DROIT & POLITIQUES
HUMANITAIRES

Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles

mars 26, 2020, Droit et conflits / Nouvelles technologies

15 minutes de lecture

Helen Durham
Directrice du département International Law and Policy, CICR, Genève

Dans les discussions actuelles initiées par les Nations Unies, un certain nombre de questions portant sur les implications juridiques et politiques de l'application du droit international humanitaire aux cyberopérations lors de conflits armés sont apparues. Ce billet s'efforce de répondre à sept questions essentielles de droit et de politique, qui vont de la supposée « légitimation » de la guerre informatique à la raison pour laquelle les questions cyber concernent tous les États.

00:00 00:00

Nul besoin d être expert en cybersécurité pour le constater : dans notre monde dépendant du numérique, les cyberattaques représentent une réelle menace pour les infrastructures essentielles et le fonctionnement des sociétés. Le CICR est particulièrement préoccupé par la vulnérabilité des hôpitaux face aux cyberattaques – un risque élevé en tout temps, mais qui est encore plus prégnant en période de conflit ou de pandémie, à l'instar de la crise que nous traversons avec le COVID-19. Le *Secrétaire général des Nations Unies* s'est dit préoccupé par le fait que, si conflit majeur éclatait aujourd'hui, « il pourrait être déclenché par une cyberattaque massive, qui viserait non seulement les installations militaires, mais aussi certaines infrastructures civiles [traduction CICR] ».

Ces derniers mois, nous avons assisté à des débats intergouvernementaux sans précédent sur les menaces réelles et possibles dans le cyberespace, sur l'applicabilité du droit international et sur la manière dont les normes peuvent aider à éviter la menace élevée que représentent les activités informatiques malveillantes. Tous les États membres participent actuellement à un *groupe de travail à composition non limitée*, tandis que des experts issus de 25 États sont rassemblés au sein du *groupe d'experts gouvernementaux* et que *des entreprises spécialisées dans le secteur de la technologie ainsi que organisations issues de la société civile* se sont jointes au débat à différentes occasions.

En sa qualité d'organisation *mandatée par les États* pour travailler à l'interprétation du droit international humanitaire, veiller à sa fidèle application lors de conflits armés et pour préparer toute possible adaptation de ce corpus juridique, le CICR a participé à plusieurs de ces discussions et a partagé *sa position* avec tous les États. Puisque des cyberopérations sont aujourd'hui conduites durant des conflits armés, le CICR est préoccupé par leur *coût humain potentiel*. Dans ce domaine où les technologies évoluent rapidement, le CICR appelle les États à recourir à des cyberopérations en respectant les limites du droit international en vigueur et, en particulier, le droit international humanitaire. Le CICR saisit ici l'opportunité de répondre à sept questions-clé de droit et de politique portant sur les cyberopérations en période de conflit armé.

1. Les cyberconflits : une question qui ne concerne que les États avancés sur le plan technologique ?

Le cyberespace est, par nature, interconnecté. C'est pourquoi une réglementation efficace des cyberopérations en temps de conflit armé intéresse tous les États, indépendamment de leur niveau de développement technologique et de leur volonté ou non de développer des cybercapacités militaires. Dans le cyberespace, les attaques dirigées contre un seul État peuvent en affecter beaucoup d'autres, indépendamment de leur situation géographique et de leur engagement ou non dans le conflit. Nous avons déjà observé ce phénomène, quand, récemment, un logiciel malveillant s'est propagé rapidement, ne laissant guère de pays indemnes.

En vertu du droit international humanitaire, les attaques qui emploient des moyens et méthodes de guerre qui ne peuvent pas être dirigés contre un objectif militaire déterminé ou dont les effets ne peuvent pas être limités comme le prescrit le droit, sont interdites (voir *article 51, par. 4 du Protocole additionnel I* et la *règle 11 de l'Étude sur le droit international coutumier du CICR*). Appliqué au contexte cybernétique actuel, ceci signifie que les cyberoutils qui se propagent et qui causent des dommages indiscriminés sont illicites. Aussi, la priorité pour les États devrait donc être de s'assurer que la communauté internationale affirme que le DIH est applicable au cyberespace au cyberespace et que tous les États en respectent les règles lors d'un conflit armé.

2. Le droit international humanitaire légitime-t-il la militarisation du cyberespace ou la cyberguerre ?

Non. Affirmer que le droit international humanitaire est applicable ne légitime pas la cyberguerre, pas plus qu'il ne légitime d'autres formes de guerres. Le fait de restreindre les cyberopérations en période de conflit armé ne revient pas à légitimer le recours à des cyberopérations hostiles ou à rendre leur emploi nécessairement licite.

Forts de plus de 150 années d'expérience dans la participation aux discussions intergouvernementales sur la guerre, nous avons maintes fois perçu la crainte d'une possible légitimation de la guerre. Cependant, en 1977, les États ont écarté, en des termes non équivoques, la crainte que le droit international humanitaire ne légitime la guerre : le préambule du Protocole additionnel I aux Conventions de Genève de 1949 dispose que le droit international humanitaire ne peut pas être « interprét[é] comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies ».

En fait, affirmer les limites que le droit international humanitaire impose aux cyberopérations en temps de conflit armé est, aujourd'hui, plus important que jamais. Les cyberopérations sont devenues une réalité dans les conflits armés et de nombreux États développent des cybercapacités offensives. Les États ont la responsabilité de veiller à ce que ces nouveaux moyens et méthodes de guerre ne soient pas illimités. Même en temps de paix, certaines règles du droit international humanitaire apportent des limites aux types d'armes qui peuvent être utilisés et aux moyens et méthodes de guerre qui peuvent être développés (voir *l'article 36 du Protocole additionnel I*). En période de conflit armé, le respect du droit international humanitaire protège les civils des pires formes que peut revêtir la violence.

3. Quand le droit international humanitaire s'applique-t-il ?

Le droit international humanitaire s'applique aux cyberopérations, seulement et uniquement, lors des conflits armés. Lorsque nous discutons avec des militaires à travers le monde, nul ne conteste que le droit international humanitaire s'applique aux cyberopérations lorsque des militaires décident de recourir à ce moyen de faire la guerre lors d'un conflit armé en cours. La position contraire mènerait à la conclusion absurde selon laquelle il serait interdit à une partie à un conflit d'attaquer un hôpital avec un missile, mais qu'elle pourrait cependant, en toute licéité, détruire les ordinateurs, les machines et les réseaux de ce même hôpital, par le biais de cyberopérations.

Déterminer si une cyberopération peut, en soi, déclencher l'application du droit international humanitaire, lequel s'applique lorsque des dissensions entre des États (ou une situation de violence entre un État et un groupe armé non étatique) dégénèrent pour se muer en un conflit armé, constitue une question récurrente (voir le *commentaire mis à jour de la Première Convention de Genève de 1949*, CICR, 2018, par. 253-256 ; 436 et 437). Concernant les conflits armés internationaux, il est aujourd'hui admis « qu'un conflit armé existe chaque fois qu'il y a recours à la force armée entre États » (TPIY, *arrêt relatif à l'appel de la défense*, par. 70). Mais quand ce seuil est-il atteint dans les cas de cyberopérations ?

Il est généralement admis que lorsque des cyberopérations ont des conséquences semblables aux opérations cinétiques classiques – comme la destruction de biens civils ou militaires ou qui entraînent des blessures, voire la mort de soldats ou de civils – elles sont régies par le DIH applicable aux conflits armés internationaux (*Manuel de Tallinn 2.0*, règle 82, par. 16).

Lorsque, en l'absence d'hostilités cinétiques, des cyberopérations ne causent aucune destruction ou dommage matériel aux infrastructures civiles ou militaires, il est moins évident de déterminer si celles-ci pourraient être considérées comme un recours à la force armée réglementé par le DIH. Reste à savoir si et à quelles conditions les États considéreront ces cyberopérations comme un emploi de la force armée qui constituerait un conflit armé au sens du DIH.

4. Quelles sont les relations entre le droit international humanitaire et la Charte des Nations Unies ?

Le droit international humanitaire et la Charte des Nations Unies sont distincts, mais complémentaires. Le *Préambule de la Charte* dispose que celle-ci vise à « préserver les générations futures du fléau de la guerre », tandis que l'objectif du droit international humanitaire est de « protég[er] les victimes des conflits armés » (*préambule, Protocole additionnel I*). Concrètement, ceci signifie que la Charte des Nations Unies interdit l'usage de la force dans d'autres circonstances que celle de la légitime défense, ou lorsque le Conseil de sécurité l'autorise. Ceci suppose que les différends internationaux soient réglés par des moyens pacifiques. L'applicabilité du droit international humanitaire n'entend pas remplacer ou écarter la Charte. Cependant, en cas de conflit armé, le droit international humanitaire procure un ensemble de protections fondamentales pour ceux qui ne participent pas (les civils) ou qui ne participent plus (par exemple, les soldats blessés ou les détenus) aux hostilités.

Puisque tant le droit international humanitaire que la Charte des Nations Unies traitent des conflits armés, la terminologie est quasi identique et peut parfois prêter à confusion.

Par exemple, en vertu de *l'article 51 de la Charte des Nations Unies*, le droit à la légitime défense est autorisé en cas d'« agression armée ». Selon la *Cour internationale de Justice*, seules « les formes les plus graves de l'emploi de la force » peuvent constituer une agression armée. Il est important de rappeler que la notion d' « agression armée » au sens de la Charte des Nations unies doit être distinguée du « recours à la force armée » susceptible de déclencher un conflit armé en vertu du droit international humanitaire (voir ci-dessus), ou de *la notion d' « attaque »*. Qualifier une cyberopération de recours à la force armée qui déclenche l'application du droit international humanitaire ou d'attaque au sens du DIH, ne signifie pas nécessairement qu'il s'agit d'une « agression armée » au sens de la Charte des Nations Unies.

5. Les cyberopérations peuvent-elles être moins nuisibles que les opérations cinétiques ?

Pour le militaire, le recours à des cyberopérations peut offrir des solutions que d'autres moyens et méthodes de guerre ne peuvent garantir, mais cela comporte aussi des risques.

Les cyberopérations peuvent permettre aux parties à des conflits armés d'atteindre leurs objectifs militaires sans causer de dommages aux civils ou sans détruire des infrastructures civiles. Les militaires mettent parfois en exergue le fait que, grâce à la cybertechnologie, il est possible de causer moins de dommages que par le biais d'attaques cinétiques. Ceci signifie aussi, que, après un conflit, la reconstruction serait plus aisée et moins onéreuse.

En même temps, l'usage de cyberopérations lors d'un conflit armé comporte aussi des risques. Les cyberopérations récentes – qui ont pour la plupart été conduites en dehors d'une situation de conflit armé – ont montré que des acteurs chevronnés ont développé la capacité de perturber *la distribution de services essentiels à la population civile*. Aujourd'hui, on sait peu de choses des cybercapacités les plus sophistiquées, de la manière dont la technologie pourrait évoluer et jusqu'à quel point le recours à des cyberopérations lors de conflits armés pourrait s'éloigner des tendances observées jusqu'ici.

6. Le droit international humanitaire est-il adéquat pour s'appliquer au cyberespace ?

Oui – mais il est nécessaire que les discussions entre les États se poursuivent afin de préciser un certain nombre de points, notamment des *notions clés du droit international humanitaire*.

D'une part, une des grandes forces du droit international humanitaire tient au fait que les États ont formulé des règles de manière à ce qu'elles puissent s'appliquer à « toutes les formes de guerre et à toutes les armes » y compris « celles (…) de l'avenir » (C.I.J., *armes nucléaires, avis consultatif*, par. 86). En

effet, les règles fondamentales sont simples : il est interdit d'attaquer les civils et les biens civils ; les armes et attaques indiscriminées sont prohibées ; les attaques disproportionnées sont interdites ; les services médicaux doivent être respectés et protégés (voir *la position du CICR*, pp. 6-8). Ces sont là des règles qui, comme bien d'autres, s'appliquent au cyberespace et doivent être respectées.

D'autre part, le CICR a conscience qu'il s'agit là de questions sur lesquelles les opinions des États et d'autres experts divergent. Parmi ces points de désaccord, il y a par exemple la question de savoir si les données civiles doivent bénéficier de la même protection que les biens civils ou encore si les cyberopérations qui perturbent les systèmes sans causer de dommage physique doivent être considérées comme « une attaque » au sens du droit international humanitaire (voir *la position du CICR*, pp. 9 et 10). Mais nous ne devrions pas oublier que ces divergences entre des États et les experts juridiques sur certaines questions ont toujours existé. Et, malgré tout, ces désaccords sur l'interprétation des différentes règles et notions ne remet pas en cause de l'applicabilité du droit en tant que tel.

7. Le droit existant est-il suffisant ou faut-il une nouvelle Convention sur le cyber ?

Dans les débats multilatéraux relatifs à l'application du droit international au cyberespace, la question de savoir si une nouvelle convention concernant le recours à des cyberopérations dans les conflits armés est ou pas nécessaire, n'est pas la première des priorités. En effet, ce sujet couvre un plus large spectre de questionnements et soulève une multitude de questions en droit international qui vont bien au-delà du droit international humanitaire.

Les États ont exprimé différents points de vue sur cette question.

S'agissant particulièrement du droit international humanitaire, l'objet et le but de ce corpus juridique est de restreindre l'emploi de moyens et méthodes de guerre afin de protéger les civils et les biens civils des effets des hostilités. Le CICR a appelé les États à adopter des positions claires sur la manière dont le droit international humanitaire doit s'appliquer au cyberespace, la protection qu'il offre d'une part aux infrastructures civiles, afin qu'elles ne soient pas endommagées par des moyens cybernétiques et, d'autre part, aux données personnelles. De telles positions vont déterminer dans quelle mesure le droit international humanitaire peut offrir une protection aux civils et aux infrastructures civiles. De la même manière, elles influenceront l'examen des règles, afin de déterminer si celles qui existent déjà sont adaptées et suffisantes, ou si de nouvelles règles seraient nécessaires pour réglementer les cyberopérations en période de conflit armé.

Si les États estiment qu'il est nécessaire de développer de nouvelles règles, il faudra que celles-ci soient élaborées à partir du cadre juridique existant et le renforcer. Dans le même temps, les cyberopérations pendant un conflit armé ne sont pas menées dans un vide juridique. Elles doivent être conformes aux règles existantes du droit international humanitaire.

Tags: Conventions de Genève, Coronavirus, COVID-19, cyber warfare, cyberattaques, cyberguerre, cybersécurité, droit international humanitaire

Ceci pourrait vous intéresser

Lorsque les hostilités prennent fin mais que les souffrances demeurent : la nécessité de poursuivre des activités humanitaires au lendemain d'un conflit armé

15 minutes de lecture

Droit et conflits / Nouvelles technologies Émilie Charpentier

Le DIH et les territoires occupés

17 minutes de lecture

Droit et conflits / Nouvelles technologies Tristan Ferraro & Mikhail Orkin

Alors que le conflit armé en Ukraine s'installe, les civils pris au piège de ce conflit subissent de plein fouet les effets des ...

Les conflits armés ont des conséquences à long terme sur les populations, même bien longtemps après la fin du conflt. Les organisations humanitaires ...