Le droit de la guerre impose des limites même aux cyberattaques

01-07-2013 Interview

La guerre informatique (ou cyberguerre) est soumise à des règles, et les infrastructures informatiques civiles (ordinateurs, réseaux et systèmes) ne doivent pas faire l'objet de cyberattaques : c'est l'une des conclusions du Manuel de Tallinn, une étude sur l'applicabilité du droit international à la cyberguerre réalisée par un groupe de juristes et d'experts militaires. Laurent Gisel, conseiller juridique au CICR, explique en quoi cet ouvrage constitue un pas important dans les efforts visant à réduire les souffrances humaines.

Qu'est-ce que la guerre informatique et pourquoi le CICR s'y intéresse-t-il ?

Dans le cadre de cet entretien, on entend par « guerre informatique » uniquement les moyens et méthodes de guerre utilisés pour mener des cyberopérations équivalant à un conflit armé, ou conduites dans le contexte d'un conflit armé, au sens du droit international humanitaire (DIH). Le DIH ne s'applique pas à tous les types d'activités qu'on qualifie de « cyberattaques » dans le langage courant.

Quelles limites le droit de la guerre impose-t-il aux cyberattaques ? questions et réponses

Les réseaux informatiques sont vulnérables. Lorsque les ordinateurs ou les réseaux d'un État sont attaqués, les civils risquent d'être privés de biens et de services essentiels comme l'eau potable, les soins médicaux ou l'électricité. Les cyberattaques peuvent entraver les services de secours dans leur travail vital ou perturber le fonctionnement d'infrastructures essentielles telles que les barrages, les centrales nucléaires et les systèmes de pilotage des avions. Le bien-être, la santé, voire la vie de centaines de milliers de personnes sont en jeu. L'une des missions du CICR est de rappeler à toutes les parties à un conflit qu'il faut veiller constamment à épargner les civils : les guerres ont des règles et des limites qui s'appliquent à tous les moyens et méthodes de guerre.

Dans le Manuel de Tallinn, des juristes et des experts militaires soutiennent que le DIH s'applique à la guerre informatique. En quoi est-ce important ?

Nous nous félicitons que des experts réaffirment la pertinence du DIH dans ce domaine, car il est essentiel de trouver des moyens de limiter le coût humain que peuvent avoir les cyberopérations dans les conflits armés. Nous espérons vivement que le Manuel de Tallinn contribuera utilement aux discussions entre les États sur ces questions complexes. Le CICR, pour sa part, continuera d'offrir son expertise en matière de DIH pour faire face à ces défis.

Si les moyens et méthodes de guerre ont évolué depuis la rédaction des Conventions de Genève en 1949, le DIH continue de s'appliquer à toutes les activités menées par les parties

dans le cadre d’un conflit armé, et ses règles doivent être respectées. Il pourrait toutefois se révéler utile de développer le droit pour s’assurer qu’il protège suffisamment la population civile, à mesure que les cybertechnologies évolueront ou que leur impact humanitaire sera mieux compris. C’est aux États qu’il appartiendra de se prononcer sur ce point.

Quel rôle le CICR a-t-il joué dans l’élaboration du manuel ?

L’institution a participé en qualité d’observateur aux débats des experts pour veiller à ce que le manuel tienne compte autant que possible des dispositions existantes du DIH, et pour faire valoir la protection que ce droit accorde aux victimes des conflits armés. Le manuel énonce des règles assorties de commentaires explicatifs. Le CICR adhère de manière générale aux règles telles qu’elles y sont formulées, à quelques exceptions près.

Quels sont les principaux défis posés par la guerre informatique ?

Il n’existe qu’un seul cyberespace que se partagent utilisateurs civils et utilisateurs militaires, et tout est interconnecté. Les grands défis consistent donc à faire en sorte que les attaques soient dirigées exclusivement contre des objectifs militaires, et que des précautions soient prises en tout temps pour épargner la population et les infrastructures civiles. Les États doivent se montrer extrêmement prudents lorsqu’ils recourent à des cyberattaques.

Les pirates informatiques sont-ils une cible légitime dans une cyberguerre ?

Comme la plupart des cyberopérations ne sont pas liées à un conflit armé, elles n’entrent pas dans le champ d’application du DIH. Même dans une situation de conflit armé, la majorité des pirates seraient considérés comme des civils et resteraient donc protégés par le DIH contre toute attaque directe. Ils risqueraient cependant des poursuites pénales pour leurs actes.

Cela dit, si un pirate informatique participe directement aux hostilités en lançant une cyberattaque à l’appui d’une partie à un conflit armé, il perd sa protection contre les attaques directes pendant la durée de cette attaque.

Les cybertechnologies peuvent-elles être utilisées à des fins positives en cas de conflit armé ?

Lorsqu’ils conduisent des opérations militaires, les États doivent veiller à éviter ou, en tout cas, réduire au minimum les pertes en vies civiles, les blessures aux personnes civiles et les dommages aux biens civils qui pourraient être causés incidemment. Les avancées technologiques permettront peut-être un jour de mettre au point des armes cybernétiques qui, dans certaines circonstances, feront moins de victimes et de dommages collatéraux que les armes traditionnelles, tout en procurant le même avantage militaire. Quoi qu’il en soit, le CICR continuera de suivre les évolutions dans ce domaine.

Cyberarmes : que dit le droit international ?

Il est dans l’intérêt de tous les États d’évaluer la licéité de ces armes nouvelles, s’ils veulent s’assurer que leurs forces armées agissent en conformité avec leurs obligations internationales. En vertu de l’article 36 du premier Protocole de 1977 additionnel aux Conventions de Genève, chaque État partie est tenu de veiller à ce que toute nouvelle arme qu’il emploie ou envisage d’employer soit conforme aux règles du DIH, comme le rappelle judicieusement le Manuel de Tallinn.

À la XXVIIIe Conférence internationale de la Croix-Rouge et du Croissant-Rouge en 2003, les États parties aux Conventions de Genève ont appelé à soumettre « à un examen rigoureux et pluridisciplinaire » les nouvelles armes et les nouveaux moyens et méthodes de guerre, pour éviter que la protection conférée par le droit ne soit dépassée par les progrès technologiques. Le recours à des cyberopérations dans le cadre des conflits armés est un parfait exemple de l’évolution rapide des technologies.