https://www.icrc.org/fre/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

11.31 29/10/2014

Pas de vide juridique dans le cyberespace

16-08-2011 Interview

La guerre informatique et le droit international humanitaire. Partout dans le monde, les décideurs et les responsables militaires réfléchissent aujourd'hui aux implications de la guerre informatique. Cordula Droege, conseillère juridique au CICR, explique que le cadre juridique existant est applicable et doit être respecté même dans l'infosphère.

Qu'entendez-vous par « guerre informatique » et en quoi préoccupe-t-elle le CICR ?

La notion de guerre informatique – ou cyberguerre – est quelque peu nébuleuse et n'est pas nécessairement comprise de la même manière par tout le monde. Aux fins de cette discussion, nous entendrons par guerre informatique les moyens et méthodes de guerre qui s'appuient sur la technologie de l'information – ou cybertechnologie –, et qui sont utilisés dans le cadre d'un conflit armé au sens du droit international humanitaire, par opposition aux opérations militaires cinétiques traditionnelles.

De même, des termes tels que « cyberattaques », « cyberopérations » ou « attaques contre des réseaux informatiques », n'ont pas de signification juridique internationalement reconnue et sont utilisés dans différents contextes – qui ne se limitent pas toujours aux conflits armés – et dans des sens différents. Nous utiliserons, quant à nous, le terme assez large de « cyberopérations » pour désigner des opérations dirigées contre un ordinateur ou un réseau informatique, ou par le biais de ceux-ci, grâce à des flux de données. De telles opérations peuvent poursuivre des objectifs divers, comme infiltrer un système informatique pour collecter, exporter, détruire, altérer et crypter des données, ou pour déclencher, détourner ou manipuler de toute autre manière des processus contrôlés par le système infiltré. Cette technologie peut être utilisée en situation de guerre et, dans des circonstances données, certaines de ces opérations peuvent constituer des attaques au sens du droit international humanitaire.

Les cyberopérations peuvent susciter des préoccupations d'ordre humanitaire ; notamment lorsque leurs effets ne se limitent pas aux données contenues dans les ordinateurs ou les systèmes informatiques qu'y en sont la cible, mais qu'elles ont plutôt pour objet d'engendrer des répercussions dans le « monde réel ». Par exemple, en s'infiltrant dans les systèmes informatiques de soutien de la partie adverse, quiconque est capable de manipuler ses systèmes de contrôle de la circulation aérienne, ses oléoducs et ses centrales nucléaires. Par conséquent, l'impact humanitaire potentiel de certaines opérations de ce genre est énorme. Les cyberopérations recensées à ce jour contre des systèmes informatiques en Estonie, en Géorgie ou en Iran ne semblent cependant pas avoir eu de graves conséquences pour la population civile. Elles font néanmoins apparaître qu'il est techniquement possible d'interférer avec les systèmes de contrôle de la circulation aérienne, terrestre ou maritime, des

barrages ou des centrales nucléaires à partir du cyberespace. Il est dès lors impossible d'écarter des scénarios potentiellement catastrophiques tels que collisions entre avions, rejet de substances toxiques par des usines chimiques ou interruption de fonctionnement d'infrastructures et de services d'importance vitale, comme les réseaux d'approvisionnement en eau et en électricité. Or, ce sont les civils qui risquent d'être les principales victimes d'opérations de ce genre.

Le droit international humanitaire s'applique-t-il aux cyberopérations ?

Le droit international humanitaire (DIH) n'entre en ligne de compte que si des attaques informatiques se produisent dans le cadre d'un conflit armé – que ce soit entre des États, entre des États et des groupes armés organisés ou entre des groupes armés organisés. Il convient dès lors de faire une distinction entre la question générale de la cybersécurité – ou sécurité informatique –, et celle plus particulière des cyberopérations dans les conflits armés. Si des termes comme « cyberattaques » ou même « cyberterrorisme » évoquent volontiers des méthodes de guerre, les opérations auxquelles ils font référence n'ont pas forcément pour cadre un conflit armé. Les cyberopérations peuvent être utilisées, et elles le sont de fait, dans le cadre de crimes commis dans des situations de tous les jours qui n'ont rien à voir avec des situations de guerre. Une grande part des opérations familièrement qualifiées de cyberattaques consistent en réalité en des attaques visant à exploiter des réseaux pour recueillir illicitement des informations, et elles ont lieu hors du cadre d'un conflit armé. Néanmoins, dans les situations de conflit armé, le DIH s'applique lorsque les parties ont recours à des moyens et méthodes de guerre qui font appel à la cybertechnologie.

Si le DIH s'applique aux cyberopérations, qu'en dit-il au juste ?

Le DIH ne mentionne pas explicitement les cyberopérations. Pour cette raison, et parce que l'exploitation de la cybertechnologie est relativement nouvelle et qu'elle semble parfois introduire un changement qualitatif radical dans les moyens et les méthodes de guerre, l'argument selon lequel le DIH est mal adapté à l'infosphère et ne peut s'appliquer à la guerre informatique a été brandi à plus d'une occasion. Toutefois, l'absence dans le DIH de références spécifiques aux cyberopérations ne signifie pas qu'elles échappent aux règles du DIH. Si les moyens et méthodes de la guerre informatique produisent les mêmes effets dans le monde réel que les armes classiques (destruction, interruption de services vitaux, dommages, blessures ou morts), leur utilisation est régie par les mêmes règles que les armes classiques.

Si de nouvelles technologies de tout genre sont constamment mises au point, le champ d'application du DIH est suffisamment large pour embrasser ces progrès. Le DIH interdit ou limite l'emploi de certaines armes en particulier, par exemple, les armes chimiques ou biologiques, ou les mines antipersonnel. Mais il réglemente aussi, par le biais de ses règles générales, tous les moyens et méthodes de guerre, et notamment l'utilisation de toutes les armes. C'est notamment le cas de l'article 36 du Protocole I additionnel aux Conventions de Genève, qui prévoit que « [d]ans 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 a 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. » Outre l’obligation spécifique qu’elle impose aux États parties, cette règle montre que les dispositions générales du DIH s’appliquent aux nouvelles technologies.

Il ne s'agit toutefois pas d'en conclure qu'il ne serait pas nécessaire de continuer à développer le droit à mesure que les technologies évolueront ou que l'impact humanitaire qu'elles auront sera mieux compris. C’est aux États qu’il incombera de se prononcer là-dessus. D’ici-là, il est important d’insister sur le fait qu’il n’y a pas de vide juridique dans le cyberespace. Cela dit, nous sommes face à un certain nombre de points d’interrogation quant à la manière dont le DIH s’appliquera dans la pratique.

En quoi les caractéristiques du cyberespace rendent-elles l’application des règles du DIH difficile ?

Les moyens et méthodes de la guerre informatique sont encore insuffisamment compris, sauf peut-être par les experts techniques qui les mettent au point et qui y ont recours. La mise au point de nouvelles technologies se fait souvent dans le plus grand secret. Or, pour savoir si les moyens et méthodes de la guerre informatique sont qualitativement différents de ceux de la guerre traditionnelle, et dans quelle mesure, le plus important est de comprendre les usages potentiels de ces nouvelles technologies et leurs possibles effets dans les conflits armés.

Un des aspects du cyberespace qui semblerait poser problème est le caractère anonyme des communications qui s’y déroulent. Dans le cadre des cyberopérations effectuées quotidiennement, l’anonymat est la règle plutôt que l'exception. Il est dès lors impossible, dans la plupart des cas, de suivre la trace de leurs auteurs. Or, comme tout système de droit est basé sur l’attribution de responsabilité (en DIH, à une partie à un conflit ou à un individu), cela engendre des difficultés de taille. Notamment, s’il est impossible d’identifier l’auteur d’une opération, et donc de faire le lien entre ladite opération et un conflit armé. Dans ces conditions, il devient en effet extrêmement difficile de déterminer si le DIH s'applique ou non à l'opération en question.

Une autre caractéristique du cyberespace est, il va sans dire, l’interconnectivité. Les interconnexions entre systèmes informatiques, civils et militaires, pourraient compliquer l’application des règles du DIH les plus élémentaires.

Quelles règles de DIH s’appliquent-elles aux cyberopérations ? De quelle manière peuvent-elles être appliquées dans ce monde de l’interconnexion ?

Toutes les règles de DIH qui régissent la conduite des hostilités s’appliquent potentiellement dans le cadre d’un conflit armé. On peut cependant se demander si ces règles sont pertinentes dans le contexte qui nous occupe, et comment elles pourraient être appliquées. Avant de donner quelques exemples, il est important de rappeler qu'une des principales raisons d'être du DIH est de protéger la population civile et les infrastructures civiles des effets des hostilités.

Penchons-nous sur quelques unes des règles fondamentales du DIH pour illustrer l’importance qu’elles ont dans le cas de cyberopérations, et aussi pour montrer que leur application au

cyberespace soulève des questions complexes. Ces règles sont étroitement liées aux principes de distinction, de proportionnalité et de précaution.

Le principe de distinction et l’interdiction des attaques indiscriminées et disproportionnées

En vertu du principe de distinction, les parties à un conflit doivent, en toutes circonstances, faire la distinction entre la population civile et les combattants, ainsi qu'entre les biens de caractère civil et les objectifs militaires. Les attaques indiscriminées, à savoir les attaques qui ne sont pas dirigées contre un objectif militaire déterminé ou dont les effets ne peuvent pas être limités comme le prescrit le DIH, sont interdites. De même que sont interdites les attaques dirigées contre des objectifs militaires ou des combattants dont on peut attendre qu’elles causeront incidemment des pertes en vies humaines dans la population civile ou des dommages de caractère civil qui seraient excessifs par rapport à l’avantage militaire concret et direct attendu ; il s'agit-là d’attaques dites disproportionnées.

Autrement dit, au moment de planifier et de mener des cyberopérations, les seules cibles possibles au regard du DIH sont les objectifs militaires tels que les ordinateurs ou les systèmes informatiques qui servent à soutenir les infrastructures militaires ou les infrastructures exclusivement utilisées à des fins militaires. Il s’ensuit que les attaques menées à partir du cyberespace ne peuvent être dirigées, par exemple, contre des systèmes informatiques utilisés dans des établissements médicaux, des écoles ou d’autres installations à vocation strictement civile. Ce qui est préoccupant sur le plan humanitaire, c’est le fait que le cyberespace est caractérisé par son interconnectivité. Il consiste en un nombre considérable de systèmes informatiques connectés les uns aux autres partout sur la planète. Or, il apparaît que les systèmes informatiques militaires sont souvent interconnectés avec des systèmes commerciaux civils dont ils dépendent intégralement ou partiellement. Il n’est par conséquent pas toujours possible de lancer une attaque informatique contre une infrastructure militaire et d’en limiter les effets à ce seul objectif militaire. Le recours à des vers qui se reproduisent et se propagent sans qu'on puisse les contrôler, risquant de mettre considérablement à mal des infrastructures civiles, constituerait un exemple de violation du DIH.

Obligation de prendre des précautions

La partie qui dirige une attaque doit prendre toutes les dispositions possibles en vue d’éviter ou de réduire au minimum les dommages causés incidemment aux infrastructures civiles ou les souffrances infligées aux populations civiles. Ce qui demande de sa part qu’elle vérifie la nature des systèmes contre lesquels elle prévoit de lancer une attaque, et qu'elle évalue les dommages qui pourraient en découler. Cela implique aussi que lorsqu'il est évident qu'une attaque provoquera des dommages ou des pertes civiles incidentes excessives, elle doit être annulée.

En outre, les parties à un conflit ont l’obligation de prendre les précautions nécessaires contre les effets des attaques. Aussi serait-il indiqué, dans le but de protéger la population civile contre les effets indirects de ces attaques, qu’elles s’assurent que les systèmes informatiques

militaires soient suffisamment indépendants des systèmes civils. Le fait que des systèmes informatiques militaires dépendent de systèmes gérés par des entreprises civiles et également utilisés à des fins civiles, et qu'ils y soient interconnectés, pourrait être une source de préoccupation.

Vue sous en autre angle, la technologie de l'information serait par contre susceptible de servir à limiter les dommages causés incidemment aux infrastructures civiles ou les souffrances infligées aux populations civiles. Il pourrait par exemple se révéler moins préjudiciable d'interrompre le fonctionnement de certains services utilisés à des fins à la fois militaires et civiles, que de détruire complètement des infrastructures. Auquel cas, on pourrait attendre qu'en vertu du principe de précaution, les États, choisissent les moyens les moins nuisibles pour atteindre leurs objectifs militaires.

Que fait le CICR dans le domaine de la guerre informatique ?

Nous devons garder à l'esprit que le potentiel militaire et l'impact humanitaire de la guerre informatique – en dépit de tout ce que nous lisons dans les médias sur la question – sont loin d'être complètement connus. Cela étant, il n'est évidemment pas exclu que les cyberopérations aient des conséquences désastreuses pour les civils. C'est pourquoi le CICR suit de près l'évolution de la situation dans ce domaine et rappelle aux parties à un conflit l'obligation qui leur incombe de respecter le DIH. Nous sommes aussi extrêmement attentifs aux initiatives visant à clarifier le droit applicable aux cyberopérations dans les conflits armés. Il s'agit pour nous de réaffirmer l'applicabilité du DIH, de prévenir l'affaiblissement de cette branche du droit provoquée par la multiplication des normes juridiques et de rappeler à ceux qui participent au monde de l'interconnexion que la nécessité d'épargner la population civile est certainement plus impérieuse que jamais.