DROIT & POLITIQUES
HUMANITAIRES

# Vers une interprétation commune : l'application des principes établis du DIH aux cyberopérations

*août 27, 2025*, Droit et conflits / Nouvelles technologies
11 minutes de lecture


**Tilman Rodenhäuser**
Conseiller juridique thématique, CICR


**Kubo Mačák**
Conseiller juridique, CICR

*Les cyberopérations sont aujourd'hui devenues réalité dans les conflits armés, et leur utilisation devrait continuer de s'accroitre dans le futur. Au vu de cette tendance, le CICR soutient depuis longtemps l'idée que le droit international humanitaire (DIH) régit et limite toute utilisation de cyberopérations en période de conflit armé. Mais qu'est-ce que cela implique vraiment dans la pratique ?*

*Dans cet article, les conseillers juridiques du CICR Kubo Mačák et Tilman Rodenhäuser expliquent plus précisément de quelle manière et à quel moment le DIH est applicable à l'utilisation des technologies de l'information et de la communication (TIC) par les États, en particulier ses principes d'humanité, de nécessité, de distinction et de proportionnalité. Avec cet article, ils inaugurent la nouvelle série d'articles du CICR sur les cyberopérations pendant des conflits armés.*

Une *étude* récente estime que plus de 60 États ont constitué des cyberforces actives au sein de leurs structures militaires. Les parties aux conflits armés, ainsi qu'une série d'acteurs non gouvernementaux ou dont l'affiliation n'est pas clairement établie, ont utilisé des cybercapacités militaires dans le contexte des

conflits armés contemporains, soit sous forme d'opérations autonomes, soit en lien avec des opérations cinétiques. Le conflit armé international en cours entre la Russie et l'Ukraine n'en est que l'exemple le plus récent.

Le fait que ces événements puissent avoir un coût humain élevé n'est guère une nouveauté en 2023. Dès 2001, Knut Dörmann, alors conseiller juridique du CICR, avait *alerté* sur le fait que les cyberopérations lancées contre des industries, des infrastructures ou des télécommunications pouvaient avoir des conséquences dévastatrices si certains dysfonctionnements du système venaient à en résulter. Aujourd'hui, cette analyse est reprise dans des déclarations de consensus des États dans les plus hautes sphères : par exemple, un groupe de travail à composition non limitée mandaté par les Nations unies a *affirmé* en 2021 que les cyberopérations pouvaient gravement affecter les infrastructures civiles et avoir ainsi des « conséquences humanitaires dévastatrices » (paragraphe 18).

Les menaces numériques qui pèsent sur les populations civiles nécessitent de toute urgence des discussions ouvertes et des clarifications sur des questions juridiques complexes. Quelles sont les limites imposées par les règles existantes du DIH aux cyberopérations qui risquent de perturber les services et infrastructures civils essentiels ou de manipuler et d'effacer des données ? Qui est responsable du comportement des acteurs non étatiques dans le domaine des TIC, quelles sont les obligations de ces acteurs et quelles sont les conséquences auxquelles ils s'exposent s'ils prennent part aux hostilités ?

Toutefois, la réponse apportée en matière de réglementation au niveau international a été plutôt mesurée. Bien que les discussions multilatérales relatives à la « sécurité de l'information » aient commencé dès 1998, lorsque la Fédération de Russie a présenté une première *résolution* sur le sujet, il a fallu attendre 2013 pour qu'un *Groupe d'experts gouvernementaux des Nations unies (GEG)* parvienne à un *consensus* sur la question fondamentale de l'applicabilité du droit international dans le cyberespace (paragraphe 19).

La question des cyberopérations pendant les conflits armés figure également depuis longtemps à l'ordre du jour des discussions multilatérales. En 2015, un autre GEG a *souligné* que « les principes de droit internationaux reconnus, y compris, lorsqu'ils sont applicables, les principes d'humanité, de nécessité, de proportionnalité et de discrimination » (paragraphe 28(d)). Six ans plus tard, le GEG final a *expressément lié* ces principes au corpus juridique auquel ils appartiennent, à savoir le droit international humanitaire (paragraphe 71(f)). Dans le même rapport, le GEG a reconnu qu'il convenait d'examiner plus avant « de quelle manière et à quel moment » ces principes s'appliquaient à l'utilisation des TIC par les États (*ibid.*).

Aujourd'hui, le CICR publie quatre courts articles destinées à appuyer les discussions sur ces questions du « comment » et du « quand » le DIH est-il applicable aux cyberopérations. Ils seront officiellement présentés à New York lors de la partie consacrée au droit international du Groupe de travail à composition non limitée (GTCNL) des Nations unies sur la sécurité des technologies de l'information et de la communication et leur utilisation, dont le *mandat* comprend la définition d'interprétations communes de concernant l'application du droit international dans le domaine des TIC. Par ailleurs, nous espérons que le contenu de ces articles suscitera l'intérêt de l'ensemble de la communauté des praticiens du droit international et des universitaires travaillant dans ce domaine.

Nous expliquons dans cet article de quelle manière et à quel moment le DIH et ses principes fondamentaux s'appliquent dans le domaine des TIC. Pour chaque question, nous proposons une brève explication de ce qu'il faut retenir (mise en gras en haut de l'article en question), un bref aperçu du contenu de l'article et un lien vers le texte intégral, où vous pourrez en apprendre davantage.

## Article 1 : Dans quels cas le droit international humanitaire s'applique-t-il à l'utilisation des technologies de l'information et de la communication ?

**Le droit international humanitaire s'applique à l'utilisation des technologies de l'information et de la communication dans les situations de conflit armé.**

Le premier élément de réponse à la question de savoir « quand » le DIH est applicable est évident, mais essentiel. En effet, comme l'a *souligné* le GEG, le DIH ne s'applique que dans les situations de conflit armé (en dehors de certaines exceptions, se référer, par exemple, à *cet article* , note 2). Il convient de rappeler que déterminer les cas où le DIH s'applique est une question juridiquement distincte de celle des comportements qui constituent une « menace ou un recours à la force » ou une « attaque armée » interdits en vertu de la Charte des Nations unies. De plus, les situations dans lesquelles le DIH s'applique sont soit des conflits armés entre États (« conflits armés internationaux »), soit des conflits armés entre États et groupes armés non étatiques, ou entre des groupes armés exclusivement (« conflits armés non internationaux »). L'article analyse donc les situations impliquant l'utilisation de cybercapacités qui peuvent être considérées comme relevant de l'un de ces types de conflit armé. Bien que certains aspects du droit applicable restent incertains, il ne fait aucun doute que le DIH s'applique lorsqu'une cyberopération est menée conjointement ou à l'appui d'opérations militaires « physiques » ou « cinétiques » classiques dans le cadre d'un conflit armé en cours.

*Lire l'article complet ici.*

## Article 2 : Les principes d'humanité et de nécessité selon le DIH

**Les principes fondamentaux d'humanité et de nécessité militaire constituent la base et le fil conducteur de l'ensemble du cadre normatif du droit international humanitaire. Toutes les règles du DIH témoignent d'un équilibre subtil entre ces deux principes, qui à leur tour guident l'interprétation de ces règles. Les deux principes imposent également des limites au-delà des règles spécifiques, y compris dans le domaine des technologies de l'information et de la communication.**

Depuis la *Déclaration de Saint-Pétersbourg de 1868*, il est entendu qu'à mesure que le DIH est élaboré, les États ne cessent de réévaluer quand, et dans quelle mesure, « les nécessités de la guerre doivent s'arrêter devant les exigences de l'humanité ». Ainsi, les deux premiers des quatre « principes juridiques établis » mentionnés par le GEG en 2015 sont traités dans un seul article. L'article examine comment les principes d'humanité et de nécessité militaire, deux principes étroitement liés, influencent l'application et l'interprétation du DIH dans le monde numérique. Il montre qu'ils sont particulièrement importants dans les cas où

l'interprétation des règles existantes applicables aux cyberopérations demeure incertaine. C'est le cas notamment de la *règle* définissant une « attaque » selon le DIH.

*Lire l'article complet ici.*

## Article 3 : Le principe de distinction selon le DIH

**Lors de l'utilisation des technologies de l'information et de la communication, le principe de distinction exige que les parties à un conflit armé fassent en tout temps la distinction entre les civils et les combattants mais également entre les biens de caractère civil et les objectifs militaires. Les cyberattaques ne peuvent être dirigées que contre des combattants ou des objectifs militaires. Les cyberattaques ne doivent pas être dirigées contre des civils ou des biens de caractère civil. Les cyberattaques sans discrimination sont interdites.**

La Cour internationale de justice a *défini* le principe de distinction comme un principe « cardinal » et « intransgressible » qui fait partie du l'essence du DIH (paragraphes 78-79). Ce principe exige que les parties à un conflit armé s'abstiennent de lancer des cyberopérations qualifiées d'attaques contre des infrastructures ou des biens de caractère civil. Le principe de distinction interdit également les attaques sans discrimination, y compris lors de l'utilisation de moyens ou méthodes de guerre numériques. L'article examine en outre comment le principe de distinction limite les cyberopérations autres que les attaques. Enfin, il examine comment le respect de ce principe peut être assuré dans le monde numérique, notamment par le développement responsable de cyberoutils et la vérification minutieuse des cibles. Ses recommandations, comme celles figurant dans l'article suivant, sont fondées sur l'étroite collaboration du CICR avec des experts techniques, sujet que nous avons également abordé sur *cet article*.

*Lire l'article complet ici.*

## Article 4 : Le principe de proportionnalité selon le DIH

**Dans l'utilisation des technologies de l'information et de la communication, le principe de proportionnalité interdit aux parties à un conflit armé de lancer une cyberattaque contre un objectif militaire dont on peut s'attendre à ce qu'elle cause incidemment des dommages aux civils qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu.**

Le principe de proportionnalité prévu par le DIH est essentiel pour protéger les civils et les infrastructures civiles en période de conflit armé et, plus particulièrement, dans l'environnement interconnecté des TIC. Il limite l'ampleur des dommages causés incidemment aux civils qui sont autorisés lorsque les parties à un conflit armé attaquent des objectifs militaires, y compris par le biais de moyens ou méthodes de guerre numériques. Cet article explique que l'évaluation des dommages causés incidemment doit prendre en compte les effets directs et indirects des cyberopérations. Il recommande aux États qui prévoient de recourir à des cyberopérations en période de conflit armé d'adapter les procédures existantes d'évaluation du respect du principe de proportionnalité (parfois également appelées « méthodes d'évaluation des dommages collatéraux ») pour tenir compte des défis spécifiques posés par les TIC.

*Lire l'article complet ici.*

Avec ces quatre articles, le CICR entend contribuer aux débats actuels sur l'application du DIH aux cyberopérations en période de conflit armé. Ils ne sont ni conçus ni rédigés comme des réponses définitives aux questions et principes qu'ils abordent, mais plutôt comme un moyen de renforcer les capacités et de faire avancer le débat. Nous pensons que ces discussions nous permettront de nous rapprocher d'une compréhension commune de l'application et de l'interprétation du DIH dans le monde numérique, protégeant ainsi les civils, les données civiles et les infrastructures civiles des effets préjudiciables des cyberopérations en période de conflit armé.

### Voir aussi

- Ruben Stewart, *Entre avancées technologiques et nouvelles tactiques, l'évolution de la guerre brouille les repères traditionnels*, 11 juin 2025
- Tilman Rodenhäuser, Mauro Vignati, *8 règles destinées aux hackers civils en temps de guerre et 4 obligations des Etats pour limiter leur action*, 12 janvier 2024

Tags: conflit armé, cyberattaques, cyberguerre, cyberopérations, DIH, droit international, droit international humanitaire, Nations Unies, opérations d'information, technologies numériques

## *Ceci pourrait vous intéresser*

## Une catastrophe évitable : retenir l'humanité au bord de l'abîme nucléaire

14 minutes de lecture

Droit et conflits / Nouvelles technologies Dominique Loye

Les 6 et 9 août 1945, Hiroshima et Nagasaki sont devenues les premières et, à ce jour, les seules, cibles d'armes nucléaires en ...

## Hors réseau et en danger : les conséquences humanitaires d'une connectivité interrompue

16 minutes de lecture

Droit et conflits / Nouvelles technologies

À l'heure où, partout dans le monde, la population dépend toujours davantage des réseaux numériques et de télécommunications pour accéder à des services ...