ICRC

Le droit international humanitaire et les cyberopérations pendant les conflits armés

Position du CICR

Document soumis au Groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale ainsi qu'au Groupe d'experts gouvernementaux sur la promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale

Novembre 2019

Sommaire

Résumé 2

I. Introduction 4

II. Le coût humain potentiel des cyberopérations 4

III. L'application du DIH aux cyberopérations pendant les conflits armés 5

IV. La protection accordée par le DIH existant 6

V. La nécessité de débattre de la *manière* dont s'applique le DIH 8

L'utilisation du cyberespace à des fins militaires et les conséquences sur son caractère civil 8

La notion d'« attaque » au regard du DIH et les cyberopérations 9

Les données civiles et la notion de « bien civil » 10

VI. L'attribution des actes dans le cyberespace aux fins de la responsabilité des États 10

VII. Conclusion 11

Résumé

- **Les cyberopérations pendant les conflits armés sont désormais une réalité**. Le Comité international de la Croix-Rouge (CICR) est préoccupé par le **coût humain potentiel** du recours croissant aux cyberopérations dans les conflits armés.
- **Le CICR considère que le droit international humanitaire (DIH) limite les cyberopérations pendant les conflits armés,** de même qu'il limite l'emploi de tout autre type d'arme, de moyen et de méthode de guerre dans un conflit armé, qu'il soit nouveau ou ancien.
- Affirmer que le DIH est applicable ne légitime en rien la cyberguerre, ni toute autre forme de guerre. **Tout emploi de la force — cybernétique ou cinétique — par les États demeure régi par la Charte des Nations Unies et par les règles pertinentes du droit international coutumier,** en particulier en ce qui concerne l'interdiction de l'emploi de la force. Les différends internationaux doivent être réglés par des moyens pacifiques, dans le cyberespace comme dans tous les autres cadres.
- Il est aujourd'hui de la plus haute importance que **la communauté internationale affirme l'applicabilité du DIH** aux cyberopérations pendant les conflits armés. Le CICR appelle aussi de ses vœux **la tenue de discussions entre experts gouvernementaux et non gouvernementaux sur la *manière* dont s'appliquent les règles existantes du DIH** et sur la question de savoir si le droit existant est adapté et suffisant. À cet égard, **le CICR se félicite des discussions en cours au niveau intergouvernemental** dans le cadre de deux processus mis sur pied par l'Assemblée générale des Nations Unies.
- Les événements des dernières années ont montré que les cyberopérations — pendant les conflits armés ou en dehors de ceux-ci — peuvent perturber le fonctionnement d'infrastructures civiles essentielles et entraver la prestation de services essentiels à la population. **Dans le contexte des conflits armés, les infrastructures civiles sont protégées contre les cyberattaques par les principes et les règles du DIH existant,** en particulier les principes de distinction, de proportionnalité et de précaution dans l'attaque. Le DIH accorde aussi une protection spéciale, entre autres, aux hôpitaux et aux biens indispensables à la survie de la population civile.
- **L'utilisation, dans les conflits armés, de cyberoutils qui se diffusent et qui causent des dommages sans discrimination est interdite.** D'un point de vue technologique, certains cyberoutils peuvent être conçus et employés pour ne cibler et n'endommager que des objets spécifiques et pour ne pas se diffuser ni causer des dommages sans discrimination. Toutefois, l'interconnectivité propre au cyberespace signifie que tout dispositif qui se connecte à Internet peut être pris pour cible à partir de n'importe quel lieu dans le monde, et qu'une cyberattaque contre un système spécifique peut avoir des conséquences pour divers autres systèmes. Il existe, de ce fait, un risque réel que des cyberoutils ne soient pas conçus ou employés dans le respect du DIH, délibérément ou par erreur.
- **C'est l'interprétation par les États des règles de DIH existantes qui déterminera l'étendue de la protection offerte par le DIH contre les effets des cyberopérations.** Les États devraient, en particulier, s'engager sans ambiguïté à interpréter le DIH de manière

à préserver les infrastructures civiles de perturbations importantes et à protéger les données civiles. Ces prises de position influenceront aussi l'évaluation de l'adéquation des règles existantes ou de la nécessité de créer des règles nouvelles. Au cas où les États percevraient le besoin d'élaborer de nouvelles règles, ils devraient **se fonder sur le cadre juridique existant, y compris le DIH, et le renforcer**.

I. Introduction

Les cyberopérations pendant les conflits armés sont désormais une réalité[1]. Bien que seuls quelques États aient publiquement reconnu mener de telles opérations, un nombre croissant d'États développent des cybercapacités militaires, et la probabilité de leur emploi à l'avenir est de plus en plus grande.

En outre, des progrès techniques importants ont été réalisés en matière de cybercapacités offensives : les événements des dernières années ont montré que les cyberopérations peuvent porter gravement atteinte aux infrastructures civiles et pourraient nuire à des êtres humains.

Conformément à sa mission et à son mandat, le Comité international de la Croix-Rouge (CICR) est concerné en premier lieu par le recours aux cyberopérations en tant que moyens et méthodes de guerre dans un conflit armé et par la protection que confère le DIH contre leurs effets.

Le CICR se félicite des discussions qui sont en cours à l'échelon intergouvernemental dans le cadre des deux processus mis sur pied par l'Assemblée générale des Nations Unies : le Groupe de travail à composition non limitée chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et le Groupe d'experts gouvernementaux sur la promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Ces deux organes ont pour tâche d'étudier « la manière dont le droit international s'applique à l'utilisation des technologies de l'information et des communications par les États[2] ». Le CICR soumet le présent document présentant sa position aux deux groupes, à l'appui des délibérations des États sur la question.

Ce document de position se limite aux questions d'ordre juridique et humanitaire découlant du recours à des cyberopérations pendant les conflits armés. Il n'aborde pas les questions liées au cadre juridique applicable aux cyberopérations sans rapport avec un conflit armé.

II. Le coût humain potentiel des cyberopérations

Dans le cadre de conflits armés, des cyberopérations ont été lancées en appui d'opérations cinétiques ou parallèlement à de telles opérations. Les cyberopérations peuvent offrir des possibilités supplémentaires par rapport à d'autres moyens ou méthodes de guerre, mais elles présentent aussi des risques. D'une part, les cyberopérations peuvent permettre aux parties à un conflit armé de parvenir à leurs fins militaires sans nuire à la population civile ni causer des dommages matériels aux infrastructures civiles. D'autre part, les cyberopérations récentes — menées, pour la plupart, hors d'un contexte de conflit armé — montrent que des acteurs recourant à des technologies très avancées sont aujourd'hui capables de perturber la fourniture de services essentiels à la population civile.

Des cyberopérations peuvent permettre à des belligérants de pénétrer un système et de collecter, extraire, modifier, encrypter ou détruire des données. Il est aussi possible d'utiliser un système informatique préalablement piraté pour déclencher, altérer ou manipuler d'une autre manière des processus qui dépendent de ce système. Toute une série de « cibles » dans le monde réel — industries, infrastructures et systèmes de télécommunication, de transport, de gouvernement ou systèmes financiers, entre autres — peuvent être perturbées, altérées ou endommagées. Après avoir consulté des experts du monde entier et réalisé ses propres recherches, le CICR est particulièrement préoccupé

[1] L'expression « cyberopérations pendant les conflits armés » est utilisée dans le présent document pour désigner des opérations visant un ordinateur, un système ou un réseau informatique ou un autre appareil connecté, au moyen d'un flux de données, lorsqu'elles sont employées comme moyen ou méthode de guerre dans le contexte d'un conflit armé. Les cyberopérations reposent sur les technologies de l'information et de la communication.

[2] Résolution 73/266 de l'Assemblée générale, doc. Nations Unies A/RES/73/266,2 janvier 2019, par. 3. Voir aussi résolution 73/27 de l'Assemblée générale, doc. Nations Unies A/RES/73/27, 11 décembre 2018, par. 5.

par le coût humain potentiel des cyberopérations lancées contre des infrastructures civiles essentielles, y compris dans le secteur de la santé[3].

Au cours des dernières années, plusieurs cyberattaques ont révélé la vulnérabilité de services essentiels. Ces attaques semblent se multiplier, et leur gravité s'accroît plus rapidement que les experts ne l'avaient prévu. Qui plus est, certains domaines restent très mal connus, comme les capacités et les outils cybernétiques les plus perfectionnés déjà mis au point ou en voie de développement, l'évolution potentielle des technologies et la mesure dans laquelle le recours aux cyberopérations pendant les conflits armés pourrait s'écarter des tendances observées jusqu'ici.

En outre, les caractéristiques du cyberespace suscitent des préoccupations spécifiques. Ainsi, les cyberopérations font courir un risque d'escalade et de dommages connexes à la population, pour la simple raison qu'il peut être difficile, pour la partie ciblée, d'établir si l'objectif de l'attaquant consiste à collecter des renseignements ou à causer des effets plus nuisibles. La partie ciblée risque, de ce fait, de réagir de manière plus virulente que nécessaire, parce qu'elle redoute le scénario le plus néfaste.

Les cyberoutils, enfin, prolifèrent de manière tout à fait particulière, puisqu'ils peuvent, une fois utilisés, être adaptés et employés à grande échelle par des acteurs différents de ceux qui les ont initialement mis au point ou utilisés.

III. L'application du DIH aux cyberopérations pendant les conflits armés

Pour le CICR, il est hors de doute que le DIH régit — et, de ce fait, limite — les cyberopérations pendant les conflits armés, de même qu'il réglemente l'emploi de tout autre type d'arme, de moyen et de méthode de guerre dans un conflit armé, qu'il soit nouveau ou ancien[4]. Cette affirmation reste vraie, que le cyberespace soit considéré comme un nouveau théâtre de guerre — comparable à l'espace aérien, à la terre, à la mer et à l'espace extra-atmosphérique — ou comme un type de théâtre de guerre différent des autres, puisque créé par l'homme, ou encore qu'il ne soit pas considéré comme un théâtre de guerre en soi.

En adoptant des traités de DIH, les États cherchent à réglementer les conflits actuels et futurs. Les États ont inclus dans les traités de DIH des règles qui anticipent la mise au point de nouveaux moyens et méthodes de guerre, en présumant que le DIH leur serait applicable. À titre d'exemple, si le DIH ne s'appliquait pas aux futurs moyens et méthodes de guerre, il ne serait pas nécessaire d'examiner leur licéité au regard du DIH existant, comme l'exige l'article 36 du Protocole additionnel I du 8 juin 1977.

Cette conclusion est fortement étayée par l'avis consultatif rendu par la Cour internationale de justice dans l'affaire *Licéité de la menace ou de l'emploi d'armes nucléaires ;* la Cour a rappelé à cette occasion que les principes et règles établis du DIH applicable dans les conflits armés s'appliquent « à toutes les formes de guerre et à toutes les armes », y inclus « celles […] de l'avenir »[5]. Selon le CICR, cette conclusion s'applique aux cyberopérations pendant les conflits armés.

---

[3] Voir CICR, *The Potential Human Cost of Cyber Operations*, 2019, disponible à l'adresse https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

[4] CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2011, 31IC/11/5.1.2, p. 41-42, disponible à l'adresse https://www.icrc.org/fr/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-fr.pdf ; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2015, 32IC/15/11, p. 48, disponible à l'adresse https://rcrcconference.org/app//uploads/2015/10/32IC-Report-on-IHL-and-the-challenges-of-contemporary-armed-conflicts_FR.pdf ; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2019, 33IC/19/9.7, p. 27, disponible à l'adresse https://rcrcconference.org/app/uploads/2019/10/33IC-Challenges-report_finalized_fr.pdf.

[5] Cour internationale de justice (CIJ), *Licéité de la menace ou de l'emploi d'armes nucléaires, avis consultatif du 8 juillet 1996, CIJ Recueil 1996,* p. 226, par. 86.

Le CICR se félicite du fait qu'un nombre croissant d'États et d'organisations internationales reconnaissent explicitement que le DIH s'applique aux cyberopérations pendant les conflits armés, et il attend avec intérêt les discussions sur les modalités d'application du DIH.

Les États peuvent aussi décider d'imposer aux cyberopérations des limites s'ajoutant à celles qui sont définies dans le droit existant, tout comme ils peuvent formuler des règles complémentaires, en particulier afin de renforcer la protection des civils et des infrastructures civiles contre les effets de ces opérations. Le CICR considère que toute nouvelle règle qui serait envisagée doit se fonder sur le cadre juridique existant, y compris le DIH, et le renforcer.

Dans les cas qui ne sont pas couverts par des règles de DIH existantes, les civils et les combattants demeurent protégés par la clause dite « de Martens », qui affirme qu'ils demeurent placés sous la sauvegarde et sous l'empire des principes du droit international, tels qu'ils résultent des usages établis, des principes de l'humanité et des exigences de la conscience publique[6].

Il importe d'insister sur le fait qu'affirmer l'applicabilité du DIH aux cyberopérations pendant les conflits armés ne légitime en rien la cyberguerre ni n'encourage la militarisation du cyberespace. De fait, le DIH fixe certaines limites à la militarisation du cyberespace en interdisant le développement de cybercapacités militaires qui enfreindraient le DIH[7]. En outre, tout emploi de la force par les États — par des moyens électroniques ou cinétiques — demeure régi par la Charte des Nations Unies ainsi que par les règles pertinentes du droit international coutumier, en particulier l'interdiction de l'emploi de la force. Les différends internationaux doivent être réglés par des moyens pacifiques, dans le cyberespace comme dans tous les autres cadres.

IV. La protection accordée par le DIH existant

Les traités de DIH en vigueur et le DIH coutumier réglementent le conflit armé au moyen d'un grand nombre de dispositions. Les règles régissant la conduite des hostilités sont particulièrement pertinentes dans le cyberespace. Elles ont pour objet de protéger la population civile contre les effets des hostilités. Elles reposent sur le principe fondamental de la distinction, qui impose aux belligérants de faire en tout temps la distinction entre la population civile et les combattants ainsi qu'entre les biens de caractère civil et les objectifs militaires, et de ne diriger leurs opérations que contre des objectifs militaires[8].

En dépit de l'interconnectivité propre au cyberespace, un examen approfondi du fonctionnement des cyberoutils montre qu'ils ne sont pas nécessairement de nature à agir sans discrimination. Bon nombre des cyberattaques signalées au cours de la période récente semblent, d'un point de vue technique, avoir ciblé assez précisément leur objet : conçues et effectuées pour ne toucher et n'endommager que des objets spécifiques, elles n'ont pas eu d'effets diffus ni causé de dommages sans discrimination. Toutefois, garantir que seuls les objets visés seront touchés peut présenter de grandes difficultés sur le plan technique et exiger une planification minutieuse dans la conception et l'exécution des cyberopérations. Il convient aussi de noter qu'une cyberopération qui, sur le plan technique, n'exerce pas d'effets sans discrimination n'est pas pour autant nécessairement licite, que ce soit pendant un conflit armé ou en dehors d'un tel contexte.

En revanche, certains cyberoutils connus ont été conçus pour s'auto-propager et affecter sans discrimination des systèmes informatiques utilisés à grande échelle. Ce comportement n'était pas le fruit du hasard ; la capacité de s'auto-propager doit en effet être spécifiquement prévue dans la conception de ces outils. L'interconnectivité qui est le propre du cyberespace signifie que tout

[6] Voir Protocole additionnel aux Conventions de Genève du 12 août 1949 relatif à la protection des victimes des conflits armés internationaux (Protocole I), 8 juin 1977 (ci-après : PA I), art. premier, par. 2 ; Convention (II) de La Haye de 1899, par. 9 du préambule ; Convention (IV) de La Haye de 1907, par. 8 du préambule.

[7] Voir J.-M. Henckaerts et L. Doswald-Beck (directeurs de publication), *Droit international humanitaire, Vol. I : Règles,* CICR et Bruylant, Bruxelles, 2006 (ci-après : Étude sur le DIH coutumier), règles 70 et 71 ; voir aussi PA I, art. 36.

[8] PA I, art. 48 ; Étude sur le DIH coutumier, règles 1 et 7 ; CIJ, *Licéité de la menace ou de l'emploi d'armes nucléaires,* par. 78.

dispositif qui se connecte à Internet peut être ciblé de n'importe quel lieu dans le monde. Qui plus est, une attaque contre un système spécifique peut avoir des conséquences pour divers autres systèmes et causer des effets sans discrimination. De ce fait, il existe un risque réel de voir des cyberoutils conçus ou utilisés en violation du DIH, de manière délibérée ou accidentelle.

Affirmer que le DIH — y compris les principes de distinction, de proportionnalité et de précaution — s'applique aux cyberopérations pendant les conflits armés signifie que, au regard du droit existant (et en complément de nombreuses autres règles) :

- Les cybercapacités qui constituent des armes et qui sont de nature à frapper sans discrimination sont interdites[9].
- Les attaques directes contre les personnes civiles et les biens de caractère civil sont interdites, y compris en cas d'utilisation de moyens ou méthodes de guerre cybernétiques.[10]
- Les actes ou menaces de violence dont le but principal est de répandre la terreur parmi la population civile sont interdits, y compris lorsqu'ils sont effectués par des moyens et méthodes de guerre cybernétiques[11].
- Les attaques sans discrimination, c'est-à-dire celles qui sont de nature à frapper indistinctement des objectifs militaires et des personnes civiles ou des biens de caractère civil, sont interdites, y compris en cas d'utilisation de moyens et méthodes de guerre cybernétiques[12].
- Les attaques disproportionnées sont interdites, y compris lorsqu'elles sont effectuées par des moyens et méthodes de guerre cybernétiques. On entend par attaques disproportionnées celles dont on peut attendre qu'elles causent incidemment des pertes en vies humaines dans la population civile, des blessures aux personnes civiles, des dommages aux biens de caractère civil, ou une combinaison de ces pertes et dommages qui seraient excessifs par rapport à l'avantage militaire concret et direct attendu[13].
- Les opérations militaires, y compris celles qui emploient des moyens et méthodes de guerre cybernétiques, doivent être conduites en veillant constamment à épargner la population civile et les biens de caractère civil ; toutes les précautions pratiquement possibles doivent être prises en vue d'éviter et, en tout cas, de réduire au minimum les pertes et dommages aux personnes civiles et aux biens de caractère civil qui pourraient être causés incidemment lors des attaques, y compris par des moyens et méthodes de guerre cybernétiques[14].
- Il est interdit d'attaquer, de détruire, d'enlever ou de mettre hors d'usage des biens indispensables à la survie de la population civile, y compris par des moyens et méthodes de guerre cybernétiques[15].
- Les structures sanitaires doivent être protégées et respectées, y compris lorsque des cyberopérations sont menées pendant des conflits armés[16].

---

[9] Étude sur le DIH coutumier, règle 71.

[10] PA I, art. 48, 51 et 52 ; Étude sur le DIH coutumier, règles 1 et 7.

[11] PA I, art. 51, par. 2 ; Étude sur le DIH coutumier, règle 2.

[12] PA I, art. 51, par. 4 ; Étude sur le DIH coutumier, règles 11 et 12. On entend par « attaque sans discrimination » les attaques a) qui ne sont pas dirigées contre un objectif militaire déterminé ; b) dans lesquelles on utilise des méthodes ou moyens de combat qui ne peuvent pas être dirigés contre un objectif militaire déterminé ; ou c) dans lesquelles on utilise des méthodes ou moyens de combat dont les effets ne peuvent pas être limités comme le prescrit le DIH ; et qui sont, en conséquence, dans chacun de ces cas, propres à frapper indistinctement des objectifs militaires et des personnes civiles ou des biens de caractère civil.

[13] PA I, art. 51, par. 5) b) et 57 ; Étude sur le DIH coutumier, règle 14.

[14] PA I, art. 57 ; Étude sur le DIH coutumier, règles 15 à 21.

[15] PA I, art. 54 ; Protocole additionnel aux Conventions de Genève relatif à la protection des victimes des conflits armés non internationaux (Protocole II), 8 juin 1977 (ci-après : PA II), art. 14 ; Étude sur le DIH coutumier, règle 54.

[16] Voir, par exemple, Convention de Genève pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne (CG I), art. 19 ; Convention de Genève pour l'amélioration du sort des blessés, des malades et des naufragés des forces armées sur mer du 12 août 1949 (CG II), art. 12 ; Convention de Genève relative à la protection des personnes

En outre, toutes les précautions pratiquement possibles doivent être prises pour protéger les personnes civiles et les biens de caractère civil contre les effets des attaques menées par des moyens et méthodes de guerre cybernétiques ; les États sont tenus de respecter cette obligation, y compris en temps de paix[17]. Diverses mesures peuvent être envisagées, notamment : isoler les cyberinfrastructures et réseaux militaires des cyberinfrastructures et réseaux civils ; isoler de l'Internet les systèmes informatiques dont dépendent des infrastructures civiles essentielles ; identifier les cyberinfrastructures et les réseaux qui desservent des biens bénéficiant d'une protection spécifique comme les hôpitaux[18].

V. La nécessité de débattre de la *manière* dont s'applique le DIH

Affirmer que le DIH s'applique aux cyberopérations pendant les conflits armés est un premier pas essentiel pour éviter ou réduire au minimum les souffrances humaines que ces opérations pourraient entraîner. Cependant, le CICR encourage aussi les États à se mettre d'accord sur la *manière* dont les principes et les règles du DIH s'appliquent aux cyberopérations. Cet accord est indispensable, car la nature interconnectée et essentiellement numérique du cyberespace pose des difficultés en termes d'interprétation des principes et concepts fondamentaux du DIH relatifs à la conduite des hostilités.

Le CICR a choisi de mettre plus particulièrement l'accent, dans le présent document, sur trois de ces problèmes.

L'utilisation du cyberespace à des fins militaires et les conséquences sur son caractère civil

Exception faite de certains réseaux militaires spécifiques, le cyberespace est utilisé avant tout à des fins civiles. Il peut arriver, toutefois, que les réseaux civils et militaires soient connectés entre eux, et les réseaux militaires peuvent dépendre de cyberinfrastructures civiles : câbles sous-marins à fibres optiques, satellites, routeurs ou nœuds. Inversement, les véhicules, la navigation et le contrôle aérien civils dépendent de plus en plus de systèmes de navigation par satellite qui peuvent aussi être utilisés par les forces armées. Les chaînes d'approvisionnement logistiques civiles ainsi que des services civils essentiels utilisent les mêmes réseaux de communication et réseaux Internet que certaines communications militaires.

L'utilisation d'un bien de caractère civil à des fins militaires ne fait pas automatiquement de ce bien un objectif militaire au regard du DIH[19]. En revanche, s'il devient un objectif militaire, il cesse d'être protégé par l'interdiction des attaques directes contre des biens de caractère civil. Il serait extrêmement préoccupant que l'utilisation militaire du cyberespace conduise à la conclusion que de nombreux biens qui en font partie ne seraient plus protégés en tant que biens de caractère civil. Il pourrait en découler une perturbation massive de l'utilisation civile du cyberespace, qui ne cesse de gagner en importance.

Ceci dit, même si certaines parties de l'infrastructure du cyberespace n'étaient plus protégées en tant que biens de caractère civil pendant les conflits armés, toute attaque éventuelle demeurerait régie par

civiles en temps de guerre du 12 août 1949 (CG IV), art. 18 ; PA I, art. 12 ; PA II, art. 11 ; Étude sur le DIH coutumier, règles 25, 28 et 29.

[17] PA I, art. 58 ; Étude sur le DIH coutumier, règles 22 à 24.

[18] CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2015, p. 52.

[19] Voir PA I, art. 52, par. 2 ; Étude sur le DIH coutumier, règle 8 : « En ce qui concerne les biens, les objectifs militaires sont limités aux biens qui, par leur nature, leur emplacement, leur destination ou leur utilisation apportent une contribution effective à l'action militaire et dont la destruction totale ou partielle, la capture ou la neutralisation offre en l'occurrence un avantage militaire précis. » Pour plus de détails sur les limites interdisant, au regard du DIH, de considérer les cyberinfrastructures comme des objectifs militaires, voir CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2015, p. 49-50.

l'interdiction des attaques sans discrimination et par les règles de la proportionnalité et des précautions dans l'attaque. Le fait que les réseaux civils et militaires sont si étroitement interconnectés est précisément la raison pour laquelle l'évaluation des dommages civils attendus de toute cyberopération est cruciale pour veiller à ce que la population civile soit protégée contre ses conséquences[20].

La notion d'« attaque » au regard du DIH et les cyberopérations

Les infrastructures civiles vitales qui permettent de fournir les services essentiels dépendent toujours plus de systèmes numérisés. Il est essentiel, pour protéger la population civile, de préserver ces infrastructures et ces services contre les cyberattaques ou les dommages incidents.

Le DIH assure une protection spécifique de certaines infrastructures, telles que les services de santé et les biens indispensables à la survie de la population, quel que soit le type d'opération hostile qui est conduite[21]. Toutefois, la majeure partie des règles découlant des principes de distinction, de proportionnalité et de précaution — qui offrent une protection générale aux personnes civiles et aux biens de caractère civil — ne s'appliquent qu'aux opérations militaires définies par le DIH comme des « attaques »[22]. L'article 49 du Protocole additionnel I définit les attaques comme « des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs »[23]. C'est pourquoi la question de l'interprétation de la notion d' « attaque », qui peut être plus ou moins stricte ou souple, est essentielle pour l'applicabilité de ces règles et la protection qu'elles accordent aux personnes et aux infrastructures civiles.

Il est communément admis que les cyberopérations conçues pour tuer, blesser ou causer des dommages matériels constituent des attaques au sens du DIH. Pour le CICR, il convient d'y inclure aussi les cyberopérations qui causent des dommages par leurs effets directs et indirects prévisibles, par exemple lorsque des patients placés en unités de soins intensifs décèdent du fait d'une cyberopération contre un réseau électrique qui prive l'hôpital d'électricité.

En outre, les attaques qui perturbent gravement des services essentiels, sans nécessairement causer de dommages matériels, représentent l'un des risques les plus importants pour les personnes civiles. Les avis divergent, toutefois, sur la question de savoir si une cyberopération qui provoque la perte de fonctionnalités sans causer de dégâts matériels doit être considérée comme une attaque au sens du DIH. Le CICR considère que dans un conflit armé, une opération conçue pour mettre hors d'usage un ordinateur ou un réseau informatique constitue une attaque au titre du DIH, que le bien soit mis hors d'usage par des moyens cinétiques ou cybernétiques[24]. Si la notion d'attaque est interprétée comme ne concernant que les opérations qui causent des morts, des blessures ou des dommages matériels, alors une cyberopération conçue pour mettre hors d'usage un réseau civil (comme un réseau électrique, bancaire ou de communications) — ou dont on peut s'attendre à ce qu'elle provoque incidemment de tels effets — pourrait ne pas être couverte par les règles essentielles du DIH qui protègent la population civile et les biens de caractère civil. Une définition aussi exagérément restrictive de la notion d'attaque serait difficilement conciliable avec l'objet et le but des règles du DIH

[20] Voir CICR, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law*, 2018, disponible à l'adresse https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf, p. 37-40.

[21] Voir le texte correspondant aux notes de bas de page 15 et 16 ci-dessus. Les « biens indispensables à la survie de la population civile » ne doivent pas être attaqués, détruits, enlevés ou mis hors d'usage.

[22] La notion d'« attaque » au sens du DIH, définie à l'art. 49 du PA I, est différente de la notion d' « agression armée » définie à l'art. 51 de la Charte des Nations Unies, qui relève du *jus ad bellum.* Le fait d'affirmer qu'une cyberopération spécifique ou un type de cyberopération constitue une attaque au sens du DIH ne signifie pas nécessairement qu'elle constituerait une agression armée au regard de la Charte des Nations Unies.

[23] Pour les règles qui s'appliquent spécifiquement aux attaques, voir le texte correspondant aux notes de bas de page 10 à 14 ci-dessus.

[24] Voir CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2011, p. 43 ; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2015, p. 50-51.

relatives à la conduite des hostilités. Il est donc essentiel, afin d'assurer une protection appropriée à la population civile contre les effets des cyberopérations, que les États parviennent à une acception commune de la notion d'attaque.

Les données civiles et la notion de « bien de caractère civil »

Les données civiles essentielles — telles que les données médicales, biométriques, relatives à la sécurité sociale, les dossiers fiscaux, les comptes bancaires, les fichiers clients des entreprises ou encore les listes et les relevés électoraux — représentent, dans des sociétés numérisées, un élément important. Ces données sont cruciales pour le fonctionnement de la plupart des aspects de la vie civile, à l'échelon individuel ou pour la société entière. La protection de ces données civiles essentielles est un sujet qui suscite une préoccupation croissante.

Certaines des mesures de protection spécifiques prévues par le DIH englobent des données essentielles ; ainsi, les données appartenant à des unités sanitaires sont couvertes par l'obligation de respecter et de protéger ces unités[25].

Plus généralement, les principes et les règles principaux du DIH régissant la conduite des hostilités protègent les personnes civiles et les biens de caractère civil[26]. Il serait donc important que les États conviennent que les données civiles sont protégées par ces règles.

La suppression ou l'altération de données civiles essentielles peut rapidement entraîner une immobilisation totale des services publics et des entreprises privées. Ce type d'opération peut nuire bien davantage à la population civile que la destruction de biens matériels. La question de savoir si les données civiles constituent des biens de caractère civil, et dans quelle mesure, demeure une question ouverte. Selon le CICR, affirmer que la suppression ou l'altération de ces données civiles essentielles ne serait pas interdite par le DIH, alors que nous vivons dans un monde toujours plus dépendant des données numériques, semble difficile à concilier avec l'objet et le but du DIH[27]. Exclure les données civiles essentielles de la protection accordée par le DIH aux biens de caractère civil créerait une grave lacune dans la protection.

VI. L'attribution des actes dans le cyberespace aux fins de la responsabilité des États

Le cyberespace offre diverses possibilités techniques permettant aux acteurs de dissimuler ou de falsifier leur identité, ce qui rend l'attribution plus complexe. Cette caractéristique est une source de grandes difficultés. À titre d'exemple, même pendant un conflit armé, le DIH ne s'applique qu'aux opérations qui sont liées au conflit. Si l'auteur d'une cyberopération ne peut être identifié, il est impossible d'établir un lien entre l'opération et le conflit armé en question ; il peut alors être difficile de déterminer si le DIH est applicable à l'opération. L'attribution des cyberopérations est importante par ailleurs pour veiller à ce que les acteurs qui violent le droit international, y compris le DIH, aient à répondre de leurs actes. La perception qu'il sera plus facile de rejeter la responsabilité de ces attaques peut également affaiblir le tabou lié à leur utilisation — et, de ce fait, les acteurs peuvent avoir moins de scrupules à enfreindre le droit international en les utilisant[28].

L'attribution, en revanche, ne représente pas un problème pour les acteurs qui exécutent, dirigent ou supervisent les cyberopérations, puisqu'ils ont en main tous les éléments permettant de déterminer le cadre juridique international dans lequel ils opèrent et les obligations qu'ils sont tenus de respecter.

---

[25] Voir la note 16.

[26] Voir le texte correspondant aux notes de bas de page 10 à 15 ci-dessus.

[27] CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2015, p. 52 ; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2019, p. 30.

[28] CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2011, p. 42 ; CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2019, p. 29.

Au regard du droit international, un État est responsable du comportement qui lui est attribuable, y compris d'éventuelles violations du DIH, ce qui inclut :

- le comportement d'organes de l'État, y compris ses forces armées ou ses services de renseignement ;
- le comportement de personnes ou d'entités — comme des entreprises privées — que l'État a habilitées à exercer des prérogatives de puissance publique ;
- le comportement de personnes ou de groupes — comme des milices ou des groupes de pirates informatiques — agissant en fait sur instructions de l'État, ou sous ses directives ou son contrôle ;
- le comportement de personnes privées ou de groupes que l'État reconnaît et adopte comme son propre comportement[29].

Ces principes s'appliquent, que le comportement soit réalisé par des voies électroniques ou par tout autre moyen.

VII. Conclusion

Le recours aux cyberopérations en tant que moyen ou méthode de guerre dans un conflit armé entraîne un risque réel de dommages pour la population civile. Afin de protéger la population et les infrastructures civiles, il est essentiel de reconnaître que ces opérations ne se déroulent pas dans un contexte de vide juridique. Le CICR appelle instamment tous les États à affirmer que le DIH s'applique aux cyberopérations pendant les conflits armés, étant entendu que cette affirmation n'encourage aucunement la militarisation du cyberespace, pas plus qu'elle ne légitime la cyberguerre.

Parallèlement, le CICR estime que l'interprétation et l'application du DIH dans le cyberespace exigent un débat plus approfondi, en particulier entre les États. Ce débat est urgent, car les États qui décident de mettre au point ou d'acquérir des cybercapacités qui constituent des armes, des moyens et des méthodes de guerre — à des fins offensives ou défensives — doivent veiller à ce que ces capacités puissent être employées dans le respect des obligations qui sont les leurs au regard du DIH[30]. Ces discussions devraient se fonder sur une compréhension approfondie de la mise au point de cybercapacités militaires, de leur coût humain potentiel et de la protection accordée par le droit existant. Les États doivent établir si le droit actuel est adapté et suffisant pour répondre aux problèmes posés par le caractère interconnecté et essentiellement numérique du cyberespace, ou s'il exige d'être adapté aux caractéristiques spécifiques du cyberespace. Au cas où de nouvelles règles devraient être conçues pour protéger les civils contre les effets des cyberopérations, ou pour d'autres raisons, elles devraient développer et renforcer le cadre juridique existant, y compris le DIH.

Le CICR se félicite des discussions en cours entre les gouvernements dans le cadre des deux processus mis sur pied par l'Assemblée générale des Nations Unies, et il est reconnaissant de la possibilité qui lui est donnée de faire connaître son point de vue aux États participants. Le CICR se tient prêt, par ailleurs, à mettre ses compétences à la disposition des États, au cas où ils le jugeraient utile, dans le cadre de ces échanges.

[29] Voir la règle 149 de l'Étude du CICR sur le DIH coutumier. Voir aussi Commission du droit international, *Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite,* 2001, en particulier les art. 4 à 11.

[30] Voir CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains,* 2019, p. 29-31 ; CICR, *Guide de l'examen de a licéité des nouvelles armes et des nouveaux moyens et méthodes de guerre : Mise en œuvre des dispositions de l'article 36 du Protocole additionnel I de 1977,* 2006, p. 5 ; PA I, art. 36.