RAPPORTS ET DOCUMENTS

Le droit international humanitaire et les nouvelles technologies de l'armement, XXXIVe table ronde sur les sujets actuels du droit international humanitaire, San Remo, 8-10 septembre 2011

Discours d'ouverture de Jakob Kellenberger, Président du CICR, et Conclusions par Philip Spoerri, Directeur du droit international et de la coopération au CICR

: : : : : : :

Discours d'ouverture de Jakob Kellenberger, Président, Comité international de la Croix-Rouge*

Les nouvelles technologies et les nouvelles armes ont révolutionné la conduite de la guerre depuis des temps immémoriaux. Il suffit de se rappeler l'invention du chariot, de la poudre à canon, de l'aéronautique ou de la bombe nucléaire pour comprendre combien les nouvelles technologies ont modifié la façon dont on fait la guerre.

* Disponible sur : http://www.icrc.org/fre/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm

Depuis la Déclaration de Saint-Pétersbourg de 1868 qui a interdit l'emploi de projectiles de moins de 400 grammes, la communauté internationale s'est efforcée de réglementer les nouvelles technologies utilisées dans la conduite de la guerre. Et le droit international humanitaire moderne s'est à de nombreux égards développé en réponse aux nouveaux défis posés par l'émergence d'armes nouvelles.

La Déclaration de Saint-Pétersbourg a interdit un type d'arme précis, mais elle a aussi établi un certain nombre de principes généraux sur lesquels allait reposer plus tard toute l'approche adoptée par le droit international humanitaire face aux nouveaux moyens et méthodes de guerre. Elle dit en effet que le seul but légitime que les États doivent se proposer, durant la guerre, est l'affaiblissement des forces militaires de l'ennemi, et que ce but serait dépassé par l'emploi d'armes qui aggraveraient inutilement les souffrances des hommes mis hors de combat ou voudraient leur mort inévitable.

C'est dans cet esprit que la réglementation des moyens et méthodes de guerre s'est développée tout au long des 150 dernières années, en suivant deux voies : par l'adoption, d'une part, de **règles et principes généraux s'appliquant à tous les moyens et méthodes de guerre**, partant du principe que les lois de l'humanité imposent des limites quant à leur choix et leur emploi ; et par la conclusion, d'autre part, d'**accords internationaux interdisant ou limitant l'emploi de certaines armes**, telles que les armes chimiques et biologiques, les armes incendiaires, les mines antipersonnel ou encore les armes à sous-munitions.

Les règles et principes généraux protègent les combattants contre les armes qui sont de nature à causer des blessures superflues ou des souffrances inutiles, mais ils ont aussi été établis dans le but de protéger les civils des effets des hostilités. C'est ainsi, par exemple, que les moyens et méthodes de guerre dont les effets sont indiscriminés sont interdits.

Partant de ces interdictions générales essentielles, le droit international humanitaire a été conçu de façon suffisamment souple pour pouvoir s'adapter aux évolutions technologiques, y compris à celles qui étaient inenvisageables à l'époque. Et il ne fait aucun doute que le droit international humanitaire s'applique aux nouvelles armes et à toutes les nouvelles technologies utilisées pour la guerre. L'article 36 du Protocole additionnel I le reconnaît explicitement quand il dit que dans l'étude, la mise au point ou l'adoption d'une nouvelle arme ou d'une nouvelle méthode de guerre, les États parties ont l'obligation de déterminer si l'emploi en serait interdit, dans certaines circonstances ou en toutes circonstances, par une règle du droit international qui leur est applicable.

Cela étant, l'application de règles juridiques préexistantes à une technologie nouvelle soulève la question de savoir si ces règles sont suffisamment claires au vu des caractéristiques spécifiques – et peut-être sans précédent – de cette technologie, et également au vu de l'impact humanitaire qu'elle peut avoir dans un avenir prévisible. Dans certaines circonstances, les États choisiront, ou ont déjà choisi, d'adopter des règles plus spécifiques.

Notre époque est celle des technologies de l'information, et on le voit, ces technologies sont aussi utilisées pour se battre. Ce n'est pas entièrement nouveau, mais la multiplication des nouvelles armes ou méthodes de guerre qui dépendent

de ces technologies semble exponentielle. Les mêmes progrès des technologies de l'information qui nous permettent d'avoir des conversations vidéo sur nos téléphones portables permettent également de construire des drones plus petits, moins chers et plus polyvalents. La même technologie qui nous permet de commander à distance l'air conditionné de notre maison permet également de plonger dans le noir une ville située à l'autre bout du monde.

La table ronde de cette année va nous permettre de regarder de plus près certaines des technologies qui commencent tout juste à être utilisées pour faire la guerre, ou qui sont susceptibles de l'être, et à en discuter. Je pense en particulier à la cybertechnologie, aux systèmes d'armement télécommandés et aux armes robotisées.

Je commencerai par la « **guerre informatique** ».

On s'interroge beaucoup aujourd'hui sur les problèmes juridiques que pose la guerre informatique, ou « cyberguerre ». Quand je parle de guerre informatique, je fais référence aux moyens et méthodes de guerre qui font appel aux technologies de l'information et qui sont employés dans un contexte de conflit armé. Le potentiel militaire du cyberespace commence à peine à être exploré. Nous savons, à partir de certaines cyberopérations qui ont été menées, qu'une partie au conflit peut « attaquer » les systèmes informatiques d'une autre partie, en s'y infiltrant ou en les manipulant. L'infrastructure informatique dont dépend l'arsenal militaire de l'ennemi peut ainsi être endommagée, désorganisée ou détruite. Mais les infrastructures civiles peuvent aussi être touchées, soit parce qu'elles sont directement visées ou parce qu'elles sont incidemment endommagées ou détruites alors que ce sont les infrastructures militaires qui sont visées.

Au jour d'aujourd'hui, nous ne savons pas avec précision quelles pourraient être les conséquences d'une guerre informatique du point de vue humanitaire. Techniquement parlant, des cyberattaques contre le contrôle du trafic aérien et d'autres modes de transport, des barrages ou des centrales nucléaires, sont possibles. De telles attaques auraient très vraisemblablement des conséquences humanitaires de grande ampleur. Elles pourraient faire de nombreuses victimes civiles et d'énormes dégâts. Bien sûr, il est pour l'instant difficile de connaître le degré de probabilité de cyberattaques d'une telle gravité, mais nous ne pouvons pas nous permettre d'attendre qu'il soit trop tard pour prévenir les pires scénarios.

Du point de vue humanitaire, le principal problème que posent les cyberopérations dans un contexte de guerre vient du fait que le cyberespace est interconnecté ; il est de ce fait même difficile de limiter les effets de ces attaques aux seuls systèmes informatiques militaires. Même si certaines infrastructures informatiques militaires sont sécurisées et indépendantes des infrastructures civiles, beaucoup d'infrastructures militaires dépendent d'ordinateurs ou de réseaux informatiques civils. Dans de telles conditions, comment l'attaquant peut-il prévoir les répercussions de son attaque sur les systèmes informatiques civils ? Il est fort probable que le système ou le réseau informatique dont dépend l'infrastructure militaire soit le même que celui dont dépend l'hôpital voisin ou le réseau d'approvisionnement en eau.

Une autre raison pour laquelle il est difficile d'appliquer les règles du droit international humanitaire au cyberespace vient du fait qu'il repose sur une architecture numérique. La numérisation garantit l'anonymat et complique l'attribution de telle ou telle conduite. C'est ainsi que dans la plupart des cas, il s'avère difficile, sinon impossible, d'identifier l'auteur d'une attaque. Comme le DIH est basé sur l'attribution de responsabilité à des personnes et à des parties à un conflit, cela pose d'énormes problèmes. En effet, s'il est impossible d'identifier l'auteur d'une opération et, de ce fait, d'établir le lien entre l'opération et le conflit armé, il est extrêmement difficile de déterminer l'applicabilité ou non du DIH à l'opération en question.

La deuxième innovation technologique dont nous parlerons à cette table ronde concerne les **systèmes d'armement télécommandés**.

Les systèmes d'armement télécommandés constituent une étape supplémentaire d'une stratégie de longue date qui consiste à éloigner de plus en plus les soldats de leurs adversaires et du champ de bataille.

Les drones – ou véhicules aériens sans pilote (UAV : *unmanned aerial vehicles*) – constituent l'exemple le plus marquant de ces nouvelles technologies, qu'ils soient armés ou non. Leur nombre s'est accru à un rythme exponentiel ces dernières années. De la même façon, les véhicules terrestres sans pilote sont de plus en plus présents sur les champs de bataille. Ils vont du robot qui sert à détecter et à détruire des bombes au bord des routes, jusqu'au robot qui inspecte les véhicules à l'approche d'un poste de contrôle.

Un des principaux arguments avancés pour défendre l'investissement dans ces nouvelles technologies est qu'elles préservent la vie des combattants. Un autre argument est que les drones, en particulier, ont une meilleure capacité de surveillance aérienne en temps réel et qu'ainsi les belligérants peuvent attaquer avec plus de précision les objectifs militaires, réduisant de ce fait les victimes civiles et les dommages aux biens de caractère civil. En d'autres termes, ils peuvent faire preuve de davantage de précaution dans l'attaque.

On peut néanmoins s'inquiéter de la façon dont ces systèmes sont dirigés et par qui. Pour commencer, ils sont parfois commandés par des civils, qui peuvent être des employés de sociétés privées. Ce cas pose la question du statut et de la protection de ces opérateurs ; il conduit aussi à se demander si leur formation et leur responsabilité sont suffisantes au vu des décisions qu'ils prennent, lesquelles sont des questions de vie ou de mort. En second lieu, des études ont montré que si on déconnecte une personne, en l'éloignant notamment (physiquement ou émotionnellement) d'un adversaire potentiel, il lui est plus facile de le prendre pour cible et de commettre des abus. L'historien militaire John Keegan appelle cela la « dépersonnalisation de la bataille ».

Enfin, je voudrais dire quelques mots des **armes robotisées**.

Les **armes automatisées** – ou robots en langage courant – vont plus loin que les systèmes télécommandés. Elles ne sont pas dirigées à distance, mais fonctionnent de façon autonome et indépendante, une fois lancées. C'est notamment le cas des mitrailleuses SG autonomes, des munitions autodirectrices et de certaines mines terrestres antivéhicule. Bien que déployés par des humains, ces sys-

tèmes vont identifier ou détecter de façon indépendante un type de cible donné puis tirer ou exploser. Une mitrailleuse SG autonome par exemple fera feu ou non après vérification du mot de passe prononcé par un intrus potentiel.

Le problème majeur que posent les systèmes automatisés est leur capacité à respecter le niveau de discrimination exigé par le DIH. Cette capacité de discrimination va entièrement dépendre de la qualité et de la diversité des capteurs et de la façon dont le système est programmé. Jusqu'à présent, la façon dont ces systèmes pourraient faire la différence entre un civil et un combattant, ou entre un combattant blessé ou hors de combat et un combattant actif, n'est pas claire. Et la façon dont ces armes pourraient évaluer la perte accidentelle en vies humaines, les blessures infligées aux civils ou les dégâts pour des objets civils, et ainsi respecter le principe de proportionnalité, ne l'est pas plus.

Une autre étape consisterait à déployer des **systèmes d'armement autonomes**, c'est-à-dire des systèmes d'armement qui peuvent analyser ou adapter leur fonctionnement en fonction d'un changement de circonstances. Un système véritablement autonome serait doté d'une intelligence artificielle qui devrait être capable de mettre en œuvre le DIH. Bien que ce domaine suscite un grand intérêt et que la recherche soit largement financée, ces systèmes n'ont pas encore été adaptés aux armements. Développer de tels systèmes est un tel défi en termes de programmation que ce sera peut-être impossible. Il est clair que le déploiement de tels systèmes représenterait une véritable révolution conceptuelle et un changement qualitatif majeur dans la conduite des hostilités. Mais il soulèverait aussi tout un ensemble de problèmes fondamentaux du point de vue légal, éthique et sociétal, et ces problèmes doivent être pris en compte avant que ces systèmes ne soient développés ou déployés. Un robot pourrait être programmé de façon à se comporter de façon plus éthique et plus prudente qu'un être humain sur le champ de bataille. Mais que faire si, du point de vue technique, il est impossible de réaliser une programmation fiable d'un système d'armement autonome de façon à garantir qu'il respecte le DIH sur le champ de bataille?

À l'occasion du débat sur ces nouvelles technologies, il nous faut voir également quels sont les avantages qu'elles pourraient apporter si elles contribuaient à une **meilleure protection**. Respecter les principes de distinction et de proportionnalité signifie qu'il faut prendre certaines **précautions dans l'attaque**, comme indiqué à l'article 57 du Protocole additionnel I. Cet article prévoit notamment l'obligation pour un attaquant de prendre toutes les précautions pratiquement possibles quant au choix des moyens et méthodes d'attaque en vue d'éviter et, en tout cas, de réduire au minimum les pertes en vies humaines dans la population civile, les blessures aux personnes civiles et les dommages aux biens de caractère civil qui pourraient être causés incidemment. Dans certains cas, les cyberopérations ou le déploiement d'armes télécommandées ou de robots pourraient faire incidemment moins de victimes civiles et causer moins de dommages aux biens de caractère civil que l'emploi d'armes classiques. Des précautions accrues devraient également être possibles dans la pratique, du fait simplement que ces armes sont déployées depuis suffisamment loin et souvent, avec suffisamment de temps pour que la cible soit choisie avec soin et que le

moment de l'attaque soit décidé de façon à minimiser l'impact sur la population civile et les biens de caractère civil. On pourrait considérer que dans de telles circonstances, l'application de cette règle voudrait qu'un commandant évalue s'il peut obtenir le même avantage militaire en utilisant ces moyens et méthodes de guerre, s'ils sont applicables.

Le monde des nouvelles technologies n'est pas un monde virtuel et ne relève pas non plus de la science-fiction. Dans les conflits armés, les nouvelles technologies peuvent tuer et causer des dommages très réels. Conscient de leurs conséquences possibles du point de vue humanitaire, le CICR considère qu'il est important d'encourager le débat sur ces questions, d'attirer l'attention sur la nécessité d'évaluer l'impact humanitaire des technologies naissantes, et de veiller à ce que celles-ci ne soient pas utilisées de façon prématurée dans des circonstances où le respect du droit ne peut être assuré. La préoccupation qui a conduit à la Déclaration de Saint-Pétersbourg est tout aussi impérieuse aujourd'hui qu'elle l'était alors.