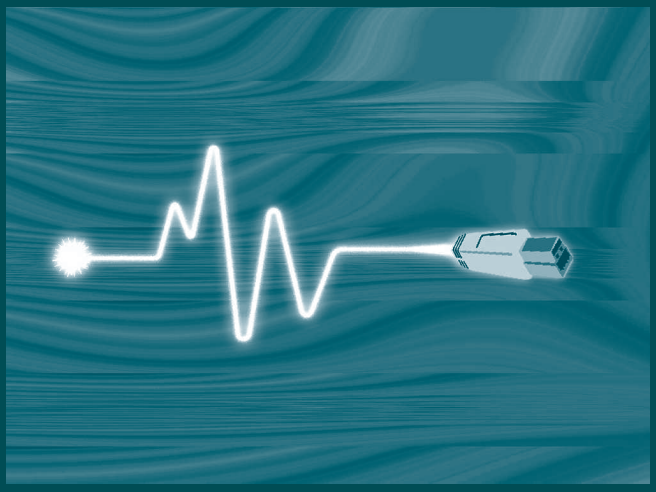
Institut des Nations Unies
pour la recherche
sur le désarmement
UNIDIR

forum du désarmement

quatre • 2011



Faire face aux cyberconflits

L'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) est un institut autonome au sein des Nations Unies financé par des contributions volontaires.

Grâce à ses projets de recherche, à ses publications, à ses conférences et à différents réseaux d'experts, l'UNIDIR favorise l'émergence d'une logique et d'un dialogue nouveaux autour des problèmes actuels et futurs de sécurité.

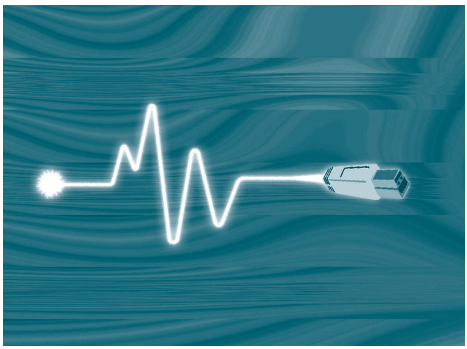
Le *Forum du désarmement* bénéficie de contributions des Gouvernements de la Fédération de Russie, de la Finlande, de la France, de la Hongrie, de l'Indonésie, de l'Irlande, d'Israël, du Luxembourg, de la Malaisie, du Mexique, de la Norvège, du Pakistan, de la Suisse et de la Turquie.

UNIDIR – des idées pour la paix et la sécurité www.unidir.org

Graphiste (couverture), Diego Oyarzún Reyes

forum du désarmement

quatre • 2011



Faire face aux cyberconflits

Rédactrice en chef
Kerstin Vignard

Traductrice (français)
Valérie Compagnion

Éditeurs (anglais)
Ross McRae
Jason Powers

Palais des Nations
CH-1211, Genève 10, Suisse
Tél. : +41 (0)22 917 31 86
Fax : +41 (0)22 917 01 76
disarmamentforum@unog.ch
www.unidir.org

Institut des Nations Unies
pour la recherche
sur le désarmement
UNIDIR

Printed at United Nations, Geneva
GE.12-00703—May 2012—4,270
UNIDIR/2012/1
ISSN 1020-7287

Imprimé sur papier recyclé

Table des matières

Note de la rédactrice en chef

Kerstin Vignard

La hantise du cyberconflit captive désormais l'attention et enflamme l'imagination dans le monde entier : du plus haut niveau des gouvernements aux scénaristes de Hollywood et de Bollywood, en passant par les couvertures de nombreux magazines. Malgré le battage médiatique que suscitent les scénarios apocalyptiques, la possibilité d'utiliser de nouvelles technologies à des fins défensives mais aussi offensives n'est pas inédite. Le cyberconflit n'est rien d'autre qu'un conflit mené avec les « armes » les plus récentes dont disposent les hommes. Toute la difficulté vient de ce que le cyberconflit exploite, dans de nombreux cas, des technologies à double usage facilement disponibles, comme les réseaux informatiques et Internet. Cette situation est aggravée par la progression exponentielle du nombre d'acteurs potentiels (gouvernements, pirates informatiques, terroristes, secteur privés, criminels, ou personnes impliquées à leur insu).

Les progrès technologiques devancent généralement les discussions sur les questions juridiques, les définitions ou les aspects éthiques ; les progrès des cybertechnologies ne font pas exception. La communauté internationale entame maintenant des discussions pour parvenir à une convergence de vues. Ce numéro du *Forum du désarmement* entend apporter des éléments de réflexion à ces débats d'une importance cruciale.

Notre prochain numéro s'intéressera à la Conférence d'examen de la Convention sur l'interdiction des armes chimiques qui aura lieu en 2013 et étudiera certaines difficultés, nouvelles ou non, auquel se heurte le régime d'interdiction des armes chimiques. Vu la rapidité des progrès scientifiques et technologiques, ce régime doit faire preuve de promptitude et de pragmatisme et être tourné sur l'avenir. Les États parties au régime de l'interdiction des armes chimiques sont-ils prêts à lever les ambiguïtés qui demeurent dans le traité, comme celles concernant les agents incapacitants ? Les États-Unis, la Fédération de Russie et la Libye ont déclaré qu'ils ne sont pas en mesure de respecter l'échéance d'avril 2012 pour la destruction des armes chimiques qu'ils ont déclarées. Quelles seront les conséquences de ces déclarations ? La vérification des opérations de destruction de ces armes devant se réduire considérablement au cours des prochaines années, quels seront les rôles et fonctions clefs de l'Organisation pour l'interdiction des armes chimiques ? Quelles seront les conséquences de cette évolution sur sa structure ? Enfin et surtout, comment rattacher le nouvel accent mis sur l'objectif d'empêcher la résurgence des armes chimiques à celui de renforcer la coopération et l'assistance internationales ? Comment inclure tout cela dans les mesures d'application nationales ?

La conférence annuelle de l'UNIDIR sur la sécurité spatiale a eu lieu les 29 et 30 mars 2012. Intitulée « Jeter les bases de progrès futurs », la conférence de 2012 visait à favoriser les discussions pour une meilleure compréhension des questions urgentes concernant la stabilité de l'espace. Pour plus d'informations sur cette conférence et celles organisées les années

précédentes et pour accéder aux rapports des conférences et aux enregistrements audio, veuillez consulter notre site web.

Plus de 50 chefs d'État et responsables d'organisations internationales se sont réunis récemment à Séoul (République de Corée) lors du Sommet sur la sécurité nucléaire. Dans la perspective de ce sommet, l'UNIDIR avait publié l'ouvrage intitulé *Global Nuclear Security: Building Greater Accountability and Cooperation*. Ce livre fait le point sur les différents accords internationaux, les programmes et les arrangements institutionnels qui constituent la base du régime international de sécurité nucléaire. Pour plus de détails sur cette publication, veuillez vous reporter à la section consacrée à l'*Actualité de l'UNIDIR* dans ce numéro du *Forum du désarmement* ou consultez notre site web.

L'année 2012 s'annonce comme une période de transition pour l'Institut. Après avoir occupé pendant quatre ans le poste de directeur adjoint de l'UNIDIR, Christiane Agboton-Johnson a quitté l'Institut à la fin du mois de février. Christiane a mis sa passion et son expérience au service de l'UNIDIR en influençant à la fois le programme de travail de l'Institut et ses processus internes. Avec ce numéro, nous tenons également à remercier Ross McRae, l'éditeur anglais du *Forum du désarmement*. Son enthousiasme et ses initiatives ont apporté une nouvelle dimension au travail de notre équipe. Valérie et moi-même leur souhaitons à tous les deux, au nom de tous nos collègues de l'UNIDIR, beaucoup de succès dans leurs prochaines activités.

Les cyber-opérations et le *jus in bello*

Nils Melzer

Le droit international humanitaire (DIH), également appelé « droit des conflits armés » ou *jus in bello*, s'applique uniquement aux situations de conflit armé et régit la conduite des hostilités par les belligérants ainsi que la protection et le traitement de ceux qui sont tombés au pouvoir de l'ennemi[1]. À ce jour, les principales sources du DIH sont les quatre Conventions de Genève de 1949 et leurs deux premiers protocoles additionnels de 1977 (Protocoles I et II), ainsi que le Règlement concernant les lois et coutumes de la guerre sur terre, révisé lors de la Conférence de La Haye de 1907, et une série de traités interdisant ou limitant l'emploi de certaines armes. En outre, au fil des décennies et des siècles, un DIH coutumier important s'est constitué ; il s'avère utile pour gérer les cas non réglementés par le droit des traités[2].

Les cyber-opérations en tant que guerres

Les notions de « cyberguerre », « cyber-hostilités » et « cyberconflit » n'ont pas été expressément définies en droit international. Il n'existe qu'une seule définition conventionnelle, établie par l'Organisation de coopération de Shanghai. Elle porte sur le concept plus large de guerre de l'information (*information war*) définie comme un affrontement entre deux États ou plus, visant à endommager les systèmes, processus et ressources informatiques et à porter atteinte aux systèmes politiques, économiques et sociaux, à endoctriner les foules pour déstabiliser la société et l'État, mais aussi à obliger l'État à prendre des décisions dans l'intérêt d'une partie adverse[3].

Comme l'a fait remarquer Michael Schmitt, l'expression « guerre de l'information » est souvent utilisée de manière abusive ; la guerre de l'information concerne uniquement les opérations informatiques menées en période de conflit armé et exclut toutes celles menées en temps de paix[4].

Si l'on applique ce principe au domaine des cyber-opérations, les termes « cyberguerre », « cyber-hostilités » et « cyberconflit » devraient être réservés aux conflits armés au sens du DIH. Les menaces que le cyberespace fait peser sur la sécurité et qui ne constituent pas un conflit armé peuvent être considérées comme de la « cybercriminalité », des « cyber-opérations », de la « cybersurveillance » ou, le cas échéant, du « cyberterrorisme » ou du « cyberpiratage », mais

---

Nils Melzer est directeur de recherche au Centre de compétence pour les droits humains de l'Université de Zurich. Il a été, auparavant, conseiller juridique pour le Comité international de la Croix-Rouge (CICR) et participe actuellement, en tant qu'expert, à la rédaction d'un manuel sur le droit international applicable aux cyberconflits, une initiative soutenue par le Centre d'excellence pour la cyberdéfense en coopération, de l'Organisation du Traité de l'Atlantique Nord (OTAN). Les vues exprimées dans cet article sont celles de l'auteur et ne reflètent pas nécessairement celles de l'Université de Zurich, du CICR, de l'OTAN ou de l'Organisation des Nations Unies. La version originale de cet article est le texte anglais.

ne devraient en aucun cas être évoquées avec des termes pouvant susciter des interrogations ou des doutes sur l'applicabilité du droit des conflits armés.

Les cyber-opérations dans les conflits actuels

De nos jours, il semble ne faire aucun doute que le DIH s'applique aux cyber-opérations menées dans le cadre d'un conflit armé en cours, qu'il soit international ou non international[5]. Les cyber-opérations n'existaient pas lorsque furent rédigés et adoptés la plupart des instruments contemporains de DIH. Il semble toutefois être communément admis que cela ne doit pas empêcher aujourd'hui de les appliquer à ce genre d'opérations. L'une des règles fondamentales du DIH est la suivante : « Les belligérants n'ont pas un droit illimité quant au choix des moyens de nuire à l'ennemi »[6], et l'article 36 du Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I) exige expressément que :

> Dans l'étude, la mise au point, l'acquisition ou l'adoption d'une nouvelle arme, de nouveaux moyens ou d'une nouvelle méthode de guerre, une Haute Partie contractante à l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par les dispositions du présent Protocole ou par toute autre règle du droit international applicable à cette Haute Partie contractante.

Le DIH prévoit l'application de ses règles et principes aux nouveaux moyens et méthodes de guerre. L'assujettissement d'un moyen ou d'une méthode aux règles et principes du DIH ne dépend pas de sa nature mais du contexte de son utilisation. La question de savoir si une cyber-opération doit être considérée comme intervenant dans un conflit armé ne dépend pas forcément d'un aspect territorial mais nécessite plutôt de savoir si cette opération est en rapport avec un conflit armé ou, selon la formule du Tribunal pénal international pour l'ex-Yougoslavie, si elle a un lien avec un conflit armé en cours[7]. Cela signifie aussi que les cyber-opérations menées pour des raisons n'ayant pas de rapport avec un conflit armé (absence de lien) peuvent être considérées, par exemple, comme de la cybercriminalité ou de la cybersurveillance, mais ne relèvent pas du DIH – même si elles sont réalisées par une partie belligérante ou sur un territoire touché par un conflit armé.

Des cyber-opérations peuvent-elles déclencher un conflit armé ?

L'une des questions les plus difficiles est de savoir si des cyber-opérations peuvent provoquer, et dans quelles circonstances, un conflit armé et entraîner l'applicabilité du DIH sans avoir déclenché d'hostilités classiques. Il ne faut pas confondre cette question et celle consistant à savoir si des cyber-opérations peuvent être considérées comme une menace, un emploi de la force ou une agression armée au sens de la Charte des Nations Unies. Le Comité international

de la Croix-Rouge (CICR) résume ainsi l'avis juridique prédominant sur la définition du conflit armé au sens du DIH :

1. Il y a **conflit armé international** chaque fois qu'il y a *recours à la force armée entre deux ou plusieurs États*.
2. Un **conflit armé non international** est un *affrontement armé prolongé* qui oppose les forces armées gouvernementales aux forces d'un ou de plusieurs groupes armés, ou de tels groupes armés entre eux, et qui se produit sur le territoire d'un État [partie aux Conventions de Genève]. Cet affrontement armé doit atteindre un *niveau minimal d'intensité* et les parties impliquées dans le conflit doivent faire preuve d'un *minimum d'organisation*[8].

Les situations peuvent évoluer : un conflit armé non international peut se transformer en conflit international et inversement. Pour le CICR : « Du point de vue juridique, il n'existe aucun autre type de conflit armé »[9]. Par conséquent, les cyber-opérations peuvent déclencher l'application du DIH si elles comportent tous les éléments constitutifs d'un conflit armé international ou non international.

S'agissant des conflits armés internationaux, les cyber-opérations doivent équivaloir au « recours à la force armée entre deux ou plusieurs États ». La question de savoir si la force armée intervient « entre » États dépend généralement de l'imputabilité telle que définie par les règles du droit international général en matière de responsabilité des États. En conséquence, l'applicabilité du DIH ne se limite pas aux actes commis par les membres des forces armées d'un État, mais s'étend aux actes de toute personne agissant en tant qu'agent de l'État, que ce soit *de jure* ou *de facto*, au nom d'une partie belligérante. Bien qu'il n'y ait aucune raison de modifier l'application du droit de la responsabilité des États pour le cyberespace, il peut être extrêmement difficile d'identifier l'origine ou l'auteur d'une cyber-opération.

Vient ensuite la question de savoir si des cyber-opérations peuvent être considérées comme une force armée (ou un affrontement armé en cas de conflit armé non international) déclenchant l'applicabilité du DIH bien qu'aucune force cinétique ne soit employée. Jusqu'à présent, un consensus semble se dégager autour de cette idée, au moins pour les cyber-opérations entraînant les mêmes effets que la force cinétique, autrement dit celles provoquant des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens[10]. Cela dit, tout recours à la force ne signifie pas nécessairement l'existence d'un conflit armé et tout acte de guerre n'implique pas un recours à la force. En réalité, les conflits armés peuvent être déclenchés par des déclarations de guerre officielles. L'existence d'un conflit armé international n'est pas nécessairement liée au recours à la force entre États mais, en l'absence d'une déclaration officielle de guerre, à l'existence d'hostilités belligérantes au sens du DIH. En conséquence, des cyber-opérations organisées par des États peuvent déclencher un conflit armé international si elles sont conçues dans l'intention de nuire à un autre État en provoquant des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens, ou en nuisant directement aux opérations militaires ou à la capacité militaire de cet État.

Les conflits armés non internationaux sont différents : ils impliquent au moins un belligérant non étatique faisant preuve d'un minimum d'organisation et les hostilités ou affrontements armés atteignent un niveau minimal d'intensité. Il doit s'agir d'une action collective organisée ; les cyber-opérations menées par des hackers isolés ne peuvent donc pas être comprises dans la notion de conflit armé. D'un point de vue purement théorique, il n'est pas exclu qu'un petit groupe organisé de hackers menant des cyber-opérations très destructrices contre le réseau militaire d'un État déclenche un conflit armé non international. Cela dit, tant que ces opérations proviennent d'un territoire sous le contrôle de l'État attaqué et tant qu'elles ne sont pas assorties d'une menace ou de l'emploi d'une force militaire classique susceptible d'empêcher l'État d'exercer son autorité sur les agresseurs, de telles opérations seraient certainement considérées comme des activités à caractère criminel devant être réglées par des mesures de maintien de l'ordre. De telles opérations sont plus facilement considérées comme des « hostilités » susceptibles de déclencher un conflit armé non international lorsqu'elles se produisent à plusieurs reprises et proviennent d'un territoire sur lequel l'État attaqué ne peut assurer le respect de la loi et où les autorités locales ne sont pas disposées à intervenir ou sont incapables de le faire.

Il est probablement encore trop tôt pour se prononcer de manière catégorique sur le seuil précis à partir duquel des cyber-opérations déclenchent un conflit armé non international (cette question est d'ailleurs toujours en suspens concernant les conflits non internationaux menés avec des méthodes et moyens classiques). Comme le CICR l'a fait justement remarquer en 2004 lors de la Conférence de Stockholm, la question de savoir si un jour les attaques contre les réseaux informatiques pourront être considérées comme constituant des conflits armés dépendra probablement de la pratique future des États[11].

Quoi qu'il en soit, une fois que l'existence d'un conflit armé aura été établie, il faudra déterminer dans quelle mesure les règles et concepts classiques du DIH pourront s'appliquer aux cyber-opérations menées dans le cadre de ce conflit. Le présent article se concentre plus particulièrement sur ceux qui seront certainement les plus pertinents, à savoir les concepts d'« attaque », d'« hostilités » et de « participation directe », ainsi que sur les règles et principes régissant le choix des cibles et la bonne foi dans la conduite des hostilités.

Les cyber-opérations en tant qu'attaques

Le terme « attaque » est un terme technique important en DIH puisque nombre de ses règles fondamentales sur la conduite des hostilités sont exprimées en termes d'attaques. Par exemple : « Ni la population civile en tant que telle ni les personnes civiles ne doivent être l'objet d'attaques »[12] ; « [l]es biens de caractère civil ne doivent être l'objet [...] d'attaques »[13] ; « [l]es attaques sans discrimination sont interdites »[14] ; et « [l]es attaques doivent être strictement limitées aux objectifs militaires »[15]. Citons également les règles régissant les « [p]récautions dans l'attaque » et les « [p]récautions contre les effets des attaques »[16], celles protégeant contre des attaques les « unités sanitaires »[17], les personnes hors de combat[18], les

ouvrages et installations contenant des forces dangereuses[19], ainsi que les règles obligeant les combattants à se distinguer de la population civile lors d'une attaque ou d'une opération militaire préparatoire d'une attaque[20], et celles interdisant d'utiliser les drapeaux ou pavillons, symboles, insignes ou uniformes militaires des parties adverses pendant des attaques[21].

D'après le paragraphe 1 de l'article 49 du Protocole I, « L'expression "attaques" s'entend des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs ». Cette définition a suscité de nombreuses discussions pour savoir dans quelle mesure des cyber-opérations pouvaient, du fait qu'elles n'ont pas de caractère cinétique, être considérées comme des actes de violence et par conséquent comme des attaques au sens du DIH. Il est généralement admis que des actes de violence ne signifient pas forcément l'utilisation de la violence cinétique, qu'il peut suffire que les effets de ces actes soient semblables à ceux généralement associés à la violence cinétique, autrement dit qu'ils provoquent des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens (conception basée sur les effets). À strictement parler, cette conception n'étend pas la notion d'attaque au-delà des actes de violence ; elle reconnaît simplement que les cyber-opérations déclenchant des processus susceptibles de provoquer directement des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens sont non seulement équivalentes mais font partie intégrante des actes de violence au sens du paragraphe 1 de l'article 49[22].

Quant à savoir si la notion d'attaque doit inclure les cyber-opérations visant simplement à capturer ou neutraliser (autrement dit à gêner, entraver ou empêcher l'exercice correct de ses fonctions) et non pas à tuer, blesser ou détruire la cible, cette question n'est pas tranchée. Le principal argument avancé pour inclure dans la conception d'une attaque basée sur ses effets les cyber-opérations visant à neutraliser une cible est le fait que la définition des objectifs militaires au paragraphe 2 de l'article 52 du Protocole I englobe les objets dont « la capture ou la neutralisation » offrirait un avantage militaire précis et met ces deux possibilités sur le même plan qu'une « destruction totale ou partielle »[23]. Ceux qui s'opposent à l'extension de cette définition se fondent sur une interprétation plus littérale des attaques comme « actes de violence » ; ils estiment que, si ce n'est l'acte, au moins ses conséquences doivent être violentes pour que l'acte soit considéré comme une attaque[24]. Ils étaient cette thèse en soulignant que le principe de proportionnalité concerne les attaques « dont on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages » mais n'inclut pas la capture ou la neutralisation[25].

Si les deux positions ont des points valables, ni l'une ni l'autre ne semble proposer une interprétation totalement satisfaisante de la notion d'attaque s'agissant des cyber-opérations. D'une part, il ne serait pas vraiment convaincant d'exclure de la notion d'attaque la neutralisation non destructrice du système de défense aérienne ou de toute autre infrastructure militaire essentielle d'un État simplement au motif qu'elle ne provoque pas directement de pertes en vies humaines, de blessures aux personnes ou de dommages aux

biens. D'autre part, il serait peut-être exagéré d'étendre la notion d'attaque à toute attaque par déni de service lancée, par exemple, contre des services de vente en ligne, des agences de voyages ou des annuaires téléphoniques.

Même si le terme « attaque » est une notion clef du DIH, une analyse de la pertinence des règles de conduite des hostilités pour les cyber-opérations ne peut se borner à un examen de cette notion. Il suffit, par exemple, de penser que le principe de distinction n'est pas formulé en termes d'« attaques » mais en termes d'« opérations »[26]. De la même façon, le droit des traités protège la population civile contre les attaques directes mais également « contre les dangers résultant d'opérations militaires »[27] et précise que « [l]es opérations militaires doivent être conduites en veillant constamment à épargner la population civile, les personnes civiles et les biens de caractère civil »[28]. Il est, en outre, interdit pour les États parties au Protocole I de recourir à la perfidie non seulement lors d'opérations visant à tuer ou blesser un adversaire, mais aussi lors d'opérations visant à capturer un adversaire[29]. Le facteur le plus déterminant est le risque qu'encourent les personnes civiles de perdre cette protection « si elles participent directement aux hostilités »[30], une notion généralement considérée comme étant plus large que celle d'attaque[31]. Par conséquent, même si les attaques sont les opérations de combat les plus courantes, il serait inexact de supposer que les cyber-opérations ne constituant pas une attaque ne seraient pas assujetties au DIH régissant la conduite des hostilités. À strictement parler, la possibilité d'appliquer aux cyber-opérations les limites imposées par le DIH à la conduite des hostilités ne dépend pas de savoir si les opérations en question peuvent être qualifiées d'« attaques » (la principale forme de conduite des hostilités) mais de déterminer si elles constituent un élément des « hostilités » au sens du DIH.

Les cyber-opérations en tant qu'hostilités et la question de la participation directe à ces opérations

Pour le CICR, les hostilités sont le recours (collectif) par des parties à un conflit à des méthodes et moyens de blesser l'ennemi ; elles peuvent être décrites comme l'ensemble des actes hostiles réalisés par des personnes directement impliquées dans ces actes[32]. En DIH, la notion de participation directe aux hostilités, quand elle concerne le comportement de personnes civiles, entraîne la suspension de la protection qui leur était accordée contre des attaques directes[33]. Par conséquent, tant que des experts civils ou des hackers isolés mènent des cyber-opérations constituant une participation directe aux hostilités, ils sont non seulement tenus de se conformer au DIH régissant la conduite des hostilités, mais deviennent des objectifs militaires légitimes, comme s'ils étaient des combattants. En outre, lorsqu'il s'agit de prendre des précautions au moment de lancer une attaque pour éviter ou limiter autant que possible les « dommages collatéraux », les personnes civiles participant directement aux hostilités ne sont pas prises en compte.

Selon la position officielle du CICR, la notion de participation directe aux hostilités dépasse la notion d'attaque et englobe non seulement le fait de provoquer des pertes en vies humaines,

des blessures aux personnes ou des dommages aux biens, mais aussi tout acte susceptible de nuire aux opérations militaires ou à la capacité militaire d'une partie belligérante (*seuil de dommage*)[34]. De plus, une cyber-opération ne peut être considérée comme un élément des hostilités que si elle provoque directement le seuil de dommage requis (*causalité directe*) ; elle doit, en outre, avoir été conçue pour appuyer un belligérant, au détriment d'un autre (*lien de belligérance*). Le caractère direct ou indirect du lien de causalité entre une opération et les dommages qu'elle entraîne dépend de son action. Si l'opération renforce la capacité qu'a un belligérant de nuire à l'ennemi, la causalité est indirecte, et si elle fait partie intégrante d'une opération utilisant cette capacité pour nuire à l'ennemi, la causalité est directe. Lorsque des cyber-opérations imputables à une partie belligérante visent à nuire à l'adversaire en provoquant directement des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens ou en nuisant directement aux opérations militaires ou à la capacité militaire de l'adversaire, ces cyber-opérations doivent être considérées comme des « hostilités » et, par conséquent, être assujetties à toutes les limitations imposées par le DIH concernant le choix et l'utilisation des moyens et méthodes de guerre. Les personnes civiles qui mènent de telles opérations n'ont plus droit à la protection contre les attaques directes.

Quant aux cyber-opérations visant à dérégler ou neutraliser les systèmes radar, les systèmes d'armes ou les réseaux de communication ou de soutien logistique d'un adversaire, si elles ne provoquent pas directement de dégâts matériels, elles peuvent certainement être considérées comme un élément des hostilités et doivent, par conséquent, respecter les règles et principes du DIH régissant la conduite des hostilités[35]. Cette règle vaut également pour les cyber-opérations s'infiltrant dans les réseaux informatiques de l'adversaire pour effacer des données de ciblage, manipuler des ordres militaires, ou changer, coder, utiliser ou rendre inexploitables d'autres données sensibles et atteindre ainsi directement la capacité de la partie belligérante à mener des hostilités. Cela dit, des cyber-opérations ne provoquant pas de pertes en vies humaines, de blessures aux personnes, de dommages aux biens ni de préjudices sur le plan militaire – comme les activités de renseignement, celles visant des fins délictueuses ou d'autres activités n'ayant aucun rapport avec les hostilités – ne constituent pas des hostilités et, si elles sont menées par des civils, n'entraînent pas pour ces derniers une perte de leur protection contre les attaques directes.

La question la plus difficile à trancher est celle de savoir si la destruction implique nécessairement des dégâts matériels, surtout en l'absence de préjudices sur le plan militaire. Autrement dit, la neutralisation non destructrice d'un réseau informatique militaire constituerait clairement un préjudice sur le plan militaire et donc un acte d'hostilités, alors que la neutralisation non destructrice d'une centrale électrique utilisée exclusivement à des fins civiles ne provoquerait aucun préjudice sur le plan militaire, ni aucune perte en vie humaine, ni blessure à des personnes ni dommages – à moins que les dommages ne soient interprétés comme englobant des dommages autres que matériels. On se retrouve une fois de plus confronté au choix d'une interprétation susceptible d'être jugée soit trop restrictive soit trop permissive. Dans le premier cas de figure, les cyber-opérations neutralisant de puissants

réseaux civils d'électricité ou de communication ne pourraient être considérées comme un acte d'hostilités que si elles provoquaient des pertes en vies humaines, des blessures aux personnes ou des dommages aux biens ou des préjudices sur le plan militaire. Dans le deuxième cas de figure, tout préjudice causé à la population civile en raison du conflit, y compris de simples désagréments ou intimidations, devrait être considéré comme un élément des hostilités militaires. Cela signifierait que le DIH s'appliquerait à la conduite des hostilités mais entraînerait aussi pour tous les civils directement impliqués la perte de leur protection.

Les cibles dans le cyberespace

Le principe de distinction est au cœur du DIH ; il oblige les parties belligérantes à toujours faire la distinction entre les objectifs militaires légitimes et les personnes et biens protégés contre toute attaque, et à ne diriger leurs opérations que contre des objectifs militaires[36]. L'interdiction de lancer des attaques sans discrimination et l'obligation de respecter les principes de précaution et de proportionnalité découlent du principe de distinction et sont indispensables pour respecter ce dernier.

Les personnes

Les objectifs militaires légitimes comprennent les combattants, les membres de groupes armés organisés et les personnes civiles directement impliquées dans les hostilités. Les personnes civiles, le personnel médical et religieux et les combattants hors de combat – parce qu'ils sont blessés, malades, ont été faits prisonniers, se sont constitués prisonniers ou pour toute autre raison – doivent être épargnés et protégés. Même si l'identification de facteurs décisifs comme la participation directe aux hostilités et l'appartenance à des groupes armés ou forces armées constitués de manière irrégulière peut poser de grandes difficultés pratiques, la plupart de ces problèmes ne sont pas propres à la question des cyber-opérations et ont été examinés en détail ailleurs[37]. Il faut toutefois s'interroger sur la façon d'interpréter dans le cyberespace les facteurs déterminant des cibles potentielles, comme l'organisation d'un groupe ou le fait d'appartenir à un groupe, car dans le cyberespace les personnes peuvent agir collectivement sans appartenir à un groupe ni dépendre d'une hiérarchie de commandement. De plus, comment l'obligation qu'ont les combattants « de se distinguer de la population civile lorsqu'ils prennent part à une attaque ou à une opération militaire préparatoire d'une attaque »[38] s'applique-t-elle au cyberespace ? Les hackers devraient-ils porter des uniformes alors qu'ils se trouvent physiquement très loin du champ de bataille ou leurs opérations devraient-elles pouvoir être identifiées comme des opérations militaires par leur adversaire ? Quel lien faut-il établir entre cette obligation et la distinction qui doit être faite entre les ruses de guerre (autorisées) et la perfidie (interdite) sur le champ de bataille ? Il est évident que ces questions et d'autres doivent être précisées dès que possible ; les personnes civiles exposées à une cyberguerre doivent, en effet, pouvoir bénéficier de la protection à laquelle elles ont

droit en vertu du droit des traités et du droit coutumier. D'ici là, il devrait suffire de rappeler qu'en cas de doute, toute personne doit être considérée comme civile et doit, à ce titre, être protégée contre toute attaque directe[39].

Les objets

Aux termes du paragraphe 2 de l'article 52 du Protocole I :

> En ce qui concerne les biens, les objectifs militaires sont limités aux biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis.

Cette définition n'est pas facile à mettre en œuvre dans le cyberespace puisque dans ce domaine les infrastructures civiles sont étroitement connectées aux infrastructures militaires. Plus encore que dans le cadre de guerres dites classiques, la probabilité est grande que les objectifs militaires visés dans le cyberespace soient à double usage. Cette situation n'est pas forcément un obstacle insurmontable pour attaquer de tels objets, mais elle exige d'identifier avec une infinie précaution les objectifs légitimes et oblige l'agresseur comme l'agressé à utiliser des moyens très avancés pour évaluer, éviter et contrôler les dommages pouvant être infligés incidemment à la population et aux infrastructures civiles.

En raison de l'interdiction des attaques sans discrimination, la question se pose de savoir dans quelle mesure il est possible d'empêcher des logiciels malveillants destinés à endommager des systèmes militaires de se propager à des infrastructures civiles et de créer une grande confusion parmi la population civile[40]. Même si les dommages collatéraux peuvent être maîtrisés, l'on peut se demander dans quelle mesure il serait justifié, par exemple, de neutraliser un serveur de nom de domaine régulant le trafic Internet mondial ou de détruire un câble sous-marin intercontinental majeur pour éviter que ceux-ci ne soient utilisés pour lancer des cyber-opérations hostiles si plus de 90 % des données transmises sont des données civiles et si cela risque d'entraîner, au niveau mondial, de graves conséquences sur le commerce, les transports et les communications[41].

Une autre question clef est de savoir si des données constituent un bien au sens du DIH et, le cas échéant, à quel seuil de dommage, de modification, de manipulation ou d'interférence estimerait-on que l'interdiction d'attaquer des biens de caractère civil aurait été violée. Quasiment aucune cyber-opération – pas même l'espionnage par l'exploitation de réseaux informatiques ou des manipulations aussi simples que l'utilisation d'un mot de passe – ne peut être effectuée sans effacer ou modifier ne serait-ce que provisoirement des données dans les systèmes infiltrés. Les données devraient probablement être considérées comme un bien ne pouvant être pris directement pour cible à moins qu'elles ne remplissent tous les critères

définissant un objectif militaire[42]. La suppression ou la modification de données civiles au cours d'une opération visant un but différent est inévitable et doit être prise en compte, au même titre que la nature du dommage, pour évaluer la proportionnalité.

Il importe donc de bien distinguer le but réel de l'opération de ses effets secondaires. Par exemple, la suppression ou modification de données civiles lors d'une attaque contre une cyber-infrastructure militaire est équivalente aux dommages « collatéraux » provoqués par des opérations employant la force cinétique. Manipuler ou modifier les données d'accès à un système informatique civil lors d'une opération d'espionnage ou de reconnaissance, c'est un peu comme forcer la porte ou la boîte à lettres du logement d'une personne civile lors d'une perquisition. Cela ne constitue pas pour autant une « attaque » au sens de l'article 49 du Protocole I car la nature, les effets et le but de l'opération ne correspondent pas à ceux des « actes de violence »[43]. La suppression et la manipulation de données pour perturber la diffusion de programmes télévisés civils peuvent être considérées comme illicites par certains[44], mais jugées par d'autres comme des attaques directes contre des biens de caractère civil[45].

Les ruses et la perfidie dans le cyberespace

En raison de ses spécificités, le cyberespace est exposé à un grand nombre de possibilités et de techniques permettant de tromper l'ennemi avec de fausses informations. Des parties belligérantes peuvent dissimuler l'origine de leurs opérations en utilisant un réseau botnet ou en usurpant des adresses IP[46] ; elles peuvent intervenir électroniquement pour faire passer des véhicules ou des troupes de combat pour des transports médicaux, manipuler les données de reconnaissance de l'ennemi ou envoyer au quartier général de l'armée des e-mails apparemment inoffensifs mais infectés de logiciels malveillants.

Il importe de faire la distinction entre les ruses de guerre (autorisées) et la perfidie (interdite). L'article 37 du Protocole I définit les ruses de guerre comme « les actes qui ont pour but d'induire un adversaire en erreur ou de lui faire commettre des imprudences, mais qui n'enfreignent aucune règle du droit international applicable dans les conflits armés ». La perfidie est quant à elle interdite. Elle consiste à tuer, blesser ou capturer un adversaire en faisant appel, avec l'intention de la tromper, à sa bonne foi pour lui faire croire qu'il a le droit de recevoir ou l'obligation d'accorder la protection prévue par le droit international. Les actes suivants sont des exemples de perfidie :

a) feindre l'intention de négocier sous le couvert du pavillon parlementaire, ou feindre la reddition ;
b) feindre une incapacité due à des blessures ou à la maladie ;
c) feindre d'avoir le statut de civil ou de non-combattant ;
d) feindre d'avoir un statut protégé en utilisant des signes, emblèmes ou uniformes des Nations Unies, d'États neutres ou d'autres États non Parties au conflit[47].

Quant au DIH, il interdit la perfidie destinée à tuer, blesser ou capturer un adversaire. Les cyber-opérations visant à toucher une infrastructure par des dommages matériels ou fonctionnels ou à provoquer d'autres formes de perturbation ou de neutralisation ne sont pas concernées par cette interdiction, même si elles recourent à la perfidie.

Une autre interdiction est plus adaptée au cas des cyber-opérations : l'interdiction de faire un usage abusif, dans un conflit armé, d'emblèmes protecteurs reconnus sur le plan international (par exemple, le signe du Mouvement international de la Croix-Rouge et du Croissant Rouge, le pavillon parlementaire ou l'emblème protecteur des biens culturels), l'emblème des Nations Unies et les drapeaux ou pavillons, symboles, insignes ou uniformes militaires d'États neutres ou d'États n'étant pas parties au conflit. Il est également interdit d'utiliser les drapeaux ou pavillons, symboles, insignes ou uniformes militaires de l'adversaire pendant des attaques ou pour dissimuler, favoriser, protéger ou entraver des opérations militaires[48]. Cela revient clairement à mettre hors-la-loi toute cyber-opération hostile semblant émaner d'un État non belligérant, du CICR ou de l'Organisation des Nations Unies, ainsi que les attaques se faisant passer pour des opérations menées par des forces amies.

Le statut des cyberguerriers

Les combattants

Les cyber-opérations sont généralement menées par du personnel hautement spécialisé. Dans la mesure où ils sont membres des forces armées d'un État belligérant, leur statut, leurs droits et leurs obligations ne sont pas différents de ceux des combattants traditionnels. L'article 43 du Protocole I stipule que les forces armées « se composent de toutes les forces, tous les groupes et toutes les unités armés et organisés qui sont placés sous un commandement responsable de la conduite de ses subordonnés devant cette Partie ». Ce concept étendu et fonctionnel des « forces armées » englobe, en réalité, tous les acteurs armés d'un État belligérant et faisant preuve d'une organisation militaire suffisante.

Les sous-traitants privés et les employés civils

Les États belligérants ont de plus en plus souvent recours à des sous-traitants privés et à des employés civils pour réaliser un certain nombre de tâches habituellement effectuées par du personnel militaire y compris la préparation et la conduite des cyber-opérations et les activités d'appui nécessaires. Tant que ces personnes remplissent des fonctions ne constituant pas une participation directe aux hostilités, elles restent des civils et, si elles sont capturées alors qu'elles accompagnent officiellement des forces armées dans un conflit armé international, elles ont droit au statut de prisonnier de guerre en vertu de l'article 4 de la Convention de Genève relative au traitement des prisonniers de guerre. Cela dit, lorsque des sous-traitants privés ou des employés civils sont expressément autorisés par un État à participer directement aux hostilités, ils deviennent des acteurs armés organisés et, de fait, des membres irréguliers

de ses forces armées. Par conséquent, ils perdent leur statut de personnes civiles et peuvent prétendre aux avantages accordés aux combattants et au statut de prisonnier de guerre à condition de remplir les quatre conditions stipulées à l'article 4 :

a) avoir à leur tête une personne responsable pour ses subordonnés ;

b) avoir un signe distinctif fixe et reconnaissable à distance ;

c) porter ouvertement les armes ;

d) se conformer, dans leurs opérations, aux lois et coutumes de la guerre.

Levée en masse

L'expression *levée en masse* désigne les habitants d'un territoire non occupé qui, à l'approche de l'ennemi, prennent spontanément les armes pour combattre l'invasion sans avoir eu le temps de s'organiser en unités armées régulières, à condition qu'ils portent ouvertement leurs armes et respectent les lois et coutumes de la guerre. Ils sont les seuls acteurs armés à pouvoir prétendre non seulement au statut de prisonnier de guerre mais également aux avantages accordés aux combattants même si, par définition, ils agissent spontanément et ne bénéficient pas d'une organisation ni d'un commandement leur permettant d'être considérés comme des membres des forces armées. Si cette catégorie de personnes est de moins en moins pertinente dans le cadre des guerres classiques, elle pourrait bien avoir une importance pratique dans les cyberguerres. Le territoire n'étant ni envahi ni occupé, la période durant laquelle une *levée en masse* est possible augmente. Le cyberespace est également un environnement idéal pour lancer et coordonner de manière non hiérarchique des actions spontanées, collectives et non organisées de cyberdéfense avec la participation d'un grand nombre d'« hacktivistes ». Il faut, bien sûr, savoir comment interpréter dans le cadre du cyberespace la condition de porter ouvertement les armes. L'on pourrait estimer que cette condition est remplie si des acteurs lançant des cyber-opérations ne feignent pas d'avoir le statut de non-combattant ou un statut protégé au sens de l'article sur l'interdiction de la perfidie[49].

Les personnes civiles

En DIH, le concept de personne civile englobe toutes les personnes qui ne sont pas membres des forces armées d'un État ni membres de parties non étatiques à un conflit armé et qui ne participent pas à une *levée en masse*. En tant que personnes civiles, elles ont droit à la protection contre les dangers découlant des opérations militaires et, plus particulièrement, contre les attaques. Dans le cadre d'une cyberguerre, cette catégorie engloberait certainement la plupart des hackers non étatiques n'appartenant pas à la branche militaire d'un groupe armé organisé. Si leurs opérations constituent une participation directe aux hostilités, les civils perdent leur protection et peuvent être attaqués directement comme s'ils étaient des combattants. À la différence des combattants, ils ne bénéficient pas d'une immunité contre des poursuites judiciaires pour des actes licites de guerre (un avantage accordé aux combattants) et ceux

qui les ont capturés peuvent donc les sanctionner pour toute infraction de leur législation nationale. Toutes les personnes civiles privées de liberté – y compris celles ayant participé directement à des hostilités – doivent être traitées avec humanité et avoir droit à un procès équitable comme le prévoient différents instruments du DIH applicables[50].

Les membres des groupes armés organisés

Dans le cadre du DIH régissant les conflits armés non internationaux, les groupes armés organisés sont les forces armées (ou branche armée) d'un belligérant non étatique ; ils ne doivent pas être confondus avec les parties belligérantes (par exemple, des forces insurrectionnelles, y compris leur branche administrative ou politique) ni avec d'autres segments de la population civile qui leur apportent un soutien. Le DIH conventionnel régissant les conflits armés non internationaux utilise les termes « civils », « forces armées » et « groupes armés organisés » sans les définir. Il est généralement admis, toutefois, que les membres des forces armées des États ne sont pas des civils et l'esprit et la lettre des Protocoles I et II et ceux de l'article 3 commun aux Conventions de Genève laissent à penser qu'il en va de même pour les membres des groupes armés organisés.

Les civils peuvent soutenir une partie non étatique de différentes manières et peuvent même participer directement aux hostilités de manière spontanée, irrégulière et non organisée. Ils ne peuvent cependant être considérés comme membres d'un groupe armé organisé à moins qu'ils n'aient pour mission de participer directement aux hostilités pour le compte de la partie non étatique. Cette fonction de combat ne leur donne pas pour autant droit aux avantages accordés aux combattants, au statut de prisonnier de guerre ni à aucun autre type d'immunité contre des poursuites judiciaires nationales pour des actes licites de guerre. Elle fait une distinction purement pratique entre les membres de forces de combat organisées et la population civile. Des personnes menant des cyber-opérations pour le compte d'une partie non étatique perdent donc leur statut de civils et deviennent des membres des « forces armées » de cette partie si leurs opérations sont menées de façon continue et si elles constituent une participation directe aux hostilités[51].

Conclusion

En droit international, le phénomène des cyberguerres ne s'inscrit pas dans un vide juridique ; il relève de règles et principes bien établis. Il n'en reste pas moins que la transposition de ces règles et principes au nouveau domaine qu'est le cyberespace se heurte à certaines difficultés et soulève des questions importantes. Certaines peuvent être réglées par une interprétation classique des traités et du bon sens ; pour d'autres, il faut des décisions à l'unanimité des États de la communauté internationale. La cyberguerre n'a pas eu, à ce jour, de conséquences dramatiques sur le plan humain, espérons qu'il en sera toujours ainsi. Le risque de tragédie humaine reste néanmoins énorme et ira grandissant à mesure qu'augmentera, pour nos

activités quotidiennes, notre dépendance à l'égard des systèmes informatiques. Il est donc d'autant plus important que les États prennent conscience non seulement de l'obligation juridique qu'ils ont de déterminer si les nouvelles armes et méthodes employées dans les cyberguerres sont compatibles avec les obligations qui leur incombent en vertu du DIH, mais aussi de la responsabilité morale qu'ils ont envers les générations futures.

Notes

1. Cet article est extrait de N. Melzer, *Cyberwarfare and International Law*, UNIDIR, 2011. L'article original examine aussi, entre autres, le *jus ad bellum* et le droit de la neutralité.
2. Voir l'étude approfondie du DIH coutumier réalisée par le Comité international de la Croix-Rouge, J.-M. Henckaerts et L. Doswald-Beck, *Customary International Humanitarian Law*, volumes I et II, 2005.
3. Organisation de coopération de Shanghai, Annexe I à l'accord entre les gouvernements des États membres de l'Organisation de coopération de Shanghai sur la question de la coopération pour la sécurité internationale de l'information, 16 juin 2009, d'après une traduction non officielle.
4. M. Schmitt, « Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework », *Columbia Journal of Transnational Law*, vol. 37, 1999, p. 885 à 937.
5. Les personnes qui avaient participé en 2004 à une conférence d'experts à Stockholm avaient conclu que le DIH s'applique aux attaques contre les réseaux informatiques lors de conflits armés internationaux. Voir K. Byström (sous la direction de), *Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden*, 2005, p. 181. À l'heure où nous écrivons cet article, cette approche est celle retenue (à l'unanimité) pour le projet de manuel sur le droit international applicable à la cyberguerre (dit *Tallinn Manual*).
6. Voir l'article 22 de la Convention concernant les lois et coutumes de la guerre sur terre et son Annexe : Règlement concernant les lois et coutumes de la guerre sur terre. Une formule similaire figure à l'article 35 du Protocole I.
7. Conseil de sécurité, *Rapport du Secrétaire général établi conformément au paragraphe 2 de la résolution 808 (1993) du Conseil de sécurité*, document des Nations Unies S/25704, 3 mai 1993.
8. CICR, « Comment le terme "conflit armé" est-il défini en droit international humanitaire ? », *Prise de position*, 2008, p. 5.
9. Ibid., p. 1.
10. Voir M. Schmitt, « Cyber Operations and the Jus in Bello: Key Issues », *Naval War College International Law Studies*, vol. 87, 2011, p. 89 à 110 ; et K. Dörmann, « The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint », *in* K. Byström (sous la direction de), *Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden*, 2004, p. 139 à 153. À l'heure actuelle, cette approche est celle retenue pour le projet de manuel sur le droit international applicable à la cyberguerre.
11. K. Dörmann, « The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint », *in* K. Byström (sous la direction de), *Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden*, 2004, p. 142. Cette approche est également celle retenue pour le projet de manuel sur le droit international applicable à la cyberguerre.
12. Art. 51, par. 2, Protocole I.
13. Art. 52, par. 1, Protocole I.
14. Art. 51, par. 4, Protocole I.
15. Art. 52, par. 2, Protocole I.
16. Voir respectivement les articles 57 et 58 du Protocole I.

17. Art. 12, par. 1, Protocole I.
18. Art. 41, par. 1, Protocole I.
19. Art. 56, Protocole I.
20. Art. 44, par. 3, Protocole I.
21. Art. 39, par. 2, Protocole I.
22. Voir l'analyse de la participation directe aux hostilités dans le cadre d'opérations collectives et de mesures préparatoires *in* N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009, p. 56 et 57, et p. 68 à 71.
23. K. Dörmann, « The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint », *in* K. Byström (sous la direction de), *Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden*, 2004, p. 139 à 153.
24. M. Schmitt, « Wired Warfare: Computer Network Attack and Jus in Bello », *International Review of the Red Cross*, vol. 84, n° 846, 2002, p. 365 à 399.
25. Art. 51, par. 5, al. *b*, Protocole I.
26. Art. 48, Protocole I.
27. Art. 51, par. 1 et 3, Protocole I. Art. 13, par. 1 et 3, Protocole II.
28. Art. 57, par. 1, Protocole I.
29. Art. 37, Protocole I.
30. Art. 51, par. 3, Protocole I. Art. 13, par. 3, Protocole II.
31. N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009, p. 49 à 52.
32. Ibid., p. 43 et 44.
33. Art. 51, par. 3, Protocole I. Art. 13, par. 3, Protocole II.
34. Pour plus d'informations, voir N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009.
35. À la fin d'une réunion d'experts organisée par le CICR, il fut convenu que les cyber-opérations qui causent directement à l'adversaire des préjudices sur le plan militaire lors d'un conflit armé constituent une participation directe aux hostilités. Voir CICR, *Third Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report*, 2005, p. 14.
36. Art. 48, Protocole I.
37. Pour une étude plus détaillée, voir N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009. Pour des critiques et la réponse du CICR, voir R. Goodman et D. Jinks, « The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law: An Introduction to the Forum », *Journal of International Law and Politics*, vol. 42, n° 3, 2010, p. 637 à 640.
38. Art. 44, par. 3, Protocole I.
39. Art. 50, par. 1, Protocole I. Voir aussi la discussion plus large sur la présomption de la protection accordée aux civils *in* N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009, p. 77 à 79.
40. Aux termes du paragraphe 4 de l'article 51 du Protocole I, les attaques sans discrimination sont : « a) des attaques qui ne sont pas dirigées contre un objectif militaire déterminé ; b) des attaques dans lesquelles on utilise des méthodes ou moyens de combat qui ne peuvent pas être dirigés contre un objectif militaire déterminé ; ou c) des attaques dans lesquelles on utilise des méthodes ou moyens de combat dont les effets ne peuvent pas être limités comme le prescrit le présent Protocole ; et qui sont, en conséquence, dans chacun de ces cas, propres à frapper indistinctement des objectifs militaires et des personnes civiles ou des biens de caractère civil ».

41. La définition des attaques sans discrimination inclut également à l'alinéa *b* du paragraphe 5 de l'article 51 du Protocole I, les attaques « dont on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages, qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu ».
42. Cette idée est réfutée *in* M. Schmitt, « Cyber Operations and the Jus in Bello: Key Issues », *Naval War College International Law Studies*, vol. 87, 2011, p. 8.
43. Art. 49, par. 1, Protocole I. Ces opérations et les destructions qu'elles engendrent peuvent néanmoins constituer un fait internationalement illicite.
44. M. Schmitt, « Cyber Operations and the Jus in Bello: Key Issues », *Naval War College International Law Studies*, vol. 87, 2011, p. 89 à 110 ; et M. Schmitt, « Wired Warfare: Computer Network Attack and *Jus in Bello* », *International Review of the Red Cross*, vol. 84, n° 846, 2002, p. 365 à 399.
45. K. Dörmann, « The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint », *in* K. Byström (sous la direction de), *Proceedings of the Conference: International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm, Sweden*, 2004, p. 139 à 153.
46. Un « botnet » est constitué d'ordinateurs mis en réseau à distance pour lancer des opérations à des fins malveillantes. Chaque ordinateur de ce réseau est victime d'un logiciel de contrôle à distance qui répond à un serveur. L'usurpation d'adresse IP (*IP spoofing*) consiste à envoyer des paquets IP en utilisant une adresse source autre que la sienne de façon à masquer l'identité de celui qui émet ou d'usurper l'identité d'un autre système.
47. Extrait du paragraphe 1 de l'article 37, Protocole I.
48. Art. 38 et 39, Protocole I.
49. Art. 37, par. 1, Protocole I.
50. Dans les conflits armés internationaux, les personnes civiles privées de leur liberté sont protégées par la Convention de Genève relative à la protection des personnes civiles en temps de guerre, le Protocole I aux Conventions de Genève de 1949 et le droit coutumier. S'agissant des conflits armés non internationaux, ces protections figurent à l'article 3 commun aux Conventions de Genève, le Protocole II et le droit coutumier. Selon le contexte, les instruments relatifs aux droits de l'homme pourraient également s'appliquer.
51. Pour la position du CICR sur cette question, voir N. Melzer, *Guide interprétatif sur la notion de participation directe aux hostilités en droit international humanitaire*, CICR, 2009.

Incompatibilité entre les priorités offensives et défensives des États pour les cyber-activités

Brian Weeden

Lorsque des stratèges militaires étudient le meilleur moyen d'attaquer un adversaire, ils tentent généralement de trouver les vulnérabilités (ou failles) des systèmes de l'adversaire. Dans les guerres classiques, cette opération signifie étudier les chars, les avions, les navires, les missiles ou tout autre matériel militaire de l'ennemi pour repérer leurs failles, par exemple, le rayon de braquage d'un avion de chasse. Des stratégies spéciales sont étudiées pour tirer profit de ces failles et, dans certains cas, des armes sont spécialement conçues pour leur être opposées. Il est rare de trouver dans ses propres systèmes les failles présentes dans les systèmes de ses adversaires car il est rare d'utiliser les mêmes systèmes que ses ennemis. Tenter de parer aux vulnérabilités de ses propres systèmes n'entrave généralement pas la possibilité d'exploiter celles de ses adversaires.

La situation est très différente dans le cas de la cyberguerre. L'intégralité du cyberdomaine repose sur du matériel utilisant les mêmes architectures informatiques et connecté par un système standard pour échanger des paquets de données. Les forces économiques et la facilité d'utilisation de certains produits ont, en outre, favorisé l'émergence de quasi-monocultures des logiciels et des systèmes d'exploitation. L'on retrouve ainsi les mêmes vulnérabilités au plus haut niveau des États et de nombreuses organisations. Les États se trouvent confrontés à un véritable dilemme politique s'ils veulent mettre au point ou utiliser des cyber-armes tout en améliorant leur propre cyberdéfense ; ces objectifs sont devenus de sérieuses préoccupations politiques.

Bugs, vulnérabilités et exploits informatiques

Pour bien comprendre ce dilemme, il convient d'expliquer d'abord comment sont conçues les cyber-armes. Les erreurs de programmation, communément appelées « bugs », sont inévitables dans la création de logiciels. Un bug est généralement défini comme la différence entre ce qu'un programmeur avait prévu qu'un bloc de code réaliserait et ce que le code exécute réellement. Cette différence peut se manifester de différentes façons, certaines étant extrêmement difficiles à détecter. Créer un logiciel sans que celui-ci comporte le moindre bug est une opération coûteuse et difficile voire quasi impossible pour les logiciels particulièrement complexes comme ceux développés par des centaines voire des milliers de programmeurs et comprenant des millions de lignes de code. Les bugs entraînent pour la plupart un simple plantage du programme, mais certains effectuent des actions qui ne sont pas autorisées, l'on parle alors de « vulnérabilités ». Le fait d'utiliser ces failles pour compromettre un ordinateur ou

---

Brian Weeden est un ancien officier de l'armée de l'air des États-Unis ; il connaît le domaine du contrôle spatial et les opérations nucléaires. Il prépare actuellement un doctorat en politique scientifique et technologique à l'Université George Washington.

pour accéder à certaines informations constitue un « exploit ». Il importe de souligner que les vulnérabilités peuvent également découler de failles au niveau de la conception d'un système, par exemple au niveau du choix d'une procédure plus rapide ou de l'utilisation incorrecte d'un algorithme de chiffrement.

Même si la cible finale d'une cyber-attaque peut être un système ou un appareil précis, celui-ci est presque certainement lié à un système plus général comme un ordinateur de bureau ou un serveur utilisant l'un des progiciels ou systèmes d'exploitation les plus courants. Bien souvent, ces ordinateurs hôtes sont connectés à d'autres ordinateurs par un réseau local. Tout comme pour la mise au point d'autres types d'armes, le processus de conception d'une cyber-arme commence par identifier la cible visée et par définir l'effet attendu de l'attaque. Le matériel et les logiciels des ordinateurs connectés à la cible sont étudiés pour repérer des failles éventuelles ; la mise au point d'un ou plusieurs exploits débute une fois que les vulnérabilités ont été identifiées. Une cyber-arme contient un logiciel et des routines qui utilisent des exploits pour attaquer et infiltrer chaque niveau du système, du point d'entrée jusqu'à la cible. Une fois que le système de la cible est atteint, un exploit spécial conçu pour effectuer des dommages précis dans ce système est déployé.

Par conséquent, découvrir de nouvelles failles dans les logiciels ou le matériel est une étape importante pour mettre au point des cyber-armes et concevoir des exploits pour les attaquer. De nombreux exploits ont recours à l'exécution de code à distance (qui permet à l'agresseur d'exécuter un code contre le système visé) ou à l'élévation de privilèges (qui permet à l'agresseur d'exécuter des commandes grâce à des privilèges plus élevés). Les plus convoités sont les exploits dits du « jour zéro » car ils ne sont connus que lorsqu'ils sont utilisés dans une cyber-attaque. Les armées, les agences de renseignement, les groupes de la criminalité organisée et les hackers cherchent en permanence des exploits qu'ils pourraient utiliser pour lancer des cyber-attaques. Pendant ce temps, les distributeurs de logiciels, les chercheurs en sécurité informatique et les hackers ayant de bonnes intentions (les *white hat hackers*) s'efforcent d'identifier les vulnérabilités existantes pour programmer les correctifs nécessaires afin d'améliorer la cyberdéfense.

Tous les logiciels peuvent comporter des failles, mais les hackers se concentrent souvent sur les applications les plus répandues car selon qu'ils aient des intentions malveillantes ou bienveillantes, ils veulent toucher ou protéger le plus grand nombre d'hôtes possible. Microsoft Windows est particulièrement visé puisqu'il représente 85 % du marché des systèmes d'exploitation[1]. De la même façon, Microsoft Office, qui est très répandu dans les systèmes des entreprises et des gouvernements, représente aussi une cible importante. Plus intéressantes encore sont les applications présentes sur toutes les plateformes, comme Java de Sun Microsystem ou Adobe Reader et Adobe Flash[2].

Étude de cas : Stuxnet

Le logiciel malveillant Stuxnet, utilisé pour attaquer une installation iranienne d'enrichissement nucléaire à Natanz, permet de comprendre la mise au point et le déploiement d'une cyber-arme ainsi que les choix qui s'imposent entre des activités offensives et défensives. Détecté pour la première fois en juin 2009 par des chercheurs en sécurité informatique, Stuxnet était un logiciel malveillant complexe dont plusieurs versions furent découvertes jusqu'au milieu de l'année 2010. Il exploitait des failles de Microsoft Windows[3]. Même si la définition de ce qu'est une cyber-arme est délicate, de nombreux experts en cybersécurité considèrent les attaques Stuxnet comme la première démonstration concrète de ce dont sont capables les cyber-armes[4].

Les centrifugeuses utilisées à Natanz pour enrichir de l'uranium étaient la véritable cible visée par Stuxnet. Pour atteindre les centrifugeuses, Stuxnet devait infecter des ordinateurs de contrôle industriel utilisés pour programmer et contrôler les automates programmables qui contrôlaient les convertisseurs de fréquence des centrifugeuses[5]. Stuxnet devait exploiter les vulnérabilités du système d'exploitation hôte avant d'infecter l'ensemble de la machine, exploiter les failles du logiciel d'application pour les automates programmables et celles de ces automates, et devait enfin commander les convertisseurs de fréquence de façon à endommager les centrifugeuses[6].

Les ordinateurs de contrôle industriel que Stuxnet devait infecter n'étaient pas directement connectés à Internet – leur protocole de sécurité utilisait des moyens physiques, électriques ou électromagnétiques pour les isoler d'autres systèmes et notamment d'Internet. Il fallait toutefois que les exploitants puissent mettre à jour les logiciels de ces ordinateurs et envoyer ou récupérer des données. Pour ce faire, ils utilisaient, comme c'est souvent le cas, des clefs USB. Stuxnet fut conçu pour tirer parti de cette habitude : il infectait les clefs USB, favorisant ainsi la propagation du ver entre ordinateurs d'un réseau local[7]. Stuxnet fut diffusé par trois vagues d'attaques lancées contre cinq organisations présentes en Iran[8]. En quelque temps, Stuxnet se propagea à plusieurs réseaux jusqu'au jour où il atteignit les ordinateurs de contrôle industriel où la charge s'exécuta.

Tous les ordinateurs infectés par Stuxnet utilisaient Microsoft Windows ; le logiciel malveillant profita de quatre exploits du « jour zéro » dans Windows pour infiltrer les cibles visées. La première version de Stuxnet, découverte en juin 2009, profitait d'une vulnérabilité d'exécution de code à distance du spouleur d'impression Windows[9]. Microsoft ne publia un correctif qu'en septembre 2010 pour cette faille qui avait été révélée en avril 2009 par le magazine de sécurité informatique *Hakin9*[10]. Une nouvelle version de Stuxnet, découverte en mars 2010, exploitait une faille d'exécution de code à distance dans la façon dont Windows gère un raccourci ou lie des fichiers[11]. Microsoft publia un avis de sécurité sur cette vulnérabilité en juillet 2010 et un correctif le mois suivant[12]. Après avoir analysé Stuxnet, la société de sécurité informatique

Symantec révéla en privé à Microsoft deux autres vulnérabilités pouvant entraîner une élévation de privilèges[13].

Les concepteurs de Stuxnet avaient soit découvert ces vulnérabilités de Windows et d'autres parties du système alors qu'ils mettaient au point leur logiciel soit avaient eu à leur disposition une liste d'exploits inconnus du public dans laquelle ils avaient puisé. Dans l'un ou l'autre cas, ces vulnérabilités avaient été gardées secrètes et n'avaient pas été communiquées à Microsoft. Plusieurs millions d'ordinateurs utilisés par des gouvernements, des sociétés et des particuliers à travers le monde étaient ainsi exposés aux mêmes exploits. Lorsque Stuxnet fut déployé puis découvert, le code de ces exploits devint public.

Les concepteurs de Stuxnet prirent de nombreuses mesures pour limiter sa diffusion. Contrairement à d'autres logiciels malveillants, Stuxnet n'était pas un ver ; il n'était pas conçu pour se propager aussi rapidement que possible par le biais d'Internet. Stuxnet ne se diffusait que par des clefs USB et au sein d'un réseau local et chaque élément infecté ne pouvait en infecter que trois autres[14]. Stuxnet comporte du code indiquant qu'il se « détruira » le 24 juin 2012 ; la question de savoir si ce code fonctionnera ou s'il déclenchera autre chose fait débat parmi les experts de sécurité[15].

Malgré ces contraintes, en septembre 2010, Stuxnet avait infecté plus de 100 000 hôtes dans 155 pays[16]. Les infections, qui touchaient principalement l'Iran, représentaient aussi un nombre important en Inde et en Indonésie. Deux facteurs expliquent cette propagation : l'absence de correctifs pour les vulnérabilités de Windows et une façon d'utiliser les clefs USB qui était peu sûre et largement répandue. En octobre 2010, Siemens confirma que 15 de ses clients industriels à travers le monde – et notamment des usines chimiques, des centrales électriques et des installations de production – avaient été « touchés » par Stuxnet[17]. L'on ignore si ces clients, qui utilisaient des automates programmables Siemens pour contrôler différents systèmes, ont subi des dommages à cause de Stuxnet.

Pour être précis, bien que Stuxnet ait infecté tous ces systèmes, rien ne prouve qu'il ait endommagé des systèmes ailleurs qu'en Iran. Les analyses du code de Stuxnet effectuées par la communauté de la sécurité de l'information ont conclu que la charge de Stuxnet avait été programmée pour s'exécuter uniquement contre les ordinateurs de contrôle industriel utilisés pour les centrifugeuses iraniennes à Natanz. Il fallait que la machine Windows visée utilise le logiciel Step 7 pour contrôler des automates programmables fabriqués par Siemens Corporation. Ces derniers devaient être le modèle Siemens 6ES7-315-2 contrôlant au moins 33 convertisseurs de fréquence fabriqués par Fararo Paya (à Téhéran) ou par Vacon (en Finlande) pour des fréquences comprises entre 807 et 1 210 Hz[18].

Une fois que Stuxnet a commencé à se propager, tous ceux qui avaient les moyens nécessaires ont tenté d'en comprendre le fonctionnement. Comme il fallut des mois voire des années pour corriger les vulnérabilités exploitées par Stuxnet, la criminalité organisée et d'autres hackers eurent largement le temps d'en profiter. À la fin du mois de juillet 2011, Microsoft signala un

pic du nombre de tentatives d'infections par un exploit utilisé par Stuxnet[19]. Des tentatives eurent lieu dans le monde entier mais furent particulièrement nombreuses au Brésil et aux États-Unis qui n'avaient jusqu'alors pas été trop exposés aux infections par Stuxnet. Un autre logiciel malveillant, appelé Duqu, circule aujourd'hui. Comme il comporte des ressemblances frappantes avec Stuxnet, certains chercheurs en sécurité informatique pensent qu'il a été mis au point par les mêmes concepteurs ou qu'il réutilise des éléments clefs de Stuxnet[20].

Les choix des États pour leurs cyber-activités

Comme le montre le cas Stuxnet, les gouvernements qui cherchent à la fois à renforcer leur cyberdéfense et à mettre au point des cyber-armes et des techniques offensives pour les utiliser contre leurs adversaires sont confrontés au dilemme que posent les spécificités du cyberdomaine. Le duel qui oppose les activités offensives et défensives de cybersécurité entraîne des conséquences au-delà du domaine militaire car les logiciels et le matériel sont également répandus dans les applications commerciales et civiles. Les exploits découverts lors de la mise au point de cyber-armes par une armée ou des services de renseignement sont susceptibles d'être utilisés contre les systèmes de ces derniers ou contre ceux de sociétés commerciales ou de particuliers. Toute décision revient donc à favoriser l'aspect offensif ou défensif des cyber-activités. Les sections suivantes étudient certaines questions qui se posent dans l'un et l'autre cas.

Une stratégie offensive

Dans le cadre d'une stratégie offensive, la politique de confidentialité des failles (découvertes dans du matériel, des logiciels ou des systèmes) permet d'élaborer des exploits puis de mettre au point des cybercapacités offensives sans que d'autres États ou cybercriminels ne puissent se les procurer. C'est le choix classique des gouvernements engagés dans des campagnes militaires offensives dans quelque domaine que ce soit. Cette stratégie fonctionne parfaitement dans les domaines classiques de la guerre, mais dans le cas des cyber-activités, il ne faut pas imaginer que les gouvernements sont les seuls acteurs impliqués. Cette hypothèse est valable pour les opérations terrestres, maritimes et aériennes mais erronée pour les cyber-opérations.

L'une des difficultés qui se pose dans le cas de la cyberdéfense est l'ampleur de la « surface d'attaque » devant être défendue. Les vulnérabilités ne se trouvent pas uniquement dans les systèmes d'exploitation et les ordinateurs de bureau ou portables. Elles existent dans de nombreux endroits. Pratiquement tout ce qui utilise des logiciels peut comporter des vulnérabilités, en particulier les catégories de logiciels n'ayant jamais été prises pour cible. Ce fut le cas des automates programmables et c'est le cas aujourd'hui des systèmes d'exploitation des téléphones portables. Il a été signalé que certains chercheurs réussissent à trouver des vulnérabilités à chaque fois qu'ils en cherchent[21]. Après Stuxnet, une attention accrue a été

portée aux automates programmables et à d'autres instruments utilisés pour le contrôle industriel. Un chercheur en sécurité informatique a découvert plusieurs vulnérabilités critiques des systèmes de contrôle industriel qu'il comptait révéler lors d'une conférence sur la cybersécurité. Ces failles étaient tellement graves que le Département de la sécurité du territoire des États-Unis et Siemens le convainquirent de renoncer à s'exprimer[22]. Avec la multiplication des instruments intelligents, le nombre potentiel de vulnérabilités augmente de plus en plus vite. Par exemple, lors de la 2011 Black Hat Conference (l'une des plus importantes réunions de hackers), des chercheurs ont fait la démonstration d'une technique permettant de déverrouiller et démarrer une voiture à l'aide de SMS[23].

Les cyber-opérations offensives seront certainement confidentielles : elles seront planifiées et exécutées de façon à dissimuler l'identité de celui ou ceux qui les soutiennent ou de façon à ce que ceux-ci puissent nier les avoir soutenues. Cela signifie souvent qu'au sein d'un même gouvernement tous les organismes ne seront pas informés de ces opérations ce qui augmente le risque que ses systèmes soient exposés à l'utilisation de ces exploits telle que décrite ci-après.

L'armée des États-Unis utilise des dizaines de réseaux informatiques pour des raisons de logistique, d'organisation et de sécurité. Les membres des forces armées doivent souvent accéder à de multiples réseaux ou transférer des données entre différents réseaux pour accomplir leur mission, une tâche qui n'est généralement pas simple car les systèmes sont isolés les uns des autres pour des questions de sécurité. L'utilisation de supports de stockage amovibles pour transférer des données entre réseaux et aussi, dans de nombreux cas, pour contourner les protocoles et dispositifs de sécurité, est une nécessité opérationnelle.

L'armée des États-Unis a interdit depuis novembre 2008 l'utilisation de supports amovibles sur le réseau NIPRNet (données non classifiées) et sur le réseau SIPRNet (données confidentielles). Cette interdiction faisait suite à une infection de grande ampleur de ces réseaux par le logiciel malveillant nommé Agent.btz à partir d'une clef USB ramassée sur le parking d'une base au Moyen-Orient[24]. Ce ver s'était propagé dans diverses versions de Microsoft Windows. En février 2010, après une opération massive de nettoyage appelée « Buckshot Yankee », l'armée des États-Unis restaura la possibilité d'utiliser des supports de stockage amovibles dans des situations précises[25]. Peu après, Bradley Manning aurait utilisé dans une installation sûre en Iraq des CD inscriptibles pour récupérer 150 000 câbles diplomatiques. Ceux-ci seraient ultérieurement révélés au monde entier par Wikileaks. En décembre 2010, l'armée des États-Unis interdit à nouveau les supports de stockage amovibles.

Bien qu'il n'existe aucun lien connu entre les logiciels malveillants Stuxnet et Agent.btz, il existe des similitudes frappantes dans les attaques. De nombreuses hypothèses ont été formulées et de nombreuses preuves indirectes laissent à penser que les États-Unis pourraient être à l'origine ou complice de la conception de Stuxnet[26] ; il fut certainement mis au point à l'époque où le logiciel Agent.btz infectait les réseaux de l'armée des États-Unis. Si l'implication d'éléments

du Gouvernement américain dans la mise au point de Stuxnet venait à être confirmée, il semblerait qu'il n'y ait eu, entre les entités développant ce logiciel à des fins offensives et celles chargées de défendre les réseaux militaires américains, aucune discussion concernant l'extrême vulnérabilité des machines utilisant Microsoft Windows face à l'utilisation de supports de stockage amovibles ni aucun échange sur la capacité pour les logiciels malveillants d'utiliser des supports amovibles afin de contourner l'isolement des systèmes. Une telle absence de communication et de coordination entre les organismes du Gouvernement américain ne serait pas sans rappeler les failles des services de renseignement avant les attentats du 11 septembre 2001[27], mais elle est encore plus probable dans le cyberdomaine en raison de la volonté d'empêcher une mise en péril des capacités ou activités offensives.

Les politiques destinées à améliorer les cybercapacités offensives d'un État entraveraient sa capacité à améliorer sa cyberdéfense, donneraient des résultats contreproductifs, susciteraient des conflits bureaucratiques internes et utiliseraient des ressources faisant double emploi. Des hésitations constantes seraient inévitables entre la volonté de signaler aux distributeurs, à l'industrie et au public les vulnérabilités repérées pour qu'elles puissent être corrigées et la tentation de maintenir ces vulnérabilités confidentielles pour que l'armée, les services de renseignement ou la police puisse les exploiter à des fins offensives. Les services de police américains et allemands ont mis au point et déployé des logiciels de surveillance qui utilisent des vulnérabilités et des techniques similaires à celles utilisées par les cybercriminels[28] ; il existe désormais toute une industrie qui cherche à signaler des vulnérabilités aux gouvernements plutôt qu'aux distributeurs ou au grand public[29]. Lors d'un événement annuel organisé par Google en mars 2012, une société bien connue de cybersécurité a refusé de communiquer des vulnérabilités et des exploits qu'elle avait découverts dans Chrome, le navigateur web de Google, car elle avait plus à gagner à conserver cette information pour ses clients qui sont les gouvernements des pays de l'OTAN et les partenaires de l'OTAN[30]. Cette attitude a soulevé des débats entre les sociétés de cybersécurité s'agissant de savoir si elles devaient signaler les logiciels malveillants conçus par des gouvernements[31]. Les sociétés de cybersécurité qui prendraient une telle décision pourraient compromettre des enquêtes en cours et risqueraient de s'exposer à des poursuites de la part des gouvernements, mais si elles ne disent rien, d'autres gouvernements ou des cybercriminels risqueraient d'utiliser ces techniques sans se faire remarquer.

Une stratégie défensive

D'un point de vue défensif, il serait logique d'opter pour la mise au point et l'acquisition de logiciels sur mesure pour les applications de sécurité nationale et pour les infrastructures essentielles. Une telle politique, qui obligerait l'agresseur à trouver des vulnérabilités dans les systèmes visés, présenterait néanmoins de sérieux inconvénients. Aucun logiciel d'une certaine ampleur n'est parfaitement sûr lorsqu'il est mis sur le marché. Tous les logiciels comportent un certain nombre de bugs dont une petite partie seulement constitue des vulnérabilités

de sécurité. Passer en revue le code n'est pas suffisant. Même dans le cas de logiciels libres dont le code source peut, en théorie, être examiné par n'importe qui pour trouver des bugs, il est arrivé que des bugs importants des protocoles de sécurité ne soient pas détectés avant plusieurs années[32]. Tester les logiciels dans toutes les conditions possibles d'utilisation est le seul moyen de trouver et corriger des bugs. C'est une activité particulièrement laborieuse pour les logiciels complexes ; dans certains cas, elle peut d'ailleurs se révéler irréaliste sur un plan économique voire impossible sur un plan pratique.

Les logiciels courants présentent l'avantage d'être utilisés dans de multiples circonstances et d'être attaqués plus souvent. Cela permet de découvrir et d'éliminer plus rapidement les bugs ainsi que les vulnérabilités exploitant ces bugs. Les vulnérabilités et bugs des logiciels les plus courants, comme les navigateurs web, ont d'ailleurs considérablement diminué[33]. Les fabricants et les utilisateurs de logiciels développent des pratiques de sécurité qui constituent une part importante de la cyberdéfense. Un logiciel utilisé par un petit nombre de personnes comportera aussi des bugs et des vulnérabilités mais il faudra plus de temps pour les découvrir et il est peu probable que les concepteurs et utilisateurs aient pu mettre au point des solutions optimales pour faire face aux attaques.

Un bon exemple pour illustrer ces deux cas de figure sont les systèmes d'exploitation développés respectivement par Microsoft et Apple, à savoir Windows et OS X. Le système Windows de Microsoft détient une part prépondérante du marché, mais il a connu des hauts et des bas en matière de sécurité. Toutes les versions de Windows comportaient de nombreuses vulnérabilités en raison de mauvais choix au niveau de l'architecture et de la nécessité de faire fonctionner des dispositifs variés et des applications tierces. Microsoft a donc mis au point un excellent processus pour repérer les vulnérabilités, alerter les utilisateurs et programmer et diffuser des correctifs. Au fil des années, Windows est devenu plus sûr ; ses utilisateurs sont aujourd'hui conscients des attaques les plus élémentaires auxquelles ils sont exposés.

Même si Apple a vu sa part du marché des ordinateurs portables et de bureau progresser rapidement ces dernières années, la société ne représente toujours qu'une petite part de marché par rapport à Microsoft[34]. Les agresseurs potentiels n'avaient pas vraiment intérêt, d'un point de vue économique, à chercher à exploiter les vulnérabilités des produits Apple puisqu'ils ne représentaient qu'une faible part de marché. Cette attitude et la campagne de marketing intensive lancée par Apple pour affirmer que OS X est un système d'exploitation plus « sûr » que Windows expliquent pourquoi de nombreux utilisateurs Apple pensent qu'ils sont en sécurité. Les attaques « Mac Defender », découvertes en mai 2011, obligèrent Apple à produire rapidement un correctif et à mettre en place de nouvelles politiques ; ces attaques eurent pour conséquence d'anéantir l'idée que la plateforme Apple était plus sûre. Apple est aujourd'hui engagé comme Microsoft dans une guerre contre les agresseurs, mais ne bénéficie pas de la même expérience en la matière que son adversaire et un grand nombre de ses utilisateurs pensent que les produits Apple sont sûrs[35].

Des progiciels libres ou disponibles dans le commerce peuvent être renforcés par une vérification du code et par une réduction des fonctionnalités en éliminant les fonctions et capacités superflues[36]. Pour une politique défensive, c'est certainement la meilleure option pour protéger des réseaux et capacités essentiels ; menée de manière intelligente, elle peut considérablement améliorer la sécurité en coûtant bien moins cher que la mise au point de logiciels sur mesure tout en stimulant la résistance des logiciels courants[37]. Cela dit, aucun système n'étant parfaitement sûr, une utilisation à grande échelle de cette stratégie ne fera qu'encourager la recherche d'autres points d'entrée dans la surface d'attaque. L'homme est souvent l'élément le plus vulnérable d'un système comme l'indique le très fort taux de succès des attaques d'ingénierie sociale comme le hameçonnage (*phishing*) et l'utilisation de pièces jointes malveillantes. Outre l'infection des réseaux de l'armée des États-Unis par le logiciel malveillant Agent.btz décrite plus haut, d'importantes attaques ont été lancées récemment contre les sociétés de sécurité informatique RSA et HBGary[38], Google et d'autres sociétés technologiques[39], et des dizaines d'organismes privés et gouvernementaux[40] en profitant des faiblesses de l'être humain.

La cyberdéfense a beaucoup à gagner d'une coopération et d'une coordination accrues entre les gouvernements, les industries privées et les chercheurs. Les applications et architectures logicielles disponibles dans le commerce étant très répandues dans les réseaux et systèmes informatiques des gouvernements, la protection des systèmes gouvernementaux repose donc en partie sur la découverte et la correction des vulnérabilités de ces logiciels. Le secteur privé représente, en outre, une partie importante de la surface d'attaque qu'un État doit défendre pour se protéger des cyber-attaques ou, en tout cas, pour en limiter les conséquences. Des entreprises privées gèrent l'exploitation de nombreuses infrastructures nationales essentielles susceptibles d'être visées par des cyber-attaques.

Les chercheurs jouent déjà un rôle majeur dans le monde de la cybersécurité, mais leurs initiatives sont souvent entravées ou réprouvées par les entreprises et par les gouvernements au motif qu'elles constituent une menace plutôt qu'un atout[41]. Cette situation doit changer ; la communauté des cybertechnologies devrait voir d'un bon œil les recherches et les expériences visant à mieux comprendre les vulnérabilités et les faiblesses des architectures de sécurité informatique.

Le grand public est généralement oublié alors qu'il pourrait jouer un rôle important au niveau de la cyberdéfense. Des millions d'ordinateurs personnels peuvent être détournés pour être utilisés comme armes ; c'est le cas, par exemple, lorsque des ordinateurs sont contrôlés à distance pour lancer des attaques par déni de service. Les appareils compromis, qu'il s'agisse d'ordinateurs personnels, d'appareils mobiles ou de comptes en ligne de hauts fonctionnaires ou de cadres d'entreprises, peuvent fournir des informations cruciales risquant de compromettre des systèmes protégés. Les amis et les connaissances sur les réseaux sociaux représentent également une autre piste pour lancer des attaques avec, d'ailleurs, plus de chances de succès puisque ce sont des personnes qui ont la confiance des utilisateurs.

Les politiques visant à améliorer la cyberdéfense d'un État doivent donc obligatoirement augmenter le nombre d'informations échangées entre les gouvernements, le secteur industriel, les chercheurs et peut-être même aussi le grand public et faire des changements considérables dans la politique actuelle de confidentialité des vulnérabilités et des cyber-attaques. Les gouvernements, le secteur industriel et les chercheurs doivent échanger des informations sur les vulnérabilités, les attaques les plus récentes et les signatures des logiciels malveillants[42]. Les programmes encourageant une attitude responsable consistant à signaler les vulnérabilités identifiées, comme ceux menés par Google et Mozilla Foundation pour leurs navigateurs web respectifs[43], permettraient de multiplier considérablement le nombre de gens recherchant des vulnérabilités et d'accélérer le rythme auquel les failles pourraient être repérées et corrigées. Cette stratégie aurait toutefois des conséquences négatives sur la capacité des États à mettre au point et à exploiter des moyens offensifs car les activités nécessaires pour repérer de nouvelles vulnérabilités et mettre au point des armes exploitant ces failles coûteraient plus cher et seraient menées en même temps que les sociétés étudieraient des correctifs.

Conclusions

La cybersécurité constitue un pari unique pour les responsables politiques surtout s'ils veulent atteindre ce double objectif consistant à protéger leurs propres réseaux tout en mettant au point des techniques et des instruments pour attaquer les réseaux de leurs adversaires. Stuxnet utilisait quatre vulnérabilités de Microsoft Windows jusqu'alors inconnues pour infecter des cibles. Ces vulnérabilités, présentes dans des centaines de millions d'ordinateurs dans le monde, une fois révélées, risquaient d'être exploitées. Les concepteurs de Stuxnet avaient décidé d'exploiter ces vulnérabilités à des fins offensives plutôt que de les communiquer aux sociétés de sécurité informatique et aux distributeurs de logiciels pour qu'ils les corrigent ; d'autres acteurs pouvaient ainsi profiter de ces vulnérabilités pour créer des logiciels malveillants et attaquer des gouvernements, des sociétés et des particuliers. Si Microsoft a réglé les quatre vulnérabilités de Windows exploitées par Stuxnet, certaines des graves vulnérabilités des systèmes de contrôle industriel de Siemens utilisées par Stuxnet n'étaient toujours pas réglées en janvier 2012[44].

Le cas Stuxnet montre les choix difficiles auxquels sont confrontés les responsables politiques qui veulent mener des cyber-activités offensives car ce faisant ils relèguent au second plan la cyberdéfense. La volonté de taire les vulnérabilités repérées pour les utiliser à des fins offensives entraîne inévitablement la persistance de ces vulnérabilités ce qui gêne les efforts défensifs. La mise au point de logiciels sur mesure, avec des logiciels libres ou commercialisés, pour les applications de sécurité nationale et les infrastructures essentielles permet, d'une certaine façon, d'échapper à ce dilemme entre activités offensives et défensives, mais coûte très cher. Autre point plus important encore, un tel choix ne protègerait que les systèmes utilisant ce logiciel sur mesure, mais pas ceux des entreprises, des citoyens ni ceux de ses alliés. De la même façon, les politiques de cyberdéfense (comme les programmes récompensant ceux

qui repèrent des vulnérabilités), qui encouragent la coopération, la coordination et le partage d'information entre les gouvernements, le secteur industriel, les chercheurs et le grand public, compliqueraient la tâche d'un État qui souhaiterait mettre au point des cyberprogrammes offensifs tout en les maintenant confidentiels.

En fin de compte, les États doivent décider s'ils veulent donner la priorité à des cyber-activités offensives ou défensives. Il est impossible de mener avec succès les deux types d'activités en parallèle ; l'accent porté aux unes compromet forcément la possibilité de réaliser les autres de manière efficace. Presque tous les États affirment de plus en plus fort leur volonté d'accroître la cybersécurité. De par les politiques qu'ils revendiquent et les actions qu'ils mènent discrètement, de nombreux États accordent actuellement la priorité aux activités offensives. Le Gouvernement américain a ainsi annoncé un certain nombre d'initiatives pour accélérer le développement militaire de cyber-armes offensives[45]. Les responsables politiques devront changer d'attitude s'ils veulent être cohérents avec leurs déclarations sur la nécessité d'une cyberdéfense ; ils devront pour cela prendre des mesures efficaces pour protéger leurs États et leurs citoyens.

Notes

1. « Operating System Market Share », NetMarketShare, mars 2012, <http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8>.
2. *Cisco 2010 Annual Security Report*, Cisco Systems, 2011, <www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf>, p. 22.
3. Pour plus de précisions, voir « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
4. Voir, par exemple, Gary D. Brown, « Why Iran Didn't Admit Stuxnet Was an Attack », *Joint Force Quarterly*, n° 63, 2011, <www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html> ; et Sydney J. Freedberg Jr., « Cyber Command Lawyer Praises Stuxnet, Disses Chinese Cyber Stance », AolDefense, 12 mars 2012, <http://defense.aol.com/2012/03/12/cyber-command-lawyer-praises-stuxnet-disses-chinese-cyber-stanc/>.
5. Voir « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
6. Voir « Enumerating Stuxnet's exploits », Langner Communications, 7 juin 2011, <www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/>.
7. « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>, p. 2.
8. Ibid., p. 9.
9. Ibid., p. 4.
10. Voir « Bulletin de sécurité Microsoft MS10-061 - Critique », Microsoft, 14 septembre 2010, <http://technet.microsoft.com/fr-fr/security/bulletin/ms10-061>.
11. « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>, p. 4.
12. Voir « Bulletin de sécurité Microsoft MS10-046 - Critique », Microsoft, 2 août 2010, <http://technet.microsoft.com/fr-ch/security/bulletin/ms10-046>.
13. « Updated W32.Stuxnet Dossier is Available », Symantec, mis à jour le 14 février 2011, <www.symantec.com/connect/blogs/updated-w32stuxnet-dossier-available>.

14. « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>, p. 10.
15. Ibid., p. 18 ; et Michael Joseph Gross, « A Declaration of Cyber-War », *Vanity Fair*, avril 2011, <www.vanityfair.com/culture/features/2011/04/stuxnet-201104>.
16. « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>, p. 5.
17. « Cyber worm found at German industrial plants », *The Local*, 2 octobre 2010, <www.thelocal.de/national/20101002-30225.html>.
18. Voir « W32.Stuxnet Dossier », Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> ; et Dale G. Peterson, « Langner's Stuxnet Deep Dive S4 Video », Digital Bond, 31 janvier 2012, <www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>.
19. Holly Stewart, « Stuxnet, malicious .LNKs, ... and then there was Sality », Microsoft Makware Protection Center, 30 juillet 2010, <http://blogs.technet.com/b/mmpc/archive/2010/07/30/stuxnet-malicious-lnks-and-then-there-was-sality.aspx>.
20. Voir « W32.Duqu », Symantec, ver. 1.4, 23 novembre 2011, <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>.
21. Voir, par exemple, « This is how Windows get infected with malware », CSIS Security Group, 27 septembre 2011, <www.csis.dk/en/csis/news/3321/> ; et Kim Zetter, « Researchers release new exploits to hijack critical infrastructure », Ars Technica, 5 avril 2012, <http://arstechnica.com/business/news/2012/04/researchers-release-new-exploits-to-hijack-critical-infrastructure.ars>.
22. Chris Blask, « Network Security: The Threats You Don't See », Infosec Island, 22 juin 2011, <www.infosecisland.com/blogview/14682-Network-Security-The-Threats-You-Dont-See.html>.
23. Voir Don Andrew Bailey, « War Texting », <www.isecpartners.com/storage/docs/presentations/iSEC_BH2011_War_Texting.pdf>.
24. Voir William J. Lynn III, « Defending a New Domain », *Foreign Affairs*, vol. 89, nº 5, 2010, <www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain>.
25. Voir Ellen Nakashima, « Cyber-intruder sparks massive federal response — and debate over dealing with threats », *Washington Post*, 9 décembre 2011, <www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html> ; et Leo Shane III, « DOD loosens restrictions on thumb drives », Stars and Stripes, 19 février 2010.
26. Voir, par exemple, Tom Gjelten, « Security Expert: U.S. 'Leading Force' Behind Stuxnet », *National Public Radio*, 26 septembre 2011, <www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-stuxnet> ; Ron Rosenbaum, « Richard Clarke on Who Was Behind the Stuxnet Attack », *Smithsonian*, avril 2012, <www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html> ; Michael Joseph Gross, « A Declaration of Cyber-War », *Vanity Fair*, avril 2011, <www.vanityfair.com/culture/features/2011/04/stuxnet-201104> ; et Dale G. Peterson, « Langner's Stuxnet Deep Dive S4 Video », Digital Bond, 31 janvier 2012, <www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>.
27. *The 9/11 Commission Report*, 2004, p. xvi et *passim*.
28. Kevin Poulsen, « FBI Spyware: How Does the CIPAV Work? — UPDATE », Wired, 18 juillet 2007, <www.wired.com/threatlevel/2007/07/fbi-spyware-how/> ; et Matthew Lasar, « Impressed by FBI trojan, Germans write their own—and national scandal ensues », Ars Technica, 14 octobre 2011, <http://arstechnica.com/security/news/2011/10/impressed-by-fbi-trojan-germans-write-their-ownand-national-scandal-ensues.ars>.
29. Michael Ray et Ashlee Vance, « Cyber Weapons: The New Arms Race », *Businessweek*, 20 juillet 2011, <www.businessweek.com/printer/magazine/cyber-weapons-the-new-arms-race-07212011.html>.
30. Andy Greenberg, « Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees) », *Forbes*, 21 mars 2012, <www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/>.

31. John Leyden, « AV vendors split over FBI Trojan snoops », The Register, 27 novembre 2001, <www.theregister.co.uk/2001/11/27/av_vendors_split_over_fbi/> ; et Stewart Mitchell, « F-Secure: security firms should block State malware », PC Pro, 8 mars 2011, <www.pcpro.co.uk/news/security/365791/f-secure-security-firms-should-block-state-malware>.
32. Voir, par exemple, Jake Edge, « A hole in crypt_blowfish », LWN.net, 22 juin 2011, <http://lwn.net/Articles/448699/>.
33. Robert Lemos, « The End Of Vulnerabilities? », Dark Reading, 15 mars 2012, <www.darkreading.com/vulnerability-management/167901026/security/security-management/232602714/the-end-of-vulnerabilities.html>.
34. Voir « Operating System Market Share », NetMarketShare, mars 2012, <http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=8>.
35. Don Reisinger, « Mac OS X Security Must Become a Priority: 10 Reasons Why », eWeek, 5 avril 2012, <www.eweek.com/c/a/Security/Mac-OS-X-Security-Must-Become-a-Priority-10-Reasons-Why-705108>.
36. Leander J Brandt IV, « Defending the Cyber Alamo: An Indefensible Position in Cyberspace », *High Frontier*, vol. 7, n° 3, 2011, <www.afspc.af.mil/shared/media/document/AFD-110519-023.pdf>, p. 24.
37. Thor Olavsrud, « Do Insecure Open Source Components Threaten Your Apps? », NetworkWorld, 30 mars 2012, <www.networkworld.com/news/2012/033012-do-insecure-open-source-components-257846.html>.
38. Uri Rivner, « Anatomy of an Attack », RSA, 1er avril 2011, <http://blogs.rsa.com/rivner/anatomy-of-an-attack/> ; et Peter Bright, « Anonymous speaks: the inside story of the HBGary hack », Ars Technica, 15 février 2011, <http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars>.
39. « Protecting Your Critical Assets », McAfee Labs et McAfee Foundstone Professional Services, 2010, <www.mcafee.com/us/resources/white-papers/wp-protecting-critical-assets.pdf>.
40. Hon Lau, « The Truth Behind the Shady RAT », Symantec, 4 août 2011, <www.symantec.com/connect/blogs/truth-behind-shady-rat>.
41. Voir, par exemple, Jaikumar Vijayan, « Carrier IQ drops legal threat against security researcher », Computerworld, 28 novembre 2011, <www.computerworld.com/s/article/9222203/Carrier_IQ_drops_legal_threat_against_security_researcher>.
42. Jason Healey, « Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More », *The Atlantic*, 15 mars 2012, <www.theatlantic.com/technology/archive/2012/03/cybersecurity-legislation-should-force-us-government-to-listen-less-and-speak-more/254491/>.
43. « Encouraging More Chromium Security Research », The Chromium Blog, 28 janvier 2010, <http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html> ; et « Bug Bounty Program », Mozilla, 1er février 2012, <www.mozilla.org/security/bug-bounty.html>.
44. Voir Dale G. Peterson, « Langner's Stuxnet Deep Dive S4 Video », Digital Bond, 31 janvier 2012, <www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>, à partir de 45:55.
45. Jim Wolf, « U.S. says will boost its cyber arsenal », Reuters, 7 novembre 2011, <www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107> ; Ellen Nakashma, « U.S. accelerating cyberweapon research », *Washington Post*, 19 mars 2012, <www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story.html> ; et Statement of General Keith B. Alexander, Commander, United States Cyber Command before the US House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, 20 mars 2012, <http://armedservices.house.gov/index.cfm/files/serve?File_id=69276bbe-070a-4b82-8d85-9440931bc8e0>.

Les mesures de transparence et de confiance dans le cyberespace : vers des normes de conduite

Ben Baseley-Walker

En 2012, le monde vit au rythme du cyberespace. Du commerce au développement, en passant par les opérations de guerre, le cyberespace est un élément caractéristique de l'ère actuelle. La progression spectaculaire de l'utilisation des cybertechnologies dans les secteurs civils, militaires et commerciaux depuis 2000 a fait apparaître un nouvel environnement en matière de sécurité. Les gouvernements doivent faire face aux conséquences potentielles de ce nouveau domaine susceptible d'engendrer des conflits. Ayant pris conscience de la dépendance du monde à l'égard des cybertechnologies, les gouvernements adoptent aujourd'hui des positions fermes pour instaurer une certaine prévisibilité et garantir la stabilité et la sécurité du cyberespace. Les attaques du virus Stuxnet et celles contre la Bourse de New York prouvent qu'aujourd'hui le cyberespace est un domaine où s'expriment désormais les intérêts fondamentaux des États comme ils le faisaient auparavant dans les domaines maritimes et aériens, et dans l'espace extra-atmosphérique. Dans le monde d'aujourd'hui, les frontières terrestres ne représentent plus la même chose. Le cyberespace est un nouveau domaine de projection de puissance gouvernementale et non gouvernementale[1].

Suite aux cyber-attaques qui touchèrent l'Estonie en 2007 et la Géorgie en 2008 et à l'attaque des installations nucléaires iraniennes en 2010, les risques de cyberguerre sont clairement devenus un « élément inévitable de toute discussion portant sur la sécurité internationale »[2]. À ce jour, la cyberguerre figure dans l'organisation et la planification militaires d'au moins 33 États[3]. Il ressort peu à peu des simulations et des analyses politiques et militaires qu'il existe aujourd'hui peu de moyens, si ce n'est aucun, de contrôler efficacement les risques d'escalade d'un cyberconflit. Il n'existe pas non plus de position commune sur la façon d'appliquer à ce domaine les normes du droit international humanitaire ni sur la question de savoir si elles devraient s'appliquer.

Cet article examine une mesure clef pour faire évoluer la situation : la création de normes de conduite et la mise en place de mesures de transparence et de confiance. Après avoir étudié la nature des mesures de transparence et de confiance possibles pour le cyberespace, cet article verra comment elles peuvent être appliquées avant d'évoquer différentes initiatives déjà engagées.

Il convient de préciser clairement ce que sont la cybercriminalité et la cyberguerre. Il est néanmoins difficile de définir les frontières qui séparent différentes activités négatives menées dans le cyberespace. La cybercriminalité s'entend des activités considérées comme illégales au niveau national ou international et réalisées par des acteurs non étatiques. Ces activités

---

Ben Baseley-Walker travaille à l'Institut des Nations Unies pour la recherche sur le désarmement (UNIDIR) où il est responsable du programme sur les nouvelles menaces. Il a été auparavant conseiller sur la politique de sécurité et le droit international pour Secure World Foundation (SWF). Les vues exprimées dans cet article sont celles de l'auteur et ne reflètent pas nécessairement celles de l'UNIDIR ou de l'Organisation des Nations Unies.

sont très variées et peuvent aller d'utilisations frauduleuses de cartes bancaires jusqu'à la pornographie enfantine. Cet article s'intéresse pour sa part à la cyberguerre qui est définie comme un ensemble de cyber-activités offensives soutenues par un État et visant un autre État, ses infrastructures ou sa population. Précisons que la communauté internationale n'a pas encore convenu des paramètres de la zone grise séparant l'espionnage – ou collecte illégale de données – et la cyberguerre.

Le concept des mesures de transparence et de confiance

Les mesures de transparence et de confiance sont des éléments de politique internationale qui réduisent les menaces, renforcent la confiance et améliorent la prévisibilité des relations entre États. Elles sont utiles, depuis longtemps, à la communauté internationale pour gérer des questions de sécurité internationale et plus particulièrement dans le domaine des armes nucléaires[4]. Les mesures de transparence et de confiance sont depuis longtemps considérées comme des instruments politiquement contraignants. Elles sont généralement envisagées comme une étape intermédiaire avant l'instauration d'instruments juridiquement contraignants pour défendre la sécurité internationale mais il n'est pas exclu qu'elles aient elles-mêmes force obligatoire.

L'idée de mesures de transparence et de confiance et celle de normes de conduite ont fait l'objet de nombreuses discussions politiques. Les mots confiance, sécurité et transparence ont été employés de manières différentes, chaque concept suscitant invariablement des réactions négatives de la part d'un État ou d'un autre. La communauté internationale s'accorde néanmoins à reconnaître que des mesures devront être prises bientôt concernant le cyberespace.

Les Nations Unies encouragent depuis longtemps les mesures de transparence et de confiance pour favoriser la sécurité entre les États Membres. Au début des années 80, la Commission du désarmement de l'ONU élabora un ensemble de directives concernant les mesures de confiance qu'elle présenta lors d'une session extraordinaire de l'Assemblée générale consacrée au désarmement :

> 2.2.5 Un des objectifs majeurs est de réduire, voire d'éliminer les causes de méfiance, de peur, de malentendus et d'erreurs d'appréciation en ce qui concerne les activités militaires et les intentions d'autres États, facteurs qui risquent de donner le sentiment d'une sécurité compromise et de justifier la poursuite des politiques d'armement sur le plan mondial aussi bien que régional.
>
> 2.2.6 Un objectif essentiel de ces mesures est de réduire les risques de méprises ou d'erreurs dans les opérations militaires, d'aider à prévenir les affrontements militaires ainsi que les préparatifs de guerre secrets, réduire le risque d'attaques surprise et de déclenchement accidentel d'une guerre ; et, enfin, de donner

> une forme effective et concrète à l'engagement solennel de toutes les nations de s'abstenir de recourir à la menace ou à l'usage de la force sous toutes ses formes et de renforcer la sécurité et la stabilité[5].

Dans le cadre de cet article, les mesures de transparence et de confiance sont destinées à limiter les risques d'escalade d'un conflit en raison d'un manque de confiance et d'une méconnaissance des cyber-activités de tous les acteurs, alliés comme adversaires. Il existe de nombreux avantages à rendre juridiquement obligatoires les mesures de transparence et de confiance ; cela dit, vu l'incertitude et la méfiance qui prévaut entre les États au sujet de la cybersécurité, les mesures de transparence et de confiance seront, au mieux, des engagements politiquement contraignants.

Il existe, en somme, deux types de mesures de transparence et de confiance : celles concernant les capacités et celles concernant les intentions. Les premières sont considérées par certains États comme une obligation de diligence ; elles démontrent quelles sont les meilleures pratiques des États en matière de sécurité. Les deuxièmes, qui se concentrent sur les normes internationales, entendent favoriser une meilleure compréhension des interactions entre États s'agissant des problèmes de sécurité internationale se rapportant au cyberespace[6]. Depuis longtemps, les mesures de transparence et de confiance viennent compléter des instruments juridiquement contraignants ou jeter les bases nécessaires pour progresser. Elles peuvent aller dans le sens d'un instrument juridiquement contraignant ou favoriser une meilleure compréhension pendant que se poursuivent des activités dans le cyberespace ou la mise au point de cyberdéfenses et que la politique justifiant ces choix est largement expliquée.

Il est important de préciser que les mesures de transparence et de confiance ne nécessitent pas une structure ou une forme particulière. Les activités menées par des entités totalement commerciales, comme le partage de données sur les cyber-attaques, peuvent constituer une mesure de transparence et de confiance visant à réduire les tensions politiques et militaires entre États. De nombreuses coopérations fructueuses ont été engagées dans d'autres secteurs. Ainsi, le partage des données de positionnement orbital entre les exploitants de satellites commerciaux par le biais de la Space Data Association a favorisé l'échange de données et d'informations entre organismes gouvernementaux.

Quel est l'objectif ?

L'objectif est, à l'évidence, de favoriser un cyberespace sûr, stable et, surtout, prévisible. La volonté d'un État d'exacerber les tensions ou d'endommager le cyber-environnement est proportionnellement inverse à son engagement dans le cyberespace. Plus un État augmente ses cyber-ressources – civiles, commerciales et militaires – et retire de l'utilisation d'Internet des bénéfices économiques toujours plus importants, plus l'avantage asymétrique d'attaquer un adversaire en comptant sur les cyber-ressources risque d'avoir des conséquences importantes pour l'auteur de l'agression.

L'une des principales difficultés dans le cyberespace est de déterminer qui est responsable d'une attaque. Même si l'agresseur est identifié à temps avec un fort degré de certitude, il est extrêmement difficile voire impossible de prouver qu'une attaque a bénéficié du soutien d'un État. Les États n'ont que peu d'options : ne rien faire ou s'exposer au risque d'une escalade rapide de la crise, car personne ne connaît avec certitude ce que leur adversaire considère comme « la ligne à ne pas franchir » ni ne sait vraiment par quoi se traduirait une escalade. Il faut absolument instaurer dans le cyberespace des mécanismes d'interaction entre États pour réduire les risques d'escalade et de conflit. Les mesures de transparence et de confiance jouent un rôle déterminant pour éviter les erreurs d'appréciation et faire connaître les intentions des États sur le long terme.

Une première étape : comprendre la position de ses alliés et celle de ses adversaires

Pour instaurer des mesures de transparence et de confiance efficaces, il faut avant toute chose connaître les critères retenus par les autres acteurs pour leurs opérations dans le cyberespace. Dans le domaine politico-militaire, l'élaboration et le partage de la doctrine militaire, l'évaluation des objectifs d'une politique nationale annoncée concernant le cyberespace et la mise en place de dispositifs de gestion de crises, comme des lignes directes, sont autant d'éléments indispensables. Certaines questions politiques s'annoncent particulièrement épineuses. La plus discutée aujourd'hui est celle de savoir si l'information peut être considérée comme une arme. Certains États considèrent certains mécanismes d'information comme des canaux diffusant des nouvelles ou de la propagande et pensent qu'ils représentent, à ce titre, une menace pour l'État. Le cyberespace et Internet sont, par conséquent, considérés comme des canaux majeurs de diffusion. D'autres États estiment que la liberté de l'information est un principe fondamental des échanges dans le cyberespace. Cette division des points de vue ne sera pas facile à surmonter. Les mesures de transparence et de confiance permettent toutefois d'envisager des progrès même sur des sujets aussi sensibles sur le plan politique. En tentant de comprendre ces deux positions, les différentes stratégies possibles et les lignes à ne pas franchir, les États peuvent trouver des terrains d'entente et essayer de s'en approcher. Cette tactique permet d'éviter une situation d'usure dans laquelle chacun campe sur ses positions. Les principes fondamentaux peuvent ainsi être posés, ce qui permet de traiter les questions principales, par exemple : quelles sont les règles d'engagement pour un conflit dans le cyberespace ?

De nombreuses autres questions se posent concernant les frontières et les lignes à ne pas franchir dans le cyber-environnement. Un État interpréterait-il une attaque contre sa plus grande banque commerciale, soutenue par un autre État, comme une attaque armée au sens de l'Article 51 de la Charte des Nations Unies[7] ? Quelles sont les infrastructures essentielles d'un État et quelle serait une réaction proportionnelle si ces infrastructures étaient attaquées ? Si ces différents éléments étaient clairement définis, les responsables politiques et les acteurs militaires comprendraient mieux ce qu'impliquerait concrètement un affrontement entre États

dans le cyberespace. Les États-Unis ont clairement dit que, pour eux, la structure juridique internationale existante, y compris le droit des conflits armés, est applicable au cyberespace. Ils ont néanmoins souligné la nécessité d'élaborer des principes pour parvenir à une conclusion juridique définitive sur la question de savoir si une activité engendrant de graves perturbations dans le cyberespace constitue une attaque armée pouvant déclencher le droit à la légitime défense[8].

Concernant les spécificités de la légitime défense, il importe de mieux comprendre quelles sont les obligations des États pour éviter que leur territoire ne soit utilisé pour mener des cyber-attaques. Il existe à ce niveau aussi une différence évidente entre cybercriminalité et cyberguerre. D'aucuns estiment qu'en vertu du droit de la neutralité, les non-belligérants ne sont pas tenus d'empêcher que leurs réseaux ne soient utilisés pour lancer des activités offensives[9]. Il faut clarifier les choses si l'on veut que tous les États – et non pas seulement ceux dotés de capacités offensives – adoptent des normes de conduite efficaces.

Les initiatives actuelles

La Conférence de Londres sur le cyberespace

La Conférence de Londres sur le cyberespace, organisée en septembre 2011, a joué un rôle crucial en mettant en évidence les mesures indispensables pour instaurer la confiance entre les partenaires internationaux. Les débats de la Conférence de Londres ont clairement démontré qu'il existe une variété d'opinions sur la nature exacte et la définition de la cybersécurité. La question de la définition du terme n'a pas été directement posée mais une dichotomie évidente est apparue entre ceux qui considèrent la liberté sur Internet comme une question relevant clairement des droits de l'homme et ceux qui s'inquiètent pour la sécurité nationale et la sécurité de l'information et qui craignent que l'information ne soit utilisée comme une arme[10].

Ces discussions prouvent la nécessité de séparer l'expression d'idées politiques dans le cyberespace des mesures concrètes qui s'imposent pour élaborer des mesures de transparence et de confiance en matière de cybersécurité et sécuriser à long terme le cyberespace. Lors des discussions sur la sécurité internationale pendant la Conférence de Londres :

> Tous les délégués ont souligné l'importance pour les gouvernements de respecter le principe de proportionnalité dans le cyberespace, les règles existantes du droit international et les normes habituelles de conduite qui régissent les relations entre États, le recours à la force ou au conflit armé, ainsi que le règlement par les États de leurs différends internationaux par des moyens pacifiques de façon à ne pas compromettre la justice, la sécurité et la paix internationales[11].

Notons que les participants n'ont pas jugé le moment opportun pour discuter de mesures juridiquement contraignantes. Le véritable succès de rencontres comme la Conférence de Londres est d'offrir un cadre informel mais structuré pour convenir d'une position commune sur les prochaines mesures à prendre et sur de futures discussions. Il reste à espérer que les conférences de 2012 et 2013 – organisées respectivement par la Hongrie et la République de Corée – donneront des résultats similaires.

Un code de conduite international pour la sécurité de l'information

La Chine, la Fédération de Russie, l'Ouzbékistan et le Tadjikistan firent une proposition de code de conduite international pour la sécurité de l'information. Cette proposition fut distribuée pour la première fois en 2011 dans une lettre adressée au Secrétaire général de l'ONU[12]. Même si cette proposition est loin de faire l'unanimité, elle a été utile pour lancer le débat.

Le code proposé ne comporte pourtant aucune recommandation concernant des définitions, la mise en place de normes ou de mesures de transparence et de confiance ; il se limite à des remarques générales sur la nature de la sécurité de l'information et l'utilisation potentielle de l'information comme arme.

> Tout État adhérant volontairement au Code s'engage :
>
> [...]
>
> b) À ne pas utiliser les technologies de l'information et de la communication, y compris les réseaux, afin de mener des activités hostiles ou des actes d'agression et de menacer la paix et la sécurité internationales, ou diffuser l'arme informationnelle ou les technologies correspondantes[13].

Cette conception d'une liberté limitée de l'information a été systématiquement dénoncée par différents États, en particulier le Royaume-Uni et les États-Unis. À ce stade de l'élaboration de normes pour la cybersécurité, il semble que la communauté internationale ne soit pas prête à travailler sur un tel document. Cette situation prouve une fois de plus la nécessité de réaliser un travail multisectoriel de fond sur la terminologie et de déterminer les points d'entente et de désaccord avant de progresser sur des questions plus complexes et politiquement sensibles.

Les organisations régionales

Les organisations régionales utilisent depuis longtemps les mesures de transparence et de confiance dans les domaines classiques de sécurité. La mise en œuvre de telles initiatives par une organisation régionale présente de nombreux aspects positifs. Elle se fonde sur des modèles et des lignes de communication que les États participants connaissent. Par conséquent, des méthodes ayant été utilisées avec succès dans d'autres domaines peuvent être appliquées au cyberespace. De plus, des organisations régionales peuvent être mieux placées pour répondre aux demandes ou préoccupations de la région – surtout si les cybercapacités

de ses États membres en sont au même stade de développement. À titre d'exemple, les États membres de l'Organisation pour la sécurité et la coopération en Europe (OSCE), soutenus par des acteurs clefs comme le Royaume-Uni[14], envisagent la possibilité d'instaurer un groupe de travail chargé d'élaborer des mesures de confiance pour le cyberespace. Le groupe de travail serait instauré par une décision du Conseil permanent de l'OSCE. S'il réussit dans sa mission, ce modèle pourrait être repris par d'autres organisations régionales.

Un autre exemple est l'accord des États membres de l'Organisation de coopération de Shanghai sur la sécurité internationale de l'information[15]. Cet accord, signé en 2009 par la Chine, la Fédération de Russie, le Kazakhstan, le Kirghizistan, l'Ouzbékistan et le Tadjikistan représente une avancée considérable dans l'élaboration de positions politiques communes en matière de sécurité de l'information. L'élément le plus important de cet accord est la liste de définitions de termes essentiels qu'il propose. Ces définitions faciliteront les discussions futures puisque les parties auront une meilleure idée des paramètres conceptuels utilisés par chacun.

Les groupes d'experts gouvernementaux de l'ONU sur la sécurité de l'information

L'Assemblée générale des Nations Unies réunit de temps à autre des groupes d'experts gouvernementaux pour examiner des sujets particulièrement préoccupants et faire des recommandations. Ces groupes ne comptent généralement pas plus de 15 experts nommés sur la base d'une représentation géographique équitable. Les groupes d'experts gouvernementaux se réunissent en séances privées et tentent d'adopter un rapport par consensus. Si le groupe réussit à s'entendre, le rapport est soumis à l'examen du Secrétaire général.

Suite à une proposition de la Fédération de Russie, un groupe d'experts gouvernementaux fut constitué en 2004 pour étudier la question de la sécurité de l'information. Le Groupe ne parvint pas à s'entendre[16]. En 2009, un deuxième groupe d'experts gouvernementaux fut réuni. Il était chargé de :

> [...] poursuivre l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures de coopération qui pourraient être prises pour y parer, ainsi que l'étude des principes susceptibles de renforcer la sécurité des systèmes mondiaux dans le domaine de la téléinformatique[17].

Dans son rapport de 2010, qui fit l'objet d'un consensus, le Groupe d'experts gouvernementaux faisait les recommandations suivantes :

> i) Poursuivre la concertation entre États sur des normes éventuelles relatives à l'utilisation des TIC [technologies de l'information et des communications] par les États, afin de réduire le risque collectif et de protéger les infrastructures nationales et internationales essentielles ;

> ii) Adopter des mesures de confiance, de stabilité et de réduction des risques qui répondent aux conséquences de l'utilisation des TIC par les États, avec notamment des échanges de vues entre pays sur l'utilisation des TIC dans les conflits ;
>
> iii) Échanger des informations sur les législations nationales et les stratégies de sécurité nationales relatives aux technologies de l'information et des communications, ainsi que sur les techniques, les politiques et les meilleures pratiques ;
>
> iv) Définir des moyens d'aider les pays moins développés à renforcer leurs capacités ;
>
> v) Mettre en évidence les possibilités d'élaborer des modalités et des définitions communes procédant de la résolution 64/25 de l'Assemblée générale[18].

L'Assemblée générale a accepté de constituer en 2012 un nouveau groupe d'experts gouvernementaux chargé de poursuivre « l'examen des risques qui se posent ou pourraient se poser dans le domaine de la sécurité de l'information et des mesures collectives qui pourraient être prises pour y parer [...], en tenant compte des constatations et recommandations figurant dans le rapport » de 2010 ainsi que l'étude des « principes internationaux visant à renforcer la sécurité des systèmes télématiques et informatiques mondiaux »[19]. D'après la structure des recommandations faites en 2010, la prochaine étape devrait préciser la mise en œuvre des recommandations et – tout aussi important – désigner un cadre pour discuter des mesures de transparence et de confiance liées à la sécurité internationale au niveau du cyberespace.

Forum FIRST

Comme nous l'avons vu précédemment, les mesures de transparence et de confiance sur la sécurité internationale et la cyberguerre ne doivent pas forcément être définies au niveau national. Le secteur privé étant très impliqué dans le cyberespace, des groupes représentant des acteurs variés et influençant les normes de conduite ont un rôle crucial à jouer.

Le Forum FIRST est une initiative de ce genre. Ce réseau international d'équipes d'intervention en cas d'urgence informatique fut constitué en 1990 dans le but de régler les difficultés que posent, entre autres, les différences de langues, les fuseaux horaires et les normes internationales. Ce réseau veut coordonner l'action des équipes d'intervention en cas d'urgence informatique face aux incidents de sécurité informatique et encourager les programmes de prévention des incidents. En réunissant des acteurs de milieux gouvernementaux, militaires, commerciaux et académiques, ce mécanisme coordonne les interventions en cas d'incident dans le cyberespace et permet de connaître les meilleures pratiques, d'utiliser les outils adaptés et de communiquer en toute sécurité avec les autres équipes membres du réseau.

De telles initiatives, bien qu'elles répondent à des besoins très spécifiques, favorisent grandement l'internationalisation des meilleures pratiques en matière de cybersécurité.

C'est particulièrement intéressant pour les États ayant moins de capacités dans le domaine de la cybersécurité. La communauté de la sécurité internationale doit absolument étudier les mécanismes de ce genre et veiller à ce que l'action multilatérale menée au niveau des gouvernements soit en harmonie avec les activités des exploitants et d'autres acteurs, notamment les sociétés privées utilisant les infrastructures du cyberespace.

L'Union internationale des télécommunications (UIT)

Avec son Programme mondial cybersécurité, l'UIT n'a cessé de jouer un rôle dans le domaine de la cybersécurité et opté, de manière générale, pour une approche globale des questions concernant les cyberconflits et la cybercriminalité. Hamadoun Touré, le Secrétaire général de l'UIT, a défini cinq principes clefs pour la « cyberpaix » :

1. Tout gouvernement devrait s'engager à donner à ses citoyens l'accès aux communications.
2. Tout gouvernement devrait s'engager à protéger ses citoyens dans le cyberespace.
3. Tout pays s'engagera à ne pas héberger de terroristes/criminels sur son propre territoire.
4. Chaque pays devrait s'engager à ne pas être le premier à lancer une cyber-attaque contre un autre pays.
5. Chaque pays doit s'engager à collaborer avec les autres pays dans un cadre international de coopération afin de garantir le maintien de la paix dans le cyberespace[20].

Ces principes, qui traduisent l'avis du Secrétaire général de l'UIT, semblent néanmoins indiquer la direction générale de l'implication de l'UIT dans le cyberespace. Il convient de saluer les efforts inlassables de l'UIT pour définir des normes, développer les capacités et établir des liens entre la cybercriminalité et les cyberconflits. Un examen plus poussé s'impose pour bien comprendre ce que ce travail technique et procédural peut apporter aux grandes discussions politiquement sensibles qui ont lieu au niveau international sur la cybersécurité. Il importe également de bien comprendre les liens avec d'autres initiatives.

Conclusion

La diplomatie de la communauté internationale marque aujourd'hui un tournant sur les questions de cybersécurité. Les États sont conscients des menaces et des difficultés qui les attendent dans un environnement en constante évolution. Les initiatives évoquées dans cet article n'en étant qu'aux premières phases, les États ne sont pas encore liés sur le plan politique à une initiative particulière les empêchant d'envisager d'autres options. Il faut profiter de cette situation. De réels progrès sont aujourd'hui possibles au niveau des définitions et des mesures opérationnelles de transparence et de confiance. Les préoccupations d'aucun État ne doivent

être négligées. Il faut néanmoins absolument faire la distinction entre les mesures qui sont dans l'intérêt de toutes les parties et celles plus conceptuelles concernant le juste équilibre entre liberté d'expression et guerre de l'information.

De nombreux sujets permettraient, à court terme, d'enregistrer des avancées : clarifier la doctrine militaire et politique sur des questions comme la protection des infrastructures essentielles et préciser les positions nationales concernant les seuils à partir desquels les États engageraient des mesures offensives ou défensives dans le cyberespace

S'agissant des mesures de transparence et de confiance, toutes les options doivent être envisagées puisque l'objectif est de parvenir à un cyber-environnement plus stable, plus prévisible et moins susceptible d'engendrer des erreurs de communication pouvant déboucher sur un conflit. Des accords bilatéraux entre cyberpuissances confirmées, un accord multilatéral ou un accord international entre le secteur public et le privé sont autant d'options envisageables ; il convient néanmoins d'étudier si elles sont réalisables.

Les années 2012 à 2014 seront cruciales pour définir l'orientation des rapports qui existeront à l'avenir entre les États et le cyberespace. Espérons que les mesures de transparence et de confiance mises au point au cours de cette période favoriseront des rapports aussi pacifiques que possible.

Notes

1. Pour plus d'informations sur les attaques de Stuxnet voir R. Langner, *Cracking Stuxnet: A 21st-Century Cyber Weapon*, <www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html>.
2. J. Lewis et K. Timlin, « Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization », UNIDIR, 2011, p. 4.
3. Ibid., p. 3.
4. Voir J. Robinson, « The Role of Transparency and Confidence-Building Measures in Advancing Space Security », *European Space Policy Institute Report 28*, 2010, p. 14 à 26.
5. Assemblée générale, *Rapport de la Commission du désarmement*, document des Nations Unies A/S-15/3, 1988, p. 29.
6. Les commentaires de M. Markoff lors de la conférence "International Engagement on Cyber", Université de Georgetown, 29 mars 2011, sont disponibles à l'adresse <www.acus.org/event/international-engagement-cyber-establishing-international-norms-improved-cyber-security/panel-4-transcript>.
7. En vertu de l'Article 51 de la Charte des Nations Unies « 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 est 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 ».
8. Département d'État des États-Unis, *Cyber security keynote address by Dr. Deborah Schneider, US Department of State*, document FSC-PC.DEL/30/10, 9 juin 2010, p. iv.
9. Voir N. Melzer, « Cyberwarfare and International Law », UNIDIR, 2011, section IV.
10. Pour plus d'informations sur Internet et les droits de l'homme, voir la Maison Blanche, « VP's Remarks to the London Cyberspace Conference », discours du Vice-Président des États-Unis Joe Biden, 1er novembre 2011.
11. Ministère des affaires étrangères et du Commonwealth, *London Conference on Cyberspace: Chair's Statement*, 2 novembre 2011.

12. Assemblée générale, *Lettre datée du 12 septembre 2011, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, de l'Ouzbékistan et du Tadjikistan*, document des Nations Unies A/66/359, 14 septembre 2011.
13. Ibid, p. 4.
14. « De son côté, le Royaume-Uni va travailler activement avec l'ONU et des organisations comme l'OSCE pour élaborer des mesures de confiance permettant de réduire le risque d'escalade et d'éviter les malentendus entre États suite à des incidents inattendus dans le cyberespace », Cabinet Office, *The UK cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, 2011, p. 26.
15. Organisation de coopération de Shanghai, Annexe I à l'accord entre les gouvernements des États membres de l'Organisation de coopération de Shanghai sur la question de la coopération pour la sécurité internationale de l'information, 16 juin 2009, d'après une traduction non officielle.
16. Outre les cinq membres permanents du Conseil de sécurité – la Chine, les États-Unis, la Fédération de Russie, la France et le Royaume-Uni –, l'Afrique du Sud, l'Allemagne, le Bélarus, le Brésil, l'Inde, la Jordanie, la Malaisie, le Mali, le Mexique et la République de Corée étaient également représentés. Pour plus d'informations, voir T. Maurer, « Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security », *Explorations in Cyber International Relations Discussion Paper 2011–11*, 2011.
17. Assemblée générale, *Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/65/201, 30 juillet 2010, p. 5.
18. Ibid., p. 8. Le Groupe d'experts gouvernementaux était composé des cinq membres permanents du Conseil de sécurité, de l'Afrique du Sud, de l'Allemagne, du Bélarus, du Brésil, de l'Estonie, de l'Inde, d'Israël, de l'Italie, du Qatar et de la République de Corée.
19. Assemblée générale, *Les progrès de l'informatique et de la télématique et la question de la sécurité internationale*, document des Nations Unies A/C.1/66/L.30, 14 octobre 2011.
20. UIT, *En quête de la cyberpaix*, 2011, p. 118 et 119.

Parvenir à une compréhension mutuelle : pourquoi le cyberpouvoir importe autant aux pays développés qu'aux pays en développement

John B. Sheldon

Le cyberespace et les problèmes de sécurité qui s'y rattachent occupent une place grandissante dans les discussions diplomatiques sur la sécurité internationale. Cet intérêt s'explique par les menaces que font peser ou semblent faire peser les cybercapacités sur la sécurité nationale et sur la prospérité économique des États. Jusqu'à présent, les débats portaient principalement sur les préoccupations des pays développés. Quant aux pays en développement, ils étaient silencieux, ignorés ou considérés comme les méchants. Les pays en développement ne sont pas aussi impliqués que les pays développés dans les discussions organisées au niveau mondial sur le cyberespace, mais je pense que certaines questions liées au cyberespace sont aussi importantes pour les pays développés que pour ceux en développement.

Les discussions sur les cybermenaces et la « cyberguerre » portent essentiellement sur les préoccupations de sécurité des États développés. Certaines de ces craintes sont légitimes, mais l'on peut regretter l'alarmisme des analyses portant sur l'ampleur et les conséquences de ces menaces et l'attitude de nombreux responsables politiques qui sous-estiment la difficulté qu'il y a à lancer des cyber-attaques d'envergure. En réalité, les cyber-attaques catastrophiques paralysant le réseau électrique d'un pays, provoquant la chute d'un avion ou perturbant les réseaux financiers sont certes possibles mais peu probables en raison de la complexité des cibles visées, des nombreuses étapes au cours desquelles une attaque peut échouer et de la chance incroyable que devrait avoir un agresseur pour atteindre son objectif. Il convient aussi de souligner que les pays développés disposent d'infrastructures leur permettant d'assurer, en cas de cyber-attaque, la continuité des opérations essentielles ou militaires.

Certains pays en développement ont été identifiés comme étant à l'origine de cyber-attaques, mais les discussions évoquent rarement l'intérêt des pays en développement en matière de cybersécurité et les conséquences des cyber-attaques pour ces pays. De telles attaques représentent pour les pays en développement un risque aussi important, et parfois plus grave, que pour les pays développés. Ce sont pourtant ces derniers qui définissent les priorités de la communauté internationale en matière de cybersécurité. Le cyberespace est néanmoins un enjeu essentiel pour tous ces pays.

Les technologies de l'information et de la communication ont conféré aux États en développement qui les ont adoptées un avantage militaire et permis de nombreux progrès dans les services publics et dans la qualité de vie en général, mais ces technologies ne sont pas un avantage absolu. Il en est de même de l'ubiquité des cybertechnologies dans les pays développés. Plus les États profitent des avantages que leur procurent les technologies

---

John B. Sheldon est professeur en Space and Cyberspace Strategic Studies, School of Advanced Air and Space Studies. Les vues exprimées dans cet article sont celles de l'auteur et ne reflètent pas nécessairement celles de l'US Air Force ou de l'Organisation des Nations Unies.

de l'information et de la communication, plus ils sont exposés à d'éventuelles cyber-attaques catastrophiques. J'ai relevé cinq sujets qui semblent être un motif d'inquiétude pour tous les États. Ils pourraient servir de point de départ pour des discussions intéressantes susceptibles de conduire à des initiatives diplomatiques plus concrètes.

Le cyberespace et les cybermenaces

Avant de poursuivre le cœur de notre discussion, il convient de décrire ce qu'est le cyberespace et les cybermenaces les plus inquiétantes.

Dans cet article, nous entendons par cyberespace :

> Un domaine mondial au sein de l'infosphère qui se distingue par l'utilisation de l'électronique et du spectre électromagnétique pour créer, stocker, modifier, échanger et exploiter des informations au moyen de réseaux connectés interdépendants utilisant les technologies de l'information et de la communication[1].

Les effets produits depuis le cyberespace – qu'ils soient stratégiques (diplomatiques, militaires) voire criminels – représentent le cyberpouvoir, autrement dit la capacité d'utiliser le cyberespace pour se procurer des avantages et influencer des événements dans tous les environnements opérationnels et tous les instruments du pouvoir[2]. Les environnements opérationnels sont l'air, la terre, la mer et l'espace ; et les instruments du pouvoir sont la diplomatie, l'information, la menace et l'emploi de la force militaire, ainsi que les instruments économiques, sociaux et culturels.

Il convient de noter qu'ici le cyberespace est décrit comme un « domaine mondial » et non comme un patrimoine commun. Cette distinction est essentielle. La description ci-dessus montre bien que si la souveraineté peut s'imposer – et réussit à le faire – dans le cyberespace c'est parce que la grande majorité de ses infrastructures matérielles appartiennent à des sociétés privées enregistrées dans des États souverains et que les autres infrastructures appartiennent à des États. Ces infrastructures comprennent tous les câbles transocéaniques et les satellites qui acheminent des paquets d'information dans ce domaine mondial.

Précisons que la définition du cyberespace retenue dans cet article le subordonne au domaine plus large qu'est l'« infosphère »[3]. Dans l'infosphère circulent des informations provenant de multiples sources – êtres humains, documents imprimés, chaînes de radio ou de télévision, films, vidéos et cyberespace. Si le cyberespace s'impose rapidement comme l'un des principaux canaux de circulation de l'information, il est loin d'être le seul moyen dont disposent les individus, les sociétés privées, les organisations non gouvernementales et les gouvernements.

Diverses caractéristiques du cyberespace expliquent la place qu'il occupe aujourd'hui dans les débats et la politique sur la sécurité internationale et l'importance croissante qu'il joue dans le

domaine stratégique. Ces caractéristiques ont des conséquences positives et négatives pour les personnes, les organisations de toutes sortes, les États et la politique internationale. Dans le cyberespace, il est difficile de faire la distinction entre ce qui est, sur un plan technologique, offensif et défensif ; les actions et comportements offensifs sont, pour leur part, identifiables, même s'il peut être extrêmement difficile de déterminer d'où ils proviennent, où ils se produisent et la raison qui les motivent.

Ces caractéristiques sont les suivantes :

- accès facile sur le plan technologique car les équipements sont abordables et largement répandus ;
- compétences techniques minimes nécessaires, le plus souvent, pour utiliser les cybertechnologies ;
- progression de l'utilisation des cybertechnologies, ce qui favorise leur omniprésence quasi totale ;
- propagation rapide des données par le biais des cyber-réseaux ;
- facilité de copier des données qui font qu'elles sont presque impossibles à détruire ;
- dépendance du cyberespace à l'égard du spectre électromagnétique ;
- et discrétion du cyberespace[4].

Le cyberespace procure des avantages en termes de productivité et de mobilisation des pays développés et de ceux en développement. D'ailleurs les pays BRIC (Brésil, Russie, Inde et Chine, autrement dit les marchés émergents) doivent leur progression rapide à l'adoption et à l'utilisation efficace des cybertechnologies[5]. Dans les pays en développement, les téléphones portables (en particulier les smartphones avec leur connexion Internet) facilitent la connectivité entre les gens et ouvrent de nouvelles perspectives économiques[6]. Parmi les autres avantages, citons la diffusion sur une grande échelle d'informations qui favorisent, de manière générale, l'éducation, la bonne gouvernance, la prise de décisions ainsi que l'automatisation de différentes actions pénibles mais indispensables au fonctionnement quotidien des sociétés.

Ces technologies posent aussi certains problèmes. Si les cybertechnologies favorisent la connectivité, l'efficacité et la productivité, elles ont aussi un pouvoir destructeur considérable puisqu'elles font disparaître certains métiers et en créent de nouveaux. Ce changement radical de l'économie mondiale produit des vainqueurs et des perdants ce qui déclenche forcément des problèmes sociaux[7]. Les cybertechnologies sont également utilisées à des fins ignobles. Elles sont impliquées dans diverse opérations criminelles, y compris des activités de recrutement ou de financement pour des organisations terroristes. Comme elles sont présentes quasiment partout, qu'elles sont difficiles à percevoir et qu'elles sont toujours plus connectées aux systèmes indispensables aux activités sociétales quotidiennes, les cybertechnologies sont très vite devenues un moyen de voler, d'espionner voire d'attaquer des particuliers, des sociétés et des gouvernements[8].

Ces problèmes sont particulièrement inquiétants pour un nombre croissant d'États et font l'objet de discussions. Si tout le monde s'accorde à dire que le cyberespace offre de nombreux avantages, les cybertechnologies représentent une menace grave pour la sécurité nationale des États lorsqu'elles ne sont pas entre de bonnes mains et peuvent avoir des répercussions sur la sécurité internationale. Les cybermenaces proviennent d'individus doués dans le maniement des cybertechnologies, d'acteurs non étatiques et d'entités étatiques. Ces technologies peuvent être utilisées à des fins malveillantes : pour lancer des attaques par déni de service qui inondent de requêtes des sites de gouvernements ou de sociétés au point de les paralyser (il s'agit le plus souvent d'actes de contestation politique ou de vandalisme criminel), ou pour mettre au point et diffuser des logiciels malveillants qui s'en prennent à des processus et systèmes essentiels dans le but d'espionner ou de perturber ou détruire des réseaux informatiques. Le cas le plus célèbre est celui du virus Stuxnet qui aurait infecté le système de contrôle des centrifugeuses de la centrale nucléaire de Natanz, en Iran[9]. Parmi les autres menaces possibles, citons les bombes logiques introduites subrepticement dans des réseaux pour les perturber ou les détruire à un instant « t » ainsi que les opérations d'ingénierie sociale qui cherchent à accéder à des réseaux informatiques en exploitant les faiblesses psychologiques des utilisateurs.

Ces outils permettent d'espionner des particuliers, des sociétés, des entités étatiques ou non étatiques pour atteindre des systèmes exclusifs contenant des informations sensibles ou confidentielles ; ils sont également utilisés par des malfaiteurs pour subtiliser des biens virtuels. Ils servent à perturber des réseaux et des systèmes d'acquisition et de contrôle des données qui permettent un suivi et un contrôle automatisés de toutes les activités, qu'il s'agisse des processus de fabrication ou du fonctionnement des infrastructures modernes essentielles. Ces perturbations peuvent provoquer des dégâts matériels et avoir des conséquences catastrophiques[10].

Pour la plupart des pays développés (en particulier les pays occidentaux), les principales cybermenaces sont l'espionnage, les perturbations informatiques et la criminalité. La fiabilité et la sécurité des réseaux est, en général, la principale préoccupation, mais la véracité des informations transmises est également importante. Pour des États comme la Chine, la Fédération de Russie, l'Iran, la République arabe syrienne, la République populaire démocratique de Corée et d'autres (principalement des pays en développement), la fiabilité et la sécurité des réseaux sont également importantes. Ils jugent néanmoins tout aussi important le concept de sécurité de l'information insistant sur la véracité de l'information en fonction de sa convenance politique et culturelle et non pas uniquement en fonction de son origine et de sa non-altération. La sécurité de l'information est l'un des sujets les plus controversés des discussions de la communauté internationale sur le cyberespace. Cela n'est d'ailleurs pas près de changer vu les avis politiques et philosophiques diamétralement opposés qui existent[11].

Nous avons défini le cyberespace, décrit les principales menaces et indiqué le sujet le plus controversé du débat international sur le cyberespace. Nous allons voir maintenant comment

les pays développés et ceux en développement pourraient parvenir à comprendre leurs préoccupations respectives s'agissant du cyberpouvoir.

Parvenir à une compréhension mutuelle

En raison du cyberespace, les pays développés et ceux en développement ont des fragilités et des intérêts en commun. Ce devrait être une bonne raison de favoriser les discussions entre toutes les parties concernées. Il convient de préciser qu'une meilleure compréhension mutuelle des problèmes que pose le cyberpouvoir est certes appréciable mais ne dissipe en rien la méfiance et l'hostilité qui peut exister entre États. Seule une habileté politique acharnée sachant s'adapter au contexte pourra améliorer cette situation. Les questions abordées ci-dessous intéressent néanmoins tous les États et peuvent, malgré les divergences possibles, favoriser des discussions riches et fructueuses. Les échanges pourraient mettre en évidence des points de concorde plutôt que de discorde.

Le problème mentionné au début n'en demeure pas moins présent. Les grandes puissances, avec leurs experts sur la sécurité et spécialistes des questions de défense, dominent les discussions diplomatiques et les débats intellectuels sur la cybersécurité et les cyberconflits. Les préoccupations des pays en développement s'agissant du cyberpouvoir sont rarement abordées lors de ces discussions. L'on ne peut qu'émettre des hypothèses pour expliquer cette situation : le manque d'experts locaux sur les questions de cybersécurité, une conception de l'information comme un instrument pouvant représenter une menace sur le plan politique ou l'attribution de ressources humaines et financières limitées à d'autres problèmes plus urgents. Une autre raison plausible peut expliquer la faible participation des pays en développement dans les discussions sur les questions de cybersécurité : nombre d'entre eux préfèrent peut-être laisser les grandes puissances s'épuiser sur le sujet ; cette attitude n'est toutefois pas sans risque.

Au fond, peu importe les motifs de la faible participation des pays en développement. De nombreuses raisons impérieuses devraient encourager les pays développés et ceux en développement à mieux comprendre leurs positions respectives pour favoriser l'émergence de conditions propices à des avancées diplomatiques concrètes.

La quasi-omniprésence du cyberespace

Le cyberespace devient rapidement quasi omniprésent. Même dans les régions du monde ou les infrastructures modernes du cyberespace sont inexistantes ou d'une importance et complexité limitées, les gens utilisent de plus en plus les technologies de l'information et de la communication pour accroître et améliorer leurs relations sociales, économiques et politiques. En raison de leur faible coût et de leur abondance, les technologies de l'information et de la communication et celles des réseaux informatiques se diffusent rapidement dans toutes les régions du monde et cette tendance ne va faire que s'accentuer.

Par conséquent, tous les pays doivent surveiller la diffusion des cybertechnologies car celles-ci influencent fortement les interactions sociétales, le développement et l'activité économiques, le discours politique, la sécurité nationale et la gestion des affaires publiques. Attention, nous ne disons pas que les cybertechnologies changent la nature des choses mais qu'elles modifient la nature des interactions quotidiennes entre les gens et la façon dont les gouvernements revendiquent le pouvoir et la souveraineté. Les cybertechnologies qui favorisent une diffusion et une progression rapides des tendances sociales et culturelles peuvent faire de même pour les revendications sociales et politiques[12]. Par exemple, les réseaux sociaux n'ont pas été à l'origine des soulèvements qui débutèrent en Tunisie à la fin de l'année 2010 et gagnèrent le monde arabe, mais ils ont certainement joué un rôle, d'une part, en accélérant la prise de conscience et les échanges entre les manifestants et, d'autre part, en permettant à des services de sécurité habiles de se procurer des informations précieuses sur les manifestants. Ce phénomène a mis fin à la notion occidentale imaginant que le cyberespace était doté de vertus magiques en faveur de la démocratie capables d'entraîner la chute des régimes qui oppriment leurs peuples[13].

L'offre et la demande

La plupart des cybertechnologies sont inventées, mises au point et détenues par des États qui savent utiliser habilement les cybertechnologies. Ces derniers exercent, par conséquent, une influence considérable sur les normes techniques, les protocoles et le contrôle des avancées technologiques dans le domaine du cyberespace. Cela signifie que les États qui maîtrisent le mieux les cybertechnologies peuvent influencer les priorités diplomatiques et politiques concernant le cyberespace.

Face à cette situation, les pays en développement ne doivent pas penser qu'ils sont automatiquement exclus. Si les pays qui maîtrisent les cybertechnologies en détiennent l'exclusivité et influencent les normes et protocoles utilisés, ils cherchent aussi à vendre leurs cybertechnologies au marché mondial. Les pays en développement représentent une part importante de ce marché mondial et influencent, d'une certaine manière, les technologies qui sont achetées et la façon dont elles sont utilisées en adoptant et imposant des lois pour réglementer le cyberespace à l'intérieur du territoire relevant de leur souveraineté ou en empêchant leurs citoyens d'accéder à des informations disponibles en ligne et jugées inopportunes. Ce dernier cas de figure rappelle la controverse sur la sécurité de l'information mentionnée plus haut. La plupart des régimes autoritaires ne maîtrisent pas parfaitement les cybertechnologies. Ils n'ont pas les connaissances ni les capacités industrielles nécessaires pour mettre au point et fabriquer leurs propres cybertechnologies. Ces régimes peuvent toutefois acheter des logiciels et technologies pour savoir qui accède à des informations « inopportunes » en ligne et pour bloquer l'accès à ces informations. Il est toutefois paradoxal de constater que de nombreuses technologies de censure sont mises au point et vendues par des entreprises de pays développés, démocratiques et libéraux[14].

Les pays développés détiennent le quasi-monopole de la conception, de la mise au point et de la propriété des cybertechnologies, mais ils effectuent la plupart de leurs activités de fabrication et d'assemblage dans des pays en développement car la main-d'œuvre y est moins chère et les réglementations sur le travail et la protection de l'environnement y sont plus souples. En outre, les métaux des terres rares utilisés pour fabriquer les cybertechnologies se trouvent surtout dans les pays en développement.

En raison des liens existant entre eux au niveau de l'offre et de la demande, les pays développés et les pays en développement ont intérêt à soutenir des discussions sérieuses sur le cyberpouvoir.

Asymétrie et fragilité

Les pays en développement sont presque aussi exposés au risque de cyberperturbations que les pays développés, considérés aujourd'hui comme très dépendants des cybertechnologies. Cette situation s'explique par la quasi-omniprésence des cybertechnologies et par l'utilisation croissante de ces technologies pour contrôler des processus et systèmes indispensables au fonctionnement quotidien des sociétés, y compris dans les pays en développement.

Par exemple, la progression des villes dites « bien aménagées » dans le monde en développement, assortie à l'urbanisation d'environ 70 % de la population mondiale d'ici 2050[15], signifie que les pays en développement seront de plus en plus exposés au risque de cyberperturbations. Au début, ces bouleversements n'auront peut-être pas de conséquences catastrophiques, mais plus les systèmes et processus essentiels seront automatisés à l'aide de cybertechnologies plus les conséquences de ces perturbations risqueront d'être graves[16]. Les pays en développement doivent impérativement s'impliquer davantage dans les discussions internationales sur la cybersécurité et les cyberconflits s'ils veulent limiter les conséquences les plus néfastes de ces cyberperturbations.

Il ne faut pas oublier non plus que de nombreux États envisagent la cyberguerre comme un moyen de se procurer un avantage asymétrique face à des adversaires militairement plus puissants. Certains pays en développement peuvent être tentés de se doter de capacités de cyberguerre et craindre d'être victimes d'une cyberguerre. Malgré quelques cyber-attaques isolées (contre l'Estonie en 2007 et la Géorgie en 2008), l'on sait peu de choses sur l'ampleur et les limites des logiques de cyberguerre entre adversaires. Si les conséquences d'une cyberguerre font l'objet de multiples spéculations, elles sont en réalité inconnues. Le premier à se lancer dans un affrontement de ce genre s'expose à des risques susceptibles de se retourner contre tous les acteurs impliqués[17].

Il ne faut pas oublier non plus que la cyberguerre pourrait ne pas procurer l'avantage asymétrique que certains semblent espérer. Les cyber-attaques lancées contre des infrastructures essentielles ou des réseaux de contrôle et de commandement peuvent avoir certains effets mais il est peu probable qu'elles conduisent à une reddition immédiate de

l'adversaire. Au lieu de capituler, un adversaire pourrait bien opter pour une escalade avec des moyens d'attaque utilisant la force cinétique. Une riposte n'utilisant que des cybertechnologies est très improbable lorsque la nature de la guerre tend à l'escalade vers les extrêmes. Il est, peut-être, plus exact de parler d'utilisation des cybertechnologies dans la guerre ; ceux qui cherchent à en faire leur principale arme de guerre risquent de s'apercevoir que le résultat ne sera probablement pas en leur faveur[18].

Aujourd'hui, la plupart des pays développés contrôlent les systèmes et processus complexes indispensables au fonctionnement quotidien de leur société grâce aux cybertechnologies ; le fonctionnement de ces pays, de leur économie et, partant, de leur sécurité nationale repose sur l'interconnectivité que permet le cyberpouvoir.

Si le cyberespace est quasi omniprésent dans les pays en développement, il est tout à fait plausible de dire que c'est déjà le cas dans les pays développés. L'être humain ne viendrait pas à disparaître si des pannes catastrophiques frappaient soudainement l'ensemble du cyberespace, mais la vie serait difficile pour les sociétés touchées. Aujourd'hui, le cyberespace joue un rôle critique dans tous les domaines, des transactions financières aux télécommunications en passant par les infrastructures essentielles et les forces militaires modernes. Ce cyberpouvoir confère des avantages considérables à ceux qui l'utilisent mais est à l'origine de faiblesses extrêmes qui peuvent avoir des conséquences désastreuses si elles sont exploitées.

Pour les pays développés qui dépendent des cybertechnologies, la menace la plus dangereuse vient d'autres pays cyberdépendants. Ces derniers ont, en effet, plus de chance d'avoir des capacités et talents techniques que les pays en développement ayant des moyens plus limités. Un pays en développement croyant détenir un avantage asymétrique lui permettant de paralyser un adversaire plus avancé pourrait surprendre un État développé cyberdépendant en lançant à point nommé quelques cyber-attaques bien ciblées. Si un tel scénario est peu probable, il n'en reste pas moins possible. Par conséquent, les pays développés cyberdépendants devraient engager des discussions avec les pays en développement sur les questions de cybersécurité s'ils veulent se protéger contre de mauvaises surprises et trouver comment juguler les cybermenaces.

Il faut absolument encourager les discussions sur le cyberpouvoir pour que tous les États comprennent bien les risques que représente l'utilisation des cybertechnologies dans la guerre, qu'ils sachent ce que leurs adversaires considèrent comme les « lignes à ne pas franchir » et qu'ils puissent prendre des mesures adaptées en cas de cyber-attaque.

Les acteurs non étatiques

Le fait que la criminalité organisée et les organisations terroristes utilisent de plus en plus les technologies comme celles du cyberpouvoir devrait être un sujet de grave préoccupation pour tous les États. Ces organisations commettent des actes criminels qui affectent la vie des citoyens, le droit et même la sécurité nationale ; leurs actes peuvent aller jusqu'à

compromettre la viabilité et la légitimité d'États souverains. Les organisations criminelles maîtrisent particulièrement bien le cyberpouvoir et utilisent des technologies avancées, y compris à des fins ignobles. Quant aux organisations terroristes, elles ont, jusqu'à présent, utilisé le cyberpouvoir uniquement pour des activités de recrutement et de financement. Avec la marchandisation croissante de cybercapacités de pointe (mises au point et vendues dans de nombreux cas par des organisations criminelles), il existe un réel danger de voir les terroristes utiliser de plus en plus le cyberpouvoir. Ils pourraient ainsi attaquer à maintes reprises des infrastructures essentielles dans le but d'accabler un gouvernement au point de lui faire perdre toute légitimité aux yeux du peuple ou lancer des cybercampagnes sophistiquées de propagande ou d'ingénierie sociale pour suborner des personnes influentes ou de hauts fonctionnaires. Certains États risquent de faire appel à des acteurs non étatiques pour lancer des cyber-attaques qu'ils pourront nier avoir initiées.

Les pays développés et ceux en développement ont tout intérêt à discuter sérieusement des problèmes que posent les acteurs non étatiques utilisant les cybertechnologies. Certaines avancées ont été enregistrées dans le domaine de la cybercriminalité avec la Convention sur la cybercriminalité rédigée par le Conseil de l'Europe et qui est entrée en vigueur en 2004. Des différends persistent néanmoins car certains États ont invoqué le prétexte de la cybercriminalité et du cyberterrorisme pour réprimer ce qui est considéré par beaucoup comme des contestations politiques légitimes.

Vous ne vous intéressez peut-être pas au cyberpouvoir...

mais le cyberpouvoir s'intéresse à vous. Autrement dit, si les arguments que nous venons d'évoquer ne sont pas suffisamment convaincants, les responsables politiques ne doivent pas oublier que s'ils ne voient pas l'intérêt de s'entendre, au niveau mondial, sur les questions touchant au cyberpouvoir, le cyberpouvoir s'intéresse beaucoup à eux. Les États qui ne participent pas aux discussions sur le cyberpouvoir risquent d'être démunis s'ils devaient être attaqués par des acteurs ayant compris l'utilité stratégique du cyberpouvoir mais n'ayant pas forcément conscience de toutes les conséquences de son utilisation.

Conclusion

Les capacités du cyberpouvoir se diffusent rapidement dans le monde avec des conséquences souvent bouleversantes pour la société, l'économie et la sécurité nationale. Le fait que les pays en développement ne s'impliquent pas vraiment dans les discussions diplomatiques ou autres organisées au niveau mondial sur les questions que pose le cyberpouvoir est un motif de préoccupation pour tous. Il faut tout faire pour parvenir à une compréhension mutuelle indispensable s'agissant du cyberpouvoir, ce qu'il annonce et comment il peut être utilisé pour le bien de tous. Nous avons présenté cinq sujets qui devraient préoccuper les pays développés comme ceux en développement ; ils devraient constituer un point de départ intéressant pour réduire cet écart, qui nous semble dangereux, s'agissant de la mobilisation des États.

Notes

1. D. Kuehl, « From Cyberspace to Cyberpower: Defining the Problem », *in* F. Kramer, S. Starr et L. Wentz (sous la direction de), *Cyberpower and National Security*, 2009, p. 28.
2. Ibid., p. 38.
3. Voir le chapitre « Information Power: Strategy, Geopolitics and the Fifth Dimension », *in* D. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, 2004, p. 179 à 200. S'agissant de l'importance cruciale des informations pour les activités humaines, voir J. Gleick, *The Information: A History, a Theory, a Flood*, 2011.
4. J. Sheldon, « Deciphering Cyberpower: Strategic Purpose in Peace and War », *Strategic Studies Quarterly*, vol. 5, n° 2, 2011, p. 95 à 112.
5. J. O'Neill, *The Growth Map: Economic Opportunity in the BRICs and Beyond*, 2011.
6. Pour plus d'informations, voir Union internationale des télécommunications, *Confronting the Crisis: Its Impact on the ICT Industry*, 2009, p. 75.
7. Voir E. Brynjolfsson et A. McAfee, *Race Against the Machine*, 2011.
8. Pour une synthèse complète, mais quelque peu centrée sur la position des États-Unis, voir R. Clarke et R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 2010 ; et J. Carr, *Inside Cyber Warfare*, 2010.
9. J. Sheldon, « Stuxnet and Cyberpower in War », *World Politics Review*, 2011.
10. Sur les différentes méthodes d'exploitation du cyberespace, voir J. Carr, *Inside Cyber Warfare*, 2010.
11. Assemblée générale, *Lettre datée du 12 septembre 2001, adressée au Secrétaire général par les Représentants permanents de la Chine, de la Fédération de Russie, de l'Ouzbékistan et du Tadjikistan*, document des Nations Unies A/66/359, 14 septembre 2011, p. 3 à 5.
12. Voir C. Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations*, 2008.
13. Evgeny Morozov dénonce à temps et de manière utile ce qu'il appelle le « cyber-utopisme », *in* E. Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, 2011.
14. Voir I. Poetranto, « Behind Blue Coat: Investigations of Commercial Filtering in Syria and Burma », posté le 9 novembre 2011, The Citizen Lab.
15. Assemblée générale, *Application des décisions prises par la Conférence des Nations Unies sur les établissements humains (Habitat II) et renforcement du Programme des Nations Unies pour les établissements humains(ONU-Habitat), Rapport du Secrétaire général*, document des Nations Unies A/65/316, 20 août 2010, p. 4.
16. Pour plus d'informations, voir S. Smith, « Code is Culture », *Discontinuities*, posté le 15 juin 2011, Current Intelligence.
17. C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*, 2011.
18. J. Sheldon, « Deciphering Cyberpower: Strategic Purpose in Peace and War », *Strategic Studies Quarterly*, vol. 5, n° 2, 2011, p. 95 à 112.

Pour une confiance accrue et une entente internationale sur la cybersécurité

James Andrew Lewis

Le réseau numérique mondial est devenu l'épine dorsale de l'économie mondiale et représente une nouvelle voie d'attaque, mais les négociations ont peu progressé sur la question plus large de la sécurité internationale. La sécurité du cyberespace est devenue un enjeu vital pour tous les États. Ces derniers considèrent les activités malveillantes dans le cyberespace comme une menace pour leur sécurité et ils craignent, qu'elles ne déclenchent, suite à une erreur d'appréciation, des conflits militaires destructeurs. Tout cela génère une grande pression internationale en faveur d'un accord multilatéral, mais les discussions n'en sont qu'au premier stade.

La plupart des armées avancées disposent de capacités pour lancer des cyber-attaques et de nombreuses autres sont en train de s'en doter. Les cybercapacités sont tout simplement un autre moyen d'attaque ; à l'instar des missiles ou des avions, elles peuvent frapper l'ennemi à grande distance. Comme les avions ou les missiles à longue portée, elles peuvent lancer des attaques à des fins tactiques ou stratégiques. Les cyber-attaques ne seront pas déterminantes, elles ne décideront pas de l'issue d'un conflit, surtout lorsqu'elles viseront un adversaire puissant, mais du fait de l'avantage militaire qu'elles représentent, elles seront utilisées. La question de savoir quand et comment elles seront utilisées peut encore être influencée par des négociations internationales. Reste à voir comment cette nouvelle dimension de la guerre s'inscrit dans le cadre régissant les conflits interétatiques et à déterminer quelles modifications et accords s'imposent pour mieux gérer les risques et les conflits.

Un rapport publié en juin 2011 par l'UNIDIR, élaboré sur la base d'informations provenant de sources librement accessibles, a passé en revue les politiques et les organisations de 133 États et constaté que la cyberguerre figure dans l'organisation et la planification militaires de 33 États[1]. Il peut s'agir d'États ayant une doctrine très poussée et dont les organisations militaires emploient des centaines voire des milliers de personnes ou d'États ayant des systèmes plus simples intégrant les cyber-attaques et la cyberguerre dans leurs capacités de guerre électronique.

Ces doctrines militaires envisagent toutes le recours aux cybercapacités pour effectuer des missions de reconnaissance ou des opérations d'informations, pour perturber des services et des réseaux essentiels, pour mener des cyber-attaques ou pour compléter une guerre électronique ou des opérations d'informations. Certains États prévoient des plans spécifiques

---

James Andrew Lewis est *senior fellow* et directeur de programme au Centre d'études stratégiques et internationales (CSIS). Auparavant, il avait été agent du service extérieur pour le Département d'État et le Département du commerce et membre du Senior Executive Service. Il fut le rapporteur du Groupe d'experts gouvernementaux des Nations Unies sur la sécurité de l'information en 2010. Ses travaux de recherche actuels examinent la concurrence stratégique et l'innovation technologique. Il a obtenu son doctorat à l'Université de Chicago.

pour des opérations politiques ou d'informations. Les cyber-attaques combinent les techniques et tactiques de la guerre électronique et le renseignement d'origine électromagnétique. Une cyber-attaque cherche à perturber le commandement et le contrôle de l'adversaire ; pour accentuer le « brouillard de la guerre » clausewitzien, elle crée une incertitude, endommage des données et entrave les communications. Un adversaire habile pourrait endommager ou détruire des infrastructures essentielles. À l'heure actuelle, seules quelques « cyberpuissances » sont en mesure d'envoyer par Internet des commandes pouvant provoquer des destructions matérielles. Une trentaine d'États travaillent à la mise au point de telles capacités et des acteurs non étatiques s'en doteront lorsque les techniques et outils nécessaires seront facilement disponibles.

L'utilisation militaire des cyber-attaques n'est pas le problème le plus urgent pour la sécurité internationale mais il est lié à d'autres comportements malveillants et constitue, d'une certaine façon, le sujet le plus propice pour parvenir à un accord, en raison des nombreux précédents en sécurité internationale. Les problèmes les plus difficiles sont le recours aux cybertechniques pour des activités de renseignement et les rapports avec les acteurs non étatiques. Ces deux sujets relevant de la compétence des États (même si le rapport n'est pas clairement établi), des mesures et normes peuvent être définies pour limiter les risques. L'efficacité des normes peut être améliorée grâce à des mesures de confiance ; ces dispositions prises par les États permettent d'éviter ou de limiter les ambiguïtés, le doute et la méfiance et d'améliorer la coopération internationale. Des normes et des mesures de confiance visant à accroître la stabilité au niveau de l'utilisation militaire du cyberespace pourraient réduire les craintes de nombreux États s'agissant des risques de cyberguerre. Une convergence de vues des États concernant les cyberconflits augmente les chances de dissuader des actions malveillantes et favorise une communication tacite en cas de conflit. Parvenir à une convergence des positions faciliterait la lutte contre les cyberconflits.

Les gouvernements s'accordent à reconnaître qu'ils n'ont pas vraiment de prise sur le risque de cyberconflit qui s'est aggravé de façon dramatique. Cette évolution explique la multiplication des stratégies nationales sur la question. Ainsi, plus de 70 États se sont dotés de plans et d'organisations pour limiter les risques. Ils sont aujourd'hui prêts à appréhender le problème de la cybersécurité internationale comme une question pouvant être gérée par les États avec des instruments ayant fait leur preuve dans des négociations. Reste qu'il n'est pas facile de passer d'une crainte partagée à des mesures concrètes. Le risque de cyberguerre n'est considéré que depuis peu comme un sujet de discussions internationales alors que les médias évoquent depuis plus d'une décennie des hypothèses catastrophiques. Avant 2000, seuls quelques États avaient commencé à mettre au point des capacités d'attaque. Les dommages envisageables étaient limités et ces programmes militaires étaient ultraconfidentiels. Il existait un contraste frappant entre ces activités et les discussions internationales sur la gouvernance de l'Internet qui étaient très animées. Cette différence reflétait le manque d'expérience de la communauté d'Internet et son incapacité à percevoir les risques potentiels pour les intérêts nationaux.

Les discussions sur un accord international visant à limiter les risques de cyberconflit débutèrent dans les années 90, mais elles s'engagèrent mal en se focalisant sur l'idée d'un traité pour favoriser la sécurité et la stabilité. Des spécialistes proposèrent des instruments juridiques complexes inspirés du Pacte Briand-Kellogg des années 20 dans lequel les États renonçaient à la guerre en tant qu'instrument de politique. Dans les années 90, le Gouvernement russe soumit aux Nations Unies un projet de traité. L'examen de cette proposition, qui devait se répéter les années suivantes, ne fit jamais consensus. Si l'idée d'un traité est soutenue par l'Assemblée générale, elle n'a jamais progressé en raison de la très vive opposition de quelques pays occidentaux. Les projets de traités n'étaient de toute façon pas applicables. Quelles mesures pourrait prendre un État en cas de non-respect du traité ou d'incertitudes concernant la vérification des cybercapacités ? Il est irréaliste d'envisager des engagements contraignants pour éviter toute attaque ou action hostile dans le cyberespace tout simplement parce qu'il est peu probable que des adversaires éventuels les respectent. Si la question des définitions n'a pas été réglée, c'est probablement parce qu'elle est insoluble. Rien ne sert d'interdire les « armes de l'information » si ce concept n'est pas défini ; d'ailleurs, les initiatives visant à définir les « cyber-armes » se sont vite heurté au problème que représentent la disponibilité et la grande utilisation des technologies de l'information.

Si un traité sur le cyberespace ne fonctionnerait pas, il en est de même pour une simple extension du droit des conflits armés au cyberespace. Il existe de nombreuses ambiguïtés y compris sur l'ampleur et la nature des dommages à partir desquelles une cyber-attaque peut être considérée comme un recours à la force (une condition indispensable pour agir en droit international). Certaines cyber-attaques risquent de ne pas respecter les principes du droit international humanitaire utilisés pour déterminer des cibles légitimes, à savoir les principes de distinction, de proportionnalité et de discrimination. Si des mesures ont déjà été prises par le passé pour lever ces ambiguïtés, il existe aujourd'hui un risque accru de voir des cyber-actions être mal interprétées. Les États craignent que cette situation ne dégénère et n'aboutisse à un conflit destructeur.

Ces problèmes pèsent toujours sur les discussions internationales sur la cybersécurité. La situation s'améliore toutefois depuis quelques années. La communauté d'Internet et ses organisations affiliées restent inadaptées pour examiner le problème des cyberconflits sous l'angle de la sécurité internationale alors que des organismes militaires et diplomatiques de plusieurs États ont identifié la cybersécurité comme un enjeu crucial. Ils ont compris, en effet, que les réseaux mondiaux à haut débit du cyberespace sont indispensables à leur prospérité économique et à leur sécurité nationale mais qu'ils représentent aussi un risque. La communauté internationale avance peu à peu dans ses discussions sur la portée, la nature et les contraintes de la cyberguerre.

D'autres pistes qu'un traité furent envisagées dès 2008. Rejetant l'idée d'un traité en bonne et due forme, ces options se fondaient sur les initiatives mondiales de lutte contre la prolifération pour concevoir un modèle pouvant être appliqué à la cybersécurité. Elles ne proposaient

pas un engagement juridiquement contraignant mais demandaient aux États d'élaborer des normes pour une conduite responsable des États dans le cyberespace. Le domaine de la non-prolifération fourmille d'exemples de normes non contraignantes qui influencent fortement la conduite des États.

Les normes exercent non seulement une influence sur les comportements mais limitent aussi l'ampleur des conflits. Elles suscitent des attentes et favorisent entre les États une concordance de vues en matière de comportement international ; elles favorisent ainsi une certaine prévisibilité des interactions aux niveaux des questions économiques et politiques et de celles de sécurité. Dans ce contexte, la cybersécurité devient la capacité des États à protéger leur souveraineté nationale et à défendre leurs intérêts nationaux. La cybersécurité représente de nouveaux défis pour la sécurité internationale : il existe une interdépendance croissante entre les États et la perception d'un risque « transnational » progresse. La cybersécurité est toutefois un élément encore relativement peu défini des relations entre États.

L'approche axée sur des normes suscite un intérêt grandissant au sein de la communauté internationale ; comme dans le domaine de la non-prolifération, l'adoption de normes sur une grande échelle ouvrirait la voie à de nouveaux accords formels. En juillet 2010, un groupe d'experts gouvernementaux créé par le Secrétaire général de l'ONU établit un rapport sur les progrès de la téléinformatique dans le contexte de la sécurité internationale. C'était une première. L'idée d'un traité envisagée à une époque n'avait pas fait l'objet d'un consensus et un précédent groupe d'experts gouvernementaux, créé en 2004, n'avait pas réussi à s'entendre sur un rapport. Il convient toutefois de préciser que le rapport de 2010 ne compte que 1 400 mots. À titre de comparaison, le premier groupe d'experts gouvernementaux aurait produit des projets longs et circonstanciés qui ne purent faire l'objet d'un consensus. La concision du rapport de 2010 explique, en partie, son succès (et c'est une indication utile pour de futurs groupes d'experts gouvernementaux sur la cybersécurité), mais la concision est aussi le reflet de problèmes plus graves qui freinent l'émergence d'un consensus international.

Les résultats obtenus en 2010 par le Groupe d'experts gouvernementaux s'expliquent par l'entente qui existait au sein de ce groupe. Pour ces experts, les cyberconflits représentaient une menace grave pour la paix et la stabilité internationales et l'absence d'accord international risquait d'accroître le risque d'un cyber-incident pouvant dégénérer et conduire à un conflit plus ravageur. Les États représentés dans le Groupe d'experts gouvernementaux craignaient qu'une cyberguerre effrénée n'aboutisse à des violences physiques. Selon eux, envisager des normes et règles pour le recours à la force dans le cyberespace, ainsi que d'autres mesures de confiance, permettrait d'améliorer la sécurité internationale et la stabilité du cyberespace et du système international.

Le Groupe d'experts gouvernementaux eut du mal à s'entendre même sur un rapport limité. Il convient de noter que les récits des médias et de milieux académiques disponibles sur les travaux du Groupe d'experts gouvernementaux de 2010 ont, pour la plupart, passé sous silence les divergences de vues entre les différents membres de ce Groupe. Si les experts s'accordaient

à dire que la cybermenace progressait, ils s'entendaient sur peu d'autres points. Certains États jugent les lois et normes internationales existantes inadaptées face au risque de cyberconflit. D'autres pensent, au contraire, que le droit des conflits armés est suffisant pour traiter des questions de cybersécurité et craignent de prendre des mesures qui sembleraient limiter la liberté d'expression. Comme souvent lors de discussions multilatérales, toute la question est de voir si les États sont prêts à renoncer à une partie de leur souveraineté pour accroître leur sécurité.

Ces divergences de vues n'étaient pas futiles ; elles traduisaient de profonds désaccords concernant la façon d'envisager un accord international, la question du recours à la force, les normes s'appliquant à la conduite des États et les facteurs de risque dans le cyberespace. Compte tenu de ces divergences, les membres du Groupe d'experts gouvernementaux de 2010 réussirent à s'entendre sur cinq recommandations générales :

> i) Poursuivre la concertation entre États sur des normes éventuelles relatives à l'utilisation des TIC [technologies de l'information et des communications] par les États, afin de réduire le risque collectif et de protéger les infrastructures nationales et internationales essentielles ;
>
> ii) Adopter des mesures de confiance, de stabilité et de réduction des risques qui répondent aux conséquences de l'utilisation des TIC par les États, avec notamment des échanges de vues entre pays sur l'utilisation des TIC dans les conflits ;
>
> iii) Échanger des informations sur les législations nationales et les stratégies de sécurité nationales relatives aux technologies de l'information et des communications, ainsi que sur les techniques, les politiques et les meilleures pratiques ;
>
> iv) Définir des moyens d'aider les pays moins développés à renforcer leurs capacités ;
>
> v) Mettre en évidence les possibilités d'élaborer des modalités et des définitions communes procédant de la résolution 64/25 de l'Assemblée générale[2].

Ces premières initiatives sont intéressantes. L'adoption par consensus, en 2010, du rapport du Groupe d'experts gouvernementaux incita la Fédération de Russie à proposer, quelques mois plus tard, à la Première Commission de l'Assemblée générale des Nations Unies de constituer un nouveau groupe d'experts gouvernementaux pour poursuivre les travaux engagés. Un nouveau groupe doit se réunir en août 2012. Les discussions de mesures de confiance se heurtent toutefois à d'autres difficultés. Reprendre des mesures utilisées dans d'autres domaines n'est pas aussi simple ne serait-ce qu'en raison de la très grande diffusion des technologies utilisées dans les cyberconflits. Le secret qui entoure les cyber-activités des États – un reliquat des opérations de renseignement d'origine électromagnétique – ralentit tout échange d'informations. Des malentendus sur la nature du cyberconflit freinent les discussions, comme l'illustrent les fréquentes analogies avec les questions nucléaires généralement inadaptées

à la cyberguerre. Les descriptions de cyberconflits publiées dans des documents librement accessibles sont généralement imprécises. Le grand secret entourant les activités des États et de mauvaises méthodologies de recherche compliquent l'élaboration de politiques.

Malgré l'entente sur l'idée d'une stratégie axée sur des normes et sur la nécessité pour la sécurité internationale d'adopter des mesures de confiance et des normes pour les cyber-activités, peu de propositions précises ont été formulées pour lier la cybersécurité au « système » plus large de sécurité internationale. Reste à fixer un objectif final pour la coopération internationale en matière de cybersécurité ainsi que la route à suivre pour l'atteindre. Si le but est d'influencer la conduite des États en instaurant un cadre mondial pour la cybersécurité, de nombreuses étapes intermédiaires doivent encore être définies. Les discussions internationales devront commencer par examiner des mesures pour renforcer la confiance.

Certains États jugent le terme « cybersécurité » inapproprié. Ils pensent que le sujet est la « sécurité de l'information ». Ils estiment que l'information est une arme et que le droit des conflits armés n'est pas adapté à cette nouvelle menace qui pèse sur la paix internationale. Ils ont présenté, dans le cadre de l'Organisation de coopération de Shanghai, un projet de code de conduite sur la sécurité de l'information pour orienter les discussions du prochain groupe d'experts gouvernementaux en combinant des objectifs comme la coopération accrue des services de répression et leurs préoccupations en matière d'accès à l'information. Pour les auteurs de ce code de conduite, le meilleur moyen de renforcer la stabilité et la sécurité est de donner aux États le contrôle souverain de l'infosphère et de renoncer à la menace ou à l'emploi de la force dans le cyberespace.

Le prochain groupe d'experts gouvernementaux aura pour défi principal de transformer les recommandations de 2010 en mesures concrètes sur lesquelles la communauté internationale pourra s'entendre afin de limiter les conséquences d'un conflit dans le cyberespace. Pour y parvenir, les experts devront tenir compte des questions de fond et de considérations politiques pour déterminer les possibilités de coopération et les restrictions envisageables. Une convergence de vues sur un certain nombre de questions est indispensable et notamment sur les points suivants : la façon dont le droit de la guerre s'applique aux cyberconflits, les caractéristiques de l'escalade d'un cyberconflit et les responsabilités des États avant et pendant un cyberconflit. Avec une position commune des États sur ces sujets, il serait plus facile de mettre en place un cadre international pour faire obstacle aux cyberconflits et de définir les conséquences éventuelles de différents niveaux d'actes hostiles. Tous ces sujets soulèvent des interrogations et les principaux États en font une analyse très différente.

Difficultés

Il faudra trouver comment surmonter les principales divergences de vues. Il n'existe pas de consensus sur ce qui constitue un cyberconflit, et notamment le seuil critique de ce qui, dans le cyberespace, peut être considéré comme un recours à la force et justifier une riposte par la

force. Peut-être plus important encore, les États ne sont pas d'accord sur les responsabilités qui sont les leurs dans le cyberespace. Cette situation est instable.

Elle s'explique par des évaluations différentes de ce qui représente une menace. Pour certains États, l'information est une arme et représente au même titre que le piratage informatique un élément de la cyberguerre. Les responsables d'État qui considèrent l'information comme une arme pouvant être utilisée contre leur pays doivent être pris au sérieux. Ils estiment que la liberté d'accès à l'information constitue une menace pour la stabilité et la survie de leur régime. Le fait que cette menace ne soit pas délibérément (ni constamment) dirigée contre leur pays ne diminue en rien le danger.

Le traitement de l'information est directement lié à la question de savoir comment les États étendront leur contrôle souverain dans le cyberespace. Le modèle actuel de gouvernance, qui repose sur un ensemble d'acteurs présents dans diverses institutions fragiles ne convient pas pour assurer la stabilité et la sécurité d'une infrastructure mondiale cruciale. De nombreux gouvernements, jugeant la situation actuelle intolérable, tentent de voir où ils pourraient intervenir davantage pour réduire les risques que représente une mauvaise gestion d'Internet pour l'économie, la sécurité publique et la sécurité nationale. Les États vont étendre leur contrôle dans le cyberespace pour protéger leurs intérêts nationaux. En raison de cette agitation autour de la gouvernance de l'Internet, il sera difficile de s'entendre sur des normes pour la cybersécurité internationale.

La façon de régler les difficultés auxquelles se heurte la cybersécurité suscite des vues très diverses. Il reste encore de nombreuses incertitudes concernant notamment le type d'accords nécessaire (implicite ou explicite), la forme de ces instruments, leur portée et les cadres où ils seront négociés. Les cyber-activités sont considérées comme une activité militaire légitime mais aucun accord n'a été trouvé sur les règles qui devraient s'appliquer à ces activités. Il existe un lien ambigu entre la cyberguerre et l'espionnage. Cette ambiguïté augmente le risque d'erreur d'appréciation ou celui d'escalade d'un cyberconflit car il n'existe qu'une différence ténue entre l'intrusion dans un ordinateur à des fins d'espionnage et celle effectuée pour lancer une attaque.

L'ambiguïté touche des domaines clefs comme l'applicabilité du droit des conflits armés aux cyberconflits, la souveraineté des tiers, et l'ampleur et la nature des dommages à partir desquelles une cyber-attaque peut être considérée comme un recours à la force. Certaines questions ne sont pas claires et notamment celle concernant le degré d'évaluation préalable nécessaire pour respecter, en droit international, les principes de distinction, de proportionnalité et de discrimination pour déterminer des cibles légitimes. Pour l'heure, peu de précédents permettent de lever ces ambiguïtés. Un nouveau groupe d'experts gouvernementaux pourrait les examiner mais il n'est pas conseillé de chercher à les régler vu le peu de chances d'aboutir à un accord pour l'instant.

Les obstacles qui gênent la conclusion d' un accord multilatéral

La très grande utilité des cyber-actions va influencer tout accord international sur la cybersécurité. Les États ne vont pas renoncer à ce nouvel outil. Les cyber-attaques ne coûtent pas cher et offrent un avantage stratégique. Les États ne peuvent renoncer aux infrastructures numériques ni aux cyber-attaques car, dans une guerre, les informations leur procurent une supériorité précieuse et leur permettent d'obtenir un réel avantage militaire. Les technologies nécessaires sont disponibles dans le commerce ou peuvent être facilement élaborées à partir de produits largement commercialisés comme des ordinateurs portables, des programmes informatiques ou des connexions Internet. Il est impossible de contrôler les « précurseurs » de ces « armes ». Ils sont petits, ne coûtent pas cher, peuvent être facilement dissimulés et sont faciles à concevoir pour des programmateurs ingénieux travaillant ou non pour des gouvernements. Les outils nécessaires pour lancer des cyber-attaques sont facilement disponibles sur le marché noir de la cybercriminalité qui est en plein expansion. Il est peu probable qu'un État renonce aux cyber-attaques.

Un traité interdisant de s'en prendre à certaines cibles avec des cyber-attaques serait absurde. Le droit de la guerre définit déjà des garanties et limite (mais n'interdit pas) les attaques contre des cibles civiles. Nous ne pouvons espérer plus pour le cyberespace. Les États pourraient s'inspirer du domaine de la non-prolifération et établir des normes multilatérales définissant une conduite responsable. La norme la plus élémentaire consisterait à étendre le droit existant et la pratique pour considérer qu'un État est responsable du comportement de ceux qui se trouvent sur son territoire – une telle décision empêcherait l'intervention d'intermédiaires ou de pirates informatiques invoquant des raisons « patriotiques ».

De plus, le cyberespace a été une véritable aubaine pour l'espionnage. Ce lien étroit avec l'espionnage explique la réticence des États à discuter et même à reconnaître qu'ils possèdent des cybercapacités et à accepter d'interdire le recours en premier à celles-ci. En prenant un engagement de non-recours en premier, les États pourraient avoir à renoncer au cyber-espionnage – ce qu'ils ne sont pas prêts à accepter. Les techniques d'attaque et d'espionnage étant similaires, exiger des États qu'ils s'engagent à ne pas mettre au point et à ne pas utiliser de tels outils pour s'introduire dans les réseaux de leurs ennemis revient à leur demander de ne pas espionner. L'engagement de « non-recours en premier » pourrait même avoir des conséquences déstabilisantes si un État venait à prendre pour une attaque des activités de cyber-espionnage.

Puisqu'il semble difficile de déterminer qui est responsable d'une attaque, certains États risquent de penser qu'ils peuvent mener des cyber-actions secrètes et ne pas être reconnus responsables de celles-ci. Une attaque secrète ne révélant pas l'identité de l'agresseur présente beaucoup moins de risque politique. En outre, des mercenaires (généralement des cybercriminels recrutés par un État) peuvent lancer des attaques complexes que l'État niera ensuite avoir lancées. La difficulté d'imputer la responsabilité d'une attaque est souvent

exagérée. Les techniques d'analyse scientifique ou de renseignement permettent de plus en plus souvent de déterminer qui sont les auteurs. Il n'en reste pas moins que l'impression qu'il est difficile d'imputer la responsabilité d'une attaque augmente la tentation d'avoir recours à de telles opérations.

Par conséquent, les initiatives visant à limiter les cyber-attaques par un accord multilatéral fixant des contraintes technologiques risquent de se heurter à des difficultés potentiellement insurmontables. Les cyber-attaques représentent plus un comportement qu'une technologie. Les cyberconflits sont influencés par le secret, la facilité d'acquisition et l'incertitude. Il est impossible d'envisager de réduire le risque que représentent les cyber-attaques pour la sécurité internationale au moyen d'une convention juridiquement contraignante basée sur l'engagement de ne pas recourir à de telles méthodes, la limitation des technologies et la vérification du respect d'une telle convention. Il semble difficilement réalisable de conclure un instrument général de cybersécurité pour régler l'ensemble des problèmes auxquels est confrontée la cybersécurité.

Une stratégie progressive

La volonté de réduire les risques d'erreur d'interprétation, d'escalade ou de conséquences imprévues des cyberconflits semble appropriée pour conclure un accord international et améliorer la sécurité internationale. De la même façon que les normes et accords en matière de non-prolifération font peser certaines contraintes sur les États, l'adoption au niveau international de normes explicites de conduite dans le cyberespace influencerait les décisions politiques concernant les coûts et risques éventuels des cyber-attaques. La mondialisation, avec la profonde interdépendance économique qu'elle a créée entre les États, a plutôt accru le besoin de coopération interétatique.

La création de normes favorisant une conduite responsable des États dans le cyberespace, des positions communes concernant l'application du droit international aux cyberconflits et l'élaboration de garanties s'agissant du recours aux cyber-attaques sont autant d'éléments qui augmenteraient la stabilité et limiteraient les risques d'erreur d'appréciation ou d'escalade. La norme la plus importante pour un accord multilatéral définirait la responsabilité des États pour les actions de ses citoyens ; avec une telle norme, il serait plus difficile pour les États d'encourager tacitement des intermédiaires à agir puis de les ignorer ou de nier avoir été impliqués dans les agissements de ces personnes.

L'idée de normes simples suscite également de vives oppositions. Les discussions internationales en matière de cybersécurité interviennent dans un contexte marqué par des priorités politiques divergentes, des actions militaires secrètes, des opérations d'espionnage et une concurrence pour l'exercice d'une influence mondiale. Aujourd'hui, rares sont les personnes favorables à l'idée d'un traité et les efforts internationaux se concentrent plutôt

sur l'adoption de normes, mais la méfiance entre les principales puissances est telle qu'une entente ne sera pas facile.

Le contexte de négociation est marqué par une grande méfiance et de profondes divergences au niveau des valeurs. Malgré le caractère universel des droits de l'homme, de sérieuses divergences de valeurs subsistent. Par conséquent, les normes susceptibles d'être acceptées dans un premier temps par de nombreux États sont limitées. Enfin, le désir des États pour une stabilité et une sécurité accrues dans le cyberespace va les obliger à s'entendre sur leurs responsabilités, sur la façon d'appliquer le droit de la guerre, sur des restrictions concernant l'utilisation de nouveaux moyens militaires et sur les risques d'escalade. Pour l'instant la défiance est trop grande pour que les différents acteurs avancent vers des normes mondiales pour la cybersécurité.

Tout cela laisse à penser que les efforts internationaux devraient, dans un premier temps, envisager les mesures de confiance comme un facteur clef de stabilité et de sécurité dans le cyberespace. Les mesures de confiance, qui nécessitent un accord sur le principe plus que sur le contenu, seraient peut-être plus facilement réalisables au début de l'instauration d'un cadre international pour la cybersécurité. Des mesures progressives pour conclure un accord multilatéral sur des processus de confiance pour la transparence et la communication – notamment pour une transparence accrue au niveau de la doctrine – pourraient être le moyen le plus efficace de conclure un accord à court terme.

À en juger d'après les discussions intéressantes qui eurent lieu lors de la conférence multinationale sur les défis de la cybersécurité (organisée les 13 et 14 décembre 2011 à Berlin avec le Ministère allemand des affaires étrangères, Freie Universität Berlin, l'Institut pour la recherche sur la paix et la politique de sécurité de l'Université de Hambourg et l'UNIDIR), une entente semble se dessiner sur l'intérêt des mesures de confiance, même si l'ensemble de mesures suggéré est relativement limité. Parmi les mesures envisagées citons une plus grande transparence au niveau de la doctrine, de meilleurs mécanismes de gestion des crises, une coopération accrue des services de répression et une entente sur l'application du droit des conflits armés aux cyber-attaques. D'autres efforts visant à étendre et préciser les mesures de confiance sont indispensables pour progresser à long terme.

Notes

1. *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, UNIDIR, 2011.
2. Assemblée générale, *Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/65/201, 30 juillet 2010, par. 18.

Nouvelle publication

Global Nuclear Stability: Building Greater Accountability and Cooperation

Pavel Podvig (UNIDIR, 2011)

La protection des installations et matières nucléaires implique toute une série d'activités aussi bien au niveau international qu'au niveau des pays. En vertu du droit international, il incombe à chaque État de s'occuper de ces activités et d'assurer une protection adéquate des matières en sa possession. La communauté internationale a également pris des mesures pour mettre en place un régime de sécurité nucléaire et l'entretenir.

Cet ouvrage fait le point sur les différents accords internationaux, les programmes et les arrangements institutionnels qui constituent la base du régime international de sécurité nucléaire. Il avance différentes propositions pour renforcer les dispositions en matière de responsabilité et explique qu'il n'est pas aisé d'étendre la portée du régime ni de créer un cadre pour les efforts engagés au niveau mondial en matière de sécurité nucléaire. Il ajoute que, malgré les progrès enregistrés lors du Sommet sur la sécurité nucléaire, d'autres actions multilatérales seront nécessaires pour garantir la sécurité des matières nucléaires et éviter des attaques terroristes nucléaires.

Cette publication est le fruit du projet de l'UNIDIR sur les mécanismes de coopération internationale sur la sécurité nucléaire. Ce projet entend fournir aux responsables politiques des analyses sur les difficultés et les possibilités dans ce domaine et aider les professionnels et les spécialistes dans leurs initiatives visant à renforcer le régime international pour lutter contre la menace du terrorisme nucléaire.

Pour plus d'informations sur nos publications, veuillez consulter notre site web <www.unidir.org>.

Nouveau projet

Les normes concernant les armes explosives

De hauts fonctionnaires de l'ONU, comme le Secrétaire général et le Coordonnateur des secours d'urgence, se sont régulièrement dits préoccupés par les conséquences sur les populations civiles de la violence des armes explosives dans les zones habitées. Les réactions suscitées dernièrement par l'utilisation d'armes explosives à Homs (République arabe syrienne) montrent que de plus en plus d'États, d'instances internationales et d'organisations de la société civile estiment que l'utilisation de ces armes représente un problème humanitaire grave auquel il faut s'attaquer.

Le projet sur « Les normes concernant les armes explosives » examine les lois et politiques qui régissent au niveau national et international la gestion et l'utilisation des armes explosives. Il analyse comment les normes protègent les civils contre les effets d'armes telles que obus d'artillerie, bombes larguées depuis les airs ou dispositifs explosifs improvisés.

Ce projet, qui fait suite à celui intitulé « Discours sur les armes explosives », entend favoriser une meilleure connaissance des aspects normatifs de la gestion des armes explosives par les États et préciser dans quelles conditions les États jugent acceptable l'emploi d'armes explosives dans les zones habitées. Le projet sur « Les normes concernant les armes explosives » s'appuie sur différents progrès enregistrés dans le domaine du désarmement humanitaire et entend sensibiliser les gens aux coûts humains importants qu'entraîne l'utilisation d'armes explosives dans les zones habitées et préciser les questions juridiques et morales que soulève l'emploi de ces armes. Le projet appuie les initiatives qui entendent prévenir et réduire les dommages que ce type de violence armée cause sur les civils, améliorer la protection des civils dans les conflits armés et renforcer les cadres juridiques applicables. Les résultats de ce projet de recherche seront publiés au milieu de l'année 2012. Vous pouvez suivre le projet à l'adresse suivante : <http://explosiveweapons.info/>.

Pour plus d'informations, veuillez vous adresser à :

Maya Brehm

Tél. : +41 (0)22 917 11 41
Fax : +41 (0)22 917 01 76
E-mail : mbrehm@unog.ch