

11.28 29/10/2014

Guerre informatique

01-09-2011 Introduction

Juristes et experts techniques s'accordent à dire que le potentiel destructeur des attaques contre les réseaux informatiques est considérable, ce qui soulève des questions non seulement quant à l'application du droit international humanitaire (DIH), mais aussi quant à la définition même de « conflit armé ».

Ni les Conventions de Genève ni leurs Protocoles additionnels ne mentionnent spécifiquement la guerre informatique ou les attaques contre les réseaux informatiques. Toutefois, les principes et les règles contenus dans ces traités, qui régissent les moyens et méthodes de guerre, ne se limitent pas aux situations qui existaient à l'époque où ils ont été adoptés. Le DIH a en effet clairement anticipé l'évolution de la technologie de l'armement et la mise au point de nouveaux moyens et méthodes de combat.

Par conséquent, il ne fait aucun doute que le droit international humanitaire s'applique à la guerre informatique. Du fait notamment que les civils et leurs moyens de subsistance peuvent être menacés et touchés par des attaques informatiques pendant un conflit armé, la guerre informatique entre tout à fait dans le champ d'application du DIH.

La notion de guerre informatique ou d'attaques contre les réseaux informatiques dans le cadre d'un conflit armé est très récente, à tel point que les débats sur l'impact potentiel de ce nouveau type de conflit reposent souvent sur des hypothèses.

Par attaque contre un réseau informatique on entend toute opération lancée à des fins hostiles contre un ennemi et destinée à obtenir, altérer, détruire, perturber ou transférer des données stockées sur un ordinateur, traitées par un ordinateur ou transmises au moyen d'un ordinateur.

Le fait qu'une attaque contre les réseaux informatiques en temps de conflit armé ne soit pas cinétique, physique ou violente en soi ne signifie pas pour autant qu'elle échappe au champ d'application du DIH.

Tout comme les autres moyens et méthodes de guerre, les attaques informatiques dirigées contre des combattants et des objectifs militaires sont licites pour autant qu'elles respectent le droit humanitaire. En vertu du DIH, les attaques de ce type ne doivent pas être menées sans discrimination, mais dans le respect des principes de distinction – entre les objectifs militaires et les biens de caractère civil – et de proportionnalité – entre l'avantage militaire attendu et les dommages causés à la population civile. À cet égard, les techniques de la guerre informatique ne sont pas très différentes des autres moyens de guerre. Elles peuvent être utilisées, par exemple, contre les systèmes bancaires, de production et de distribution de la partie ennemie, qui sont de caractère civil.

La guerre informatique vient ajouter un niveau de complexité supplémentaire aux conflits armés, soulevant des questions qui ne s'étaient jamais posées en matière de DIH. Aussi

convient-il de réaffirmer la pertinence du DIH, dès lors qu'il est la principale branche du droit capable de réglementer cette guerre d'un nouveau type. Les normes du droit international humanitaire relatives notamment à l'emploi d'armes frappant sans discrimination, à la distinction entre cibles militaires et cibles civiles, à la proportionnalité et à la perfidie, elles peuvent et doivent aussi s'appliquer à la guerre informatique.