mace, pour leurs encouragements et confiance.
  2. « Cyberattaque avortée », *Le Devoir*, jeudi 24 octobre 2002, p. B5.
  3. Les statistiques produites par le Carnegie Mellon Software Engineering Institute ([www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)) démontrent bien la progression du nombre de cyberattaques depuis 1998.
  4. 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>. Le plan d'action est disponible à l'adresse suivante : <http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>, page consulté le 29 juin 2003.
  5. Le rapport du Service canadien du renseignement de sécurité circonscrit très bien la problématique des 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](http://www.csis-scrs.gc.ca/fra/misdocs/200111_f.html), page consulté le 28 octobre 2002.
  6. Lire, à titre d'exemple : GOMPERT, David C. « National Security in the Information Age », *Naval War College Review*, vol. 51, n° 4, automne 1998, p. 22-41.
  7. Plusieurs auteurs n'hésitent pas à brandir la menace d'un Pearl Harbor électronique face aux nombreuses failles de la sécurité dans le cyberspace.
  8. BUNKER, Robert J. « Higher-dimensional warfighting », *Military Review*, vol. 79, n° 5, sept./oct. 1999, p. 53-62.
  9. GANSLER, Jacques S. « Protecting Cyberspace », dans BINNENDIJK, Hans (dir.). *Transforming America's Military*, Washington DC, National Defense University Press, 2002, p. 331-344.
  10. WAUTELET, Michel. *Les cyberconflits, Internet, autoroutes de l'information et cyberspace : quelles menaces ?*, Bruxelles, Éditions GRIP, 1998, p. 45-46.
  11. GANSLER, Jacques S. *Op cit.*, p. 335.
  12. WAUTELET, Michel. *Op cit.*, p. 48.
  13. Nous aimerions remercier le réviseur anonyme pour avoir soulevé cette ambiguïté chez Wautelet.
  14. *Ibid.*, p. 53.
  15. 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, p. 37-60.
  16. Department of Defense, Joint Pub. 3-13, *Joint Doctrine for Information Operations*, 9 octobre 1998, GL-7.

- 
17. Service canadien du renseignement de sécurité, *loc cit.*
  18. CLEMMONS, Byard, Q. et BROWN, Gary D. « Cyberwarfare: Ways, warriors and weapons of mass destruction », *Military Review*, vol. 79, n° 5, sept./oct. 1999, p. 35-45.
  19. La distinction entre les deux termes est celle de mesure. Effectivement, par « cyberconflit », nous entendons une activité réciproque entre deux ou plusieurs antagonistes constituée de « cyberattaques ». Conséquemment, une « cyberattaque » est un acte isolé d'un contexte conflictuel et d'interactions entre plusieurs acteurs.
  20. WAUTELET, Michel. *Op cit.*, p. 85.
  21. GANSLER, Jacques S. *Op cit.*, p. 332.
  22. WAUTELET, Michel. *Op cit.*, p. 71.
  23. RATTRAY, Greg. *Strategic Warfare in Cyberspace* Cambridge, Mass., The MIT Press, 2001, p. 1.
  24. 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.
  25. *Idem.*
  26. GANSLER, Jacques S. *Op cit.*, p. 331.
  27. WAUTELET, Michel. *Op cit.*, p. 87-88.
  28. 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, p. 121-125.
  29. BUNKER, Robert J. *Op cit.*, p. 53-62.
  30. *Idem.*
  31. GODELUCK, Solveig, *La géopolitique d'Internet*, Paris, Éditions La Découverte, 2002, p. 7-11.
  32. GANSLER, Jacques S. *Op cit.*, p. 335.
  33. GODELUCK, Solveig. *Op cit.*, p. 223-231.
  34. Selon James Adams, « quelques 30 000 sites Web publient des outils de piratage ». « Virtual Defense », *Foreign Affairs*, vol. 80, n° 30, mai/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.
  35. Pour exécuter une cyberattaque ou une cyberréponse (contre-attaque cybernétique).
  36. CLEMMONS et BROWN, *Op cit.*, p. 35-45.
  37. « Les infrastructures essentielles se composent des installations matérielles et des technologies de l'information, des réseaux et des biens matériels dont la perturbation ou la destruction aurait de sérieuses conséquences pour la santé, la sécurité ou le bien-être économique des Canadiennes et des Canadiens ou pour le fonctionnement efficace des gouvernements du Canada. » [http://www.ocipep.gc.ca/whoweare/partner\\_f.asp](http://www.ocipep.gc.ca/whoweare/partner_f.asp).
  38. « White House Officials Debating Rules for Cyberwarfare », *Washington Post*, <http://www.washingtonpost.com/wp-dyn/articles/A46967-2002Aug21.html>, page consulté le 24 février 2003.
  39. La capacité cybernétique officielle d'un État peut se définir comme la compétence institutionnalisée d'un gouvernement en matière informatique. Plusieurs pays, notamment les États-Unis, la Chine, la Russie, la Grande-Bretagne, la Corée du Nord et la France, disposent d'unités gouvernementales ayant les compétences explicites en matière de cyberconflit. L'expression « capacité officieuse » renvoi plutôt à l'ensemble des organisations n'étant pas officiellement reconnu par l'État en question mais dont les compétences sont disponibles pour celui-ci. Par exemple, les unités subversives gouvernementales, certains groupes paramilitaires, organisations non-gouvernementales, entreprises privées, individus, etc...
  40. ORGANISATION DES NATIONS UNIES, *Charte des Nations Unies*, <http://www.un.org/french/aboutun/charte/>, page consulté le 2 juillet 2003.
  41. *Idem.*
  42. UNITED STATES CONGRESSIONAL RESEARCH SERVICE, *Cyberwarfare*, Order code RL30735, 19 juin 2001.
  43. Voir, pour de plus amples informations, WENGER, Andreas, Jan METZGER et Myriam DUNN (dir.), *An Inventory of Protection Policies in Eight Countries. Critical Information Infrastructure Protection*, International CIIP Handbook, Swiss Federal Institute of Technology Zurich, 2002.
  44. GOUVERNEMENT DU CANADA, Bureau de la protection des infrastructures essentielles et de la protection civile, [http://www.ocipep.gc.ca/whoweare/mission\\_f.asp](http://www.ocipep.gc.ca/whoweare/mission_f.asp), consulté le 31 juillet 2003.
  45. GOUVERNEMENT DU CANADA, Bureau du Conseil privé, *La collectivité canadienne de la sécurité et du renseignement*, [http://www.pco-bcp.gc.ca/docs/publications/si/si\\_f.pdf](http://www.pco-bcp.gc.ca/docs/publications/si/si_f.pdf) consulté le 3 mai 2003.

---

46. Problème majeur auquel est confronté nos homologues américains, voir Robert LEMOS et Declan MCCULLAGH, « Cybersecurity Plan Lacks Muscle », *Tech News – CENT.com*, [http://www.news.com.com/2100-10230-958545.html?tag=fd\\_lede](http://www.news.com.com/2100-10230-958545.html?tag=fd_lede), page consulté le 19 septembre 2002.

47. Dans une moindre mesure, le même constat pourrait être fait pour nos voisins du Sud même s'ils ont publié récemment leur *National Strategy to Secure Cyberspace* document disponible : [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)

48