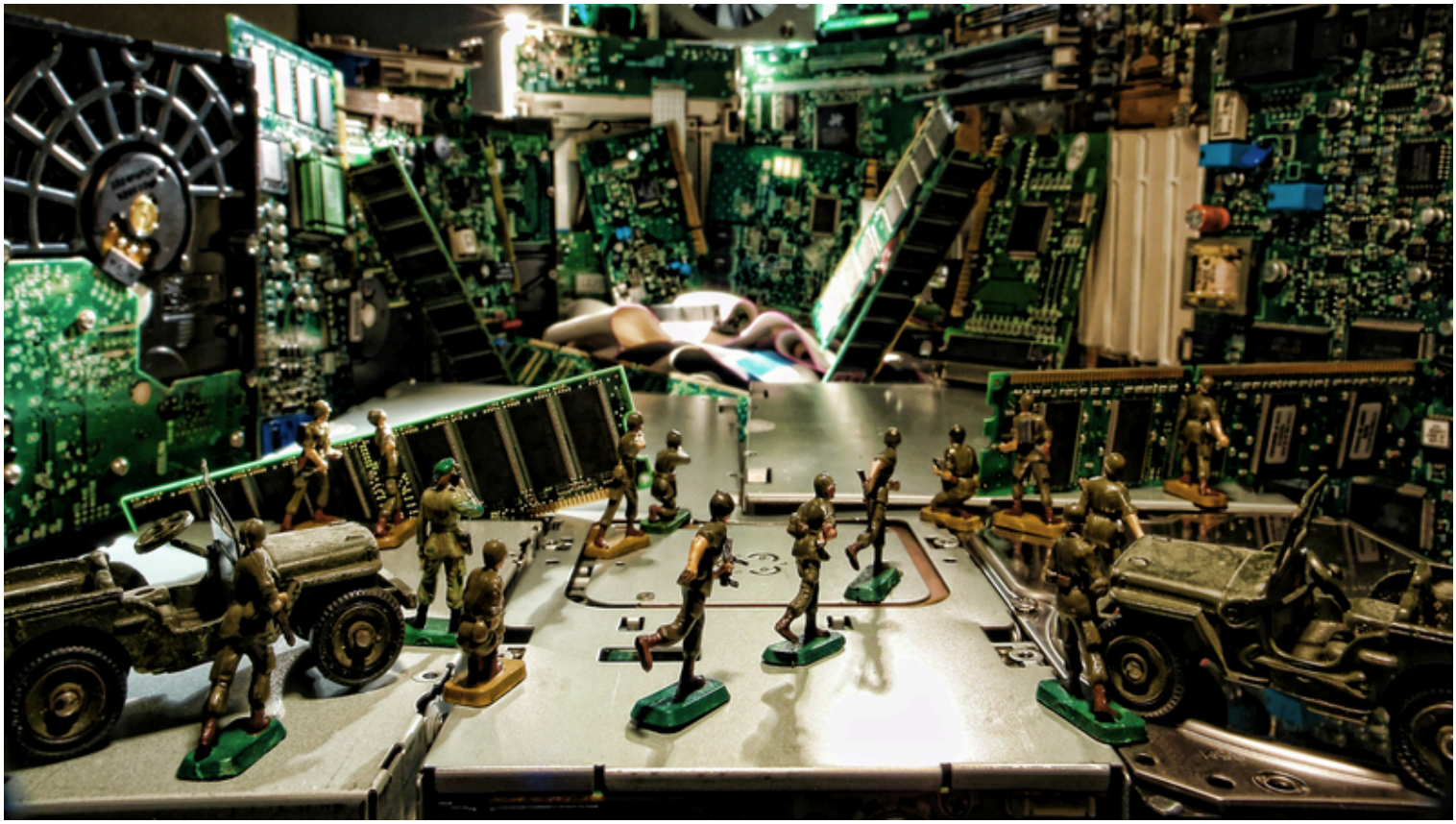
DROIT & POLITIQUES
HUMANITAIRES

Même les « cyberguerres » ont des limites. Et si elles n'en avaient pas ?

décembre 19, 2025, Action humanitaire / Droit et conflits / Nouvelles technologies
14 mins read


Tilman Rodenhäuser
Conseiller juridique thématique, CICR


Kubo Mačák
Conseiller juridique, CICR



Les cyberopérations sont devenues une réalité des conflits armés contemporains, et il est probable qu'elles soient de plus en plus utilisées à l'avenir. En réponse à cette tendance, le CICR a longtemps soutenu l'idée que le droit international humanitaire (DIH) régit, et limite, toute utilisation de cyberopérations pendant les conflits armés. Mais qu'est-ce qui est vraiment en jeu ?

Dans cet article, Tilman Rodenhäuser et Mačák Kubo, conseillers juridiques au CICR, expliquent que le risque de blesser des humains est important, et que la question en apparence technique de l'applicabilité du DIH dans le cyberespace a en réalité une vraie incidence dans le monde réel.

Dans un monde de plus en plus numérique, les États et les groupes armés non étatiques ont de plus en plus recours aux cybercapacités dans leurs opérations militaires, et cette tendance devrait se renforcer. Toutefois, un débat persiste, notamment dans le cadre des deux processus multilatéraux menés sous l'égide des Nations unies, quant à la manière dont les réglementations internationales en vigueur s'appliquent à de telles activités dans le cyberespace.

Au cours des 20 dernières années, la position du CICR n'a pas changé : pour nous, il ne fait aucun doute que le droit international humanitaire (DIH, également appelé le « droit de la guerre ») s'applique, et limite par conséquent, les cyberopérations pendant les conflits armés (voir exemple *ici*, pages 41-43, ou *ici*, page 5).

Cependant, en terme de protection humanitaire, des questions juridiques techniques peuvent obscurcir les avantages réels qu'offre l'application de cette branche du droit aux cyberopérations. Ainsi, au lieu de se risquer à un débat superflu, imaginons un moment que le DIH ne s'applique pas aux cyberopérations pendant les conflits armés : à quoi pourraient ressembler les conflits modernes ?

La population pourrait être privée de services essentiels, tels que l'électricité

Les cyberopérations contre les réseaux électriques ne sont pas *sans précédent*. En situation de conflit armé, les belligérants peuvent être tentés de pirater le réseau électrique en territoire ennemi, couper l'électricité dans les zones peuplées, et tout mettre en œuvre pour éviter que le courant ne soit rapidement rétabli, que ce soit pour affaiblir l'adversaire ou saper le moral de la population. De tels incidents pourraient sévèrement aggraver la vulnérabilité de la population dans les régions affectées par ce conflit.

Cependant, le DIH impose des limites claires sur de telles opérations si elles sont redirigées contre, ou si l'on s'attend à ce qu'elles endommagent accidentellement, des biens de caractère civil. Le principe de distinction, *considéré* par la Cour internationale de justice (CIJ) comme l'un des « principes cardinaux » qui constituent le « tissu du droit humanitaire », *condamne* les attaques contre les biens de caractère civil. De plus, les règles du DIH *interdisent* de rendre inutilisables des objets indispensables à la survie de la population, tels que des installations d'eau potable. C'est pourquoi toutes les parties de conflits armés doivent rediriger leurs attaques, y compris celles qui utilisent des cyberoutils, seulement contre des objectifs militaires, et doivent *veiller constamment* à épargner les populations et biens de caractère civil des effets des hostilités.

Sans le DIH, quel cadre juridique apporterait une protection efficace aux infrastructures civiles essentielles contre les cyberopérations destructrices pendant les conflits armés ? Les coupures de courant dans les zones peuplées pourraient durer plusieurs jours, voire plusieurs semaines. Dans les climats froids où le chauffage dépend de l'électricité, être privé de celui-ci peut littéralement faire la différence entre la vie et la mort, comme l'ont montré les *récents évènements* survenus aux États-Unis. Dans de telles conditions climatiques, les coupures de courant peuvent également provoquer des dommages collatéraux, par exemple, un gel de l'eau dans les canalisations, les faisant éclater et interrompant ainsi l'approvisionnement en eau. Pendant un conflit armé, le risque de porter atteinte à la population est particulièrement élevé, car sa vulnérabilité est souvent exacerbée par les hostilités. Protéger les civils dans ces situations exceptionnelles est la « raison d'être » du DIH.

Les patients dans les hôpitaux seraient gravement menacés

Un autre exemple simple et précis d'un domaine où le DIH est d'une nécessité critique concerne les cyberopérations contre le secteur des soins de santé en période de conflit armé. Si le DIH ne s'appliquait pas dans de telles opérations, un commandant militaire peu scrupuleux pourrait remettre en question les obstacles juridiques à la diffusion de logiciels malveillants désactivant indirectement les ordinateurs et les réseaux des hôpitaux situés en territoire ennemi.

Là encore, le DIH ne laisse planer aucun doute sur la question. Ses règles exigent que les *unités*, les *moyens de transport* et le *personnel sanitaires* — peu importe qu'ils assistent les forces ennemies ou les civils — soient respectés et protégés par les parties au conflit en tout temps. Ainsi, comme détaillés dans un article que nous avons publié il y a un an, les belligérants ne doivent pas nuire aux infrastructures sanitaires par le biais des cyberopérations et doivent faire preuve d'une grande prudence afin d'éviter de causer indirectement des dommages par ces opérations. Cette analyse a également *servi de base* à la rédaction d'une *déclaration* signée par plus d'une centaine d'avocats en droit international dans le cadre d'un processus organisé par l'Université d'Oxford, réaffirmant cette protection (voir paragraphe 5).

« Il est inconcevable — et franchement inacceptable — de s'attaquer aux soins de santé, en particulier pendant la pandémie de la COVID », a *souligné* Peter Maurer, le président du CICR, en mai 2020. Pourtant, sans les interdictions énoncées par le DIH, quelle protection juridique existerait contre le risque que les hôpitaux soient endommagés, ou pire, directement visés, par des cyberopérations lors des conflits armés ? En effet, la pandémie de la COVID-19 nous a rappelé que la protection du secteur médical est plus importante que jamais : si les hôpitaux ne fonctionnent plus, les traitements qui permettent de sauver des vies ne seront pas disponibles.

Les États tiers seraient exposés à des cyber-dommages involontaires, mais potentiellement importants

L'une des principales caractéristiques du cyberespace est sa nature interconnectée. Cela signifie qu'une cyberopération contre un système spécifique peut avoir des répercussions sur plusieurs autres systèmes, causant potentiellement des effets indiscriminés à *échelle mondiale*. En particulier, si un logiciel malveillant est programmé pour se répandre automatiquement et sans limites géographiques ou autres, il peut très bien affecter au moins les machines qui utilisent un logiciel similaire dans le monde entier, où qu'elles se trouvent.

Sous le DIH, les attaques qui emploient des moyens ou des méthodes de guerre qui ne peuvent pas être redirigées contre des objectifs militaires spécifiques, ou dont les effets ne peuvent pas être limités de manière licite, sont *prohibées*. Dans le contexte cybernétique, cela *signifie* que les cyberoutils qui répandent et causent des dégâts sans discrimination sont illégaux. Par conséquent, l'interdiction du DIH des attaques sans discrimination protège non seulement les civils dans les territoires touchés par les hostilités, mais aussi — en pratique — les États tiers qui peuvent être affectés par inadvertance par de telles attaques.

Par conséquent, une régulation efficace des cyber activités pendant des conflits armés concerne tous les États. Et ce, qu'ils développent ou non des cybercapacités militaires, où qu'ils se trouvent et qu'ils prennent part ou qu'ils aient pris part à un conflit armé ou non.

Les limites imposées par le DIH font la différence

Mais est-il vraiment important que le DIH s'applique formellement aux cyberopérations telles que celles qui ont été décritesplus haut ? On pourrait croire qu'aucun acteur responsable n'attaquerait des hôpitaux ou ne laisserait des civils mourir de froid, peu importe que ces opérations soient prohibées par le droit ou non. Après tout, une telle conduite est si ouvertement honteuse que le DIH n'est pas nécessaire pour la limiter : tout le monde ne sait-il pas que des attaques contre les hôpitaux et les civils sont inacceptables ?

Cependant, l'histoire montre que la question de savoir si le DIH s'applique et protège les personnes affectées par un conflit armé a des conséquences réelles et concrètes. Si le droit est rarement le seul facteur qui détermine le comportement des belligérants, il existe de nombreux exemples dans lesquels le *DIH fait la différence*. Par exemple, des études ont suggéré que les prisonniers de guerre étaient bien mieux traités par les États partie à la *Convention relative au traitement des prisonniers de guerre de 1929*. En revanche, le traitement des prisonniers de guerre qui n'étaient pas protégés par cette convention était nettement plus sévère, entraînant de nombreux décès et des souffrances innommables (voir, par exemple, *ici*, p. 3, ou *ici*, paragraphes 5-7 et 12).

C'est aussi la raison pour laquelle les États se sont eux-mêmes *engagés* à diffuser les dispositions du DIH aussi largement que possible aussi bien en temps de paix qu'en période de conflit armé. Cette obligation est basée sur l'idée qu'une solide connaissance des règles du DIH est essentielle pour une application efficace et, par conséquent, pour la protection des victimes des conflits armés. Pour les forces armées, assurer le respect du DIH est une activité complexe, qui nécessite des moyens formels et informels d'internaliser les règles de retenue établies par le DIH (voir le rapport complet *ici*, pages 28-31). Une formation intense et répétée de ces règles dans tous les contextes pertinents, y compris le cyberespace, est essentielle pour garantir que tous les combattants comprennent, bien à l'avance et sans l'ombre d'un doute, quels sont les personnes et les biens qui sont strictement protégés et ne doivent en aucun cas être pris pour cibles.

Enfin, l'applicabilité du DIH aux cyberopérations est également une condition préalable essentielle pour que les auteurs de violations soient tenus de rendre compte de leurs actes. Les États ont l'obligation juridique de rechercher des personnes susceptibles d'avoir commis ou ordonné la commission de crimes de guerre — en d'autres termes, des violations graves du DIH — et d'engager des poursuites criminelles à l'encontre de ces individus (voir *ici*, paragraphe 12). Après tout, même des belligérants par ailleurs responsables peuvent contenir des « pommes pourries » qui choisiront d'agir en dehors des limites établies d'un comportement acceptable. Le fait qu'une telle conduite puisse se produire dans le cyberespace ne justifie pas de la récompenser par l'impunité.

Conclusion et voie à suivre

Certes, le DIH n'est pas la seule branche du droit international à imposer des limites aux cyberconduite hostile. Plus particulièrement, les États ont *établi* dans le Protocole additionnel I qu'aucune lecture du DIH « ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies ». En d'autres termes, une cyberopération qui est conforme au DIH peut néanmoins constituer une violation, par exemple, de l'interdiction du recours à la force. De plus, certaines cyberopérations mentionnées dans cet article peuvent mettre en jeu d'autres règles juridiques internationales, notamment les principes de souveraineté et de non-intervention, ou le droit international des droits de l'homme — comme nous l'avons détaillé dans l'*analyse* déjà mentionnée des protections du droit international contre les cyberopérations ciblant les soins de santé.

Cependant, il ne fait aucun doute que parmi les différentes branches du droit international, le DIH joue un rôle central dans la protection des civils contre les dangers posés par les conflits armés. Comme l'a *déclaré* la CIJ, le DIH est l'ensemble de droits qui « régit la conduite des hostilités dans un conflit armé et vise à protéger différentes catégories de personnes et de biens » (au paragraphe 153). Contrairement aux autres règles mentionnées ci-dessus, les groupes armés non étatiques sont également tenus de respecter le DIH lorsqu'ils prennent part à conflit armé (voir *ici*, paragraphes 539-542, ou voir *ici*, page 8). Pour toutes ces raisons, il est essentiel de comprendre dans quelle mesure le DIH protège les diverses catégories de personnes mentionnées par la CIJ contre les cyber-dommages, qu'il s'agisse de civils dans les zones affectées par un conflit, de personnel hospitalier ou de patients, ou des biens tels que les infrastructures civiles essentielles.

Comme nous l'avons expliqué, l'utilisation des cyberopérations dans un conflit armé peut avoir de réelles conséquences humanitaires — surtout si elles sont utilisées d'une manière non conforme au DIH. Comme indiqué dans le *projet de rapport* du Groupe de travail à composition non limitée des Nations unies, qui est en cours de négociation cette semaine, « le droit international humanitaire réduit les risques et les dommages potentiels pour les civils et les biens de caractère civil ainsi que pour les combattants dans le contexte d'un conflit armé » (au paragraphe 84 ; pour plus de contexte, voir également l'article en anglais du *commentaire* du CICR sur le rapport). De plus en plus d'États affirment expressément l'applicabilité du droit international humanitaire aux cyberopérations menées dans le cadre de conflits armés. Selon nous, il est impératif que tous les États affirment cette position qui fait de plus en plus l'objet d'un consensus. La communauté internationale ne devrait laisser aucune place au doute : même les cyberguerres ont des limites.

Cet article a été initialement publié en anglais sur EJIL:Talk!. Il a été traduit par Tristan Rochas, en Master 1 de Traduction spécialisée multilingue de l'Université de Grenoble Alpes, en France.

Voir aussi

- Kubo Mačák, Tilman Rodenhäuser, *Vers une interprétation commune : l'application des principes établis du DIH aux cyberopérations*, 27 août 2025
- Helen Durham, *Les cyberopérations en période de conflit armé : 7 questions juridiques et politiques essentielles*, 26 mars 2020.

Tags: conflit armé, Conventions de Genève, Cour internationale de Justice, cyber, cyberguerre, cyberopérations, DIH, droit international humanitaire, technologies numériques

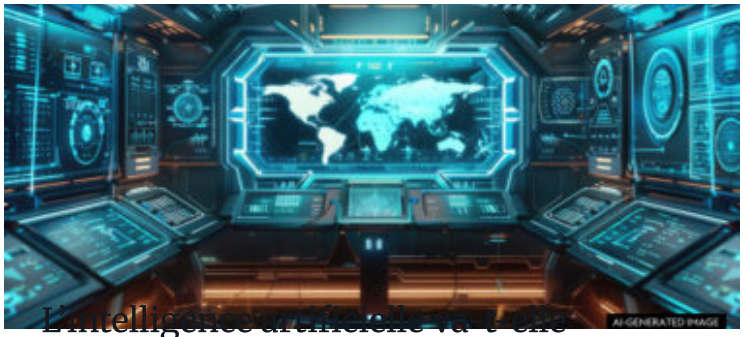
You should also read these articles

Comprendre les liens entre les violences sexuelles et les armes en période de conflit pour renforcer la prévention

9 mins read

Action humanitaire / Droit et conflits / Nouvelles technologies Hana Salama

La violence sexuelle est souvent considérée comme une arme de guerre, mais les armes réelles ...



L'intelligence artificielle va-t-elle profondément transformer la manière dont les conflits armés sont déclenchés, menés et résolus ?

14 mins read

Action humanitaire / Droit et conflits / Nouvelles technologies Erica Harper

Dans le cadre du débat concernant les effets de l'intelligence artificielle (IA) sur les stratégies ...