Humanity In War

GROUPE DE TRAVAIL 6

VEILLER À CE QUE LES TECHNOLOGIES NUMÉRIQUES SOIENT UTILISÉES D'UNE MANIÈRE CONFORME AU DIH DANS LES CONFLITS ARMÉS

DOCUMENT DE RÉFÉRENCE*

INTRODUCTION 2

I. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS ET LE DIH : DISCUSSIONS MONDIALES ET VISIONS COMMUNES ÉMERGENTES 2

II. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS CONTEMPORAINS ET LEUR COÛT HUMAIN 3

III. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS : QUESTIONS JURIDIQUES ET HUMANITAIRES DÉCOULANT DU DIH 5

I. PROTÉGER LES CIVILS, AINSI QUE LES AUTRES PERSONNES ET BIENS PROTÉGÉS, CONTRE LES DANGERS RÉSULTANT DES ACTIVITÉS NUMÉRIQUES MENÉES DANS LES CONFLITS ARMÉS 6

II. PROTÉGER LES CIVILS, AINSI QUE LES AUTRES PERSONNES PROTÉGÉES, CONTRE LA PROPAGATION D'INFORMATIONS EN VIOLATION DU DIH DANS LES CONFLITS ARMÉS 9

III. LE RISQUE DE DOMMAGES RÉSULTANT DE L'UTILISATION À DES FINS MILITAIRES D'INFRASTRUCTURES NUMÉRIQUES CIVILES ET LA PARTICIPATION DE CIVILS AUX ACTIVITÉS NUMÉRIQUES DANS LES CONFLITS ARMÉS 10

* Le présent document de référence a été rédigé à l'origine pour la première consultation avec les États. Seules quelques petites corrections et mises à jour y ont été apportées en septembre 2025.

INTRODUCTION

L'utilisation croissante des technologies numériques dans les conflits armés pose d'importantes questions humanitaires et juridiques. S'il est largement admis que le droit international humanitaire (DIH) impose des limites à l'utilisation des technologies numériques dans les conflits armés, les spécificités de l'environnement numérique soulèvent des questions complexes quant à sa mise en œuvre. Les États ont reconnu la nécessité de poursuivre les discussions sur ces thématiques. Le groupe de travail sur le numérique s'inscrit dans le cadre des efforts actuellement déployés pour favoriser une vision commune.

I. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS ET LE DIH : DISCUSSIONS MONDIALES ET VISIONS COMMUNES ÉMERGENTES

L'application du droit international, notamment du DIH, aux activités numériques fait l'objet de discussions multilatérales depuis près de vingt ans. En 2021, le Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale a noté que « le droit international humanitaire s'appliquait uniquement en cas de conflit armé. Il rappelle les principes juridiques internationaux établis, notamment, lorsqu'ils sont applicables, les principes d'humanité, de nécessité, de proportionnalité et de distinction notés dans le rapport de 2015. Il a reconnu qu'il convenait d'examiner plus avant de quelle manière et à quel moment ces principes s'appliquaient à l'utilisation des technologies numériques par les États et a souligné que le rappel de ces principes ne légitimait ni n'encourageait en aucun cas les conflits »[1]. Le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation (2021-2025) a repris cette conclusion dans ses rapports[2].

À ce jour, et à notre connaissance, 35 États ont publié des positions nationales individuelles sur la manière dont le droit international s'applique aux cyberopérations[3]. En outre, deux organisations régionales – l'Union africaine et l'Union européenne – ont publié des positions ou des interprétations communes sur l'application du droit international à l'utilisation des technologies numériques, ce qui marque un progrès dans la recherche d'un consensus régional et porte à plus de 100 le nombre d'États qui se prononcent sur ce sujet. Des positions communes se dégagent ainsi pour réaffirmer l'application des principes et des règles du DIH, notamment les principes d'humanité, de nécessité, de proportionnalité et de distinction, à l'utilisation des technologies numériques dans les conflits armés. Un nombre croissant d'États se sont également exprimés sur la protection offerte par le DIH, entre autres, aux

---

[1] *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*, A/76/135, 2021, par. 71.f). Voir également les par. 2 et 3 de la Résolution 76/19 de l'Assemblée générale des Nations Unies de 2021, adoptée par consensus, qui accueille avec satisfaction le rapport final établi par consensus par le Groupe d'experts gouvernementaux et demande aux États membres de s'inspirer de ce rapport en ce qui concerne l'utilisation du numérique.

[2] Voir le Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, *Premier rapport d'activité annuel*, A/77/275, 2022, par. 15b.ii) ; *Deuxième rapport d'activité annuel*, A/78/265, 2023, par. 29b.ii) ; *Troisième rapport d'activité annuel*, A/79/214, 2024, par. 36b)ii) ; *Projet de rapport final,* A/AC.292/2025/CRP.1, 2025, par. 40b)ii).

[3] On trouvera toutes les positions individuelles des États ainsi que les positions communes sur le Cyber Law Toolkit, « Common and National Positions », à l'adresse https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions.

personnes civiles, aux infrastructures civiles, aux données civiles, au personnel et aux installations médicales, ainsi qu'aux activités et au personnel humanitaires contre les activités numériques malveillantes.

Sur cette lancée, la XXXIVe Conférence internationale de la Croix-Rouge et du Croissant-Rouge – qui a réuni tous les États et toutes les composantes du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) – a adopté, en octobre 2024, la résolution intitulée « Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés » (résolution sur le numérique). La résolution demande instamment aux États et aux parties aux conflits armés de protéger la population civile ainsi que les autres personnes et biens protégés dans les situations de conflit armé, y compris contre les risques résultant des activités numériques malveillantes. Elle appelle également les États et les parties aux conflits armés à faire respecter les protections prévues par le DIH pour les civils, les infrastructures civiles critiques (y compris les infrastructures numériques essentielles, telles que les câbles sous-marins et les réseaux de communication satellitaire), le personnel médical et les activités humanitaires, ainsi que les biens culturels, notamment contre les risques résultant des activités numériques. Elle réitère l'interdiction d'encourager ou d'inciter à commettre des violations du DIH et aborde les questions relatives aux civils qui mènent des activités numériques et aux entreprises technologiques privées qui fournissent des services numériques dans le contexte d'un conflit armé.

Malgré les progrès susmentionnés, il a été reconnu que les spécificités de l'environnement numérique soulèvent des questions sur la manière dont les principes et les règles du DIH s'appliquent aux activités numériques et qu'il convient de poursuivre les discussions[4].

Ce groupe de travail répond à ce besoin et offre un espace dédié permettant des échanges ciblés et approfondis. Compte tenu du coût humain de l'utilisation des technologies numériques dans les conflits armés, l'objectif de ce groupe de travail est de favoriser une compréhension commune des limites que le DIH impose aux activités numériques dans les conflits armés afin de protéger les civils.

II. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS CONTEMPORAINS ET LEUR COÛT HUMAIN

La numérisation rapide des sociétés a apporté des avantages significatifs, améliorant les opportunités dans le domaine social, économique et de la communication. Dans les zones touchées par un conflit, il est indispensable de disposer de technologies numériques fiables pour permettre aux civils d'accéder aux biens et aux services essentiels et pour que les gouvernements soient à même de fournir des services et de soutenir les activités médicales et humanitaires, y compris celles du Mouvement.

[4] *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*, A/76/135, 2021, par. 71f), et XXXIVe Conférence internationale de la Croix-Rouge et du Croissant-Rouge, Genève, 2024, résolution 2 intitulée « Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés » (ci-après dénommée « résolution sur le numérique »), par. 19 du préambule.

Ces avantages vont toutefois de pair avec des risques, tels ceux résultant de l'utilisation accrue des technologies numériques par les États et les acteurs non étatiques dans les conflits armés. Un certain nombre d'États développent des capacités numériques à des fins militaires, déployant et utilisant de plus en plus les technologies numériques comme moyens ou méthodes de guerre. Si le développement et l'utilisation de capacités numériques à des fins militaires peuvent offrir aux belligérants la possibilité d'atteindre leurs objectifs sans nécessairement causer de dommages directs aux civils ou de dommages physiques aux infrastructures civiles, ces activités font néanmoins peser des menaces bien réelles sur les populations et les infrastructures civiles. En utilisant les capacités numériques à des fins militaires, des processus contrôlés par des systèmes informatiques peuvent être déclenchés, altérés ou manipulés d'une autre manière, au risque de porter gravement atteinte à des civils.

L'utilisation des technologies numériques contre les infrastructures civiles essentielles – installations nucléaires, réseaux électriques, systèmes d'approvisionnement en eau et réseaux de télécommunications – peut avoir des « conséquences humanitaires potentiellement dévastatrices »[5]. Les activités numériques peuvent également perturber les services de gouvernance électronique et les activités du secteur privé, engendrant des coûts pour la société et l'économie. Ces risques sont décuplés par l'interconnectivité qui caractérise le cyberespace. Les activités numériques visant un système peuvent ainsi avoir des répercussions sur d'autres systèmes, quel que soit l'endroit où ils se trouvent.

Le secteur de la santé, ainsi que les organisations humanitaires, sont particulièrement vulnérables aux activités numériques menées dans les conflits armés, qui peuvent perturber des opérations médicales vitales, entraver le travail des organisations humanitaires impartiales et de leur personnel, et compromettre la fourniture d'une aide essentielle aux personnes vulnérables. Par exemple, le Comité international de la Croix-Rouge (CICR) et d'autres composantes du Mouvement ont été la cible d'activités numériques[6].

Par ailleurs, la participation de civils dans des activités militaires à travers l'utilisation de technologies numériques dans les conflits armés s'est amplifiée. Les États ont toléré, facilité ou encouragé le fait que des hackers civils et des groupes de hackers se livrent à des activités numériques, ciblant ou touchant des civils et des biens de caractère civil associés à l'adversaire. Les civils ont également été encouragés à signaler les mouvements des troupes ennemies, notamment grâce à des applications sur smartphone. Les entreprises privées sont de plus en plus nombreuses à fournir des services de cybersécurité ou d'autres services numériques aux parties à un conflit armé. Si des civils sont trop proches des hostilités, ils risquent de subir des dommages. En outre, ils ne sont souvent pas au fait des risques encourus, des conséquences juridiques de leurs activités ou des règles du DIH qu'ils doivent respecter.

Un autre aspect est l'utilisation des technologies numériques pour diffuser des informations préjudiciables dans les conflits armés. Si les opérations d'information font depuis longtemps partie de la guerre et ne sont pas illicites en tant que telles, l'utilisation des technologies numériques – en particulier sur les plateformes de médias sociaux ou lorsqu'elles sont associées à l'intelligence artificielle et à d'autres technologies émergentes – accroît la vitesse et l'ampleur de la propagation d'informations préjudiciables, y compris les tentatives

[5] Groupe de travail à composition non limitée sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale, *Rapport final de fond*, A/AC.290/2021/CRP.2, 2021, par. 18.

[6] La violation des données perpétrée en 2022 et les attaques répétées du type « déni de service » sur le site web du CICR soulignent la nécessité d'une protection solide des données pour préserver les informations sensibles, assurer la continuité opérationnelle et protéger le dialogue humanitaire confidentiel avec les parties aux conflits. Voir CICR, « Cyberattaque contre le CICR : le point sur ce que nous savons », à l'adresse https://www.icrc.org/fr/document/cyberattaque-cicr-ce-que-nous-savons.

d'inciter à la violence, d'exposer les détenus à la curiosité publique ou de saper la confiance dans les organisations humanitaires.

Les États ont pris acte de ces évolutions et de ces risques. Le groupe de travail 2021-2025 sur les développements dans le domaine de l'information et des télécommunications dans le contexte de la sécurité internationale a noté que les États mettent au point des capacités numériques à des fins militaires, qu'il est de plus en plus probable que les technologies numériques soient utilisées dans des conflits futurs, et que ces technologies ont déjà été utilisées dans des conflits dans différentes régions, avec des conséquences humanitaires qui pourraient s'avérer dévastatrices pour les civils et les biens de caractère civil, ainsi que pour les organisations internationales et humanitaires[7]. La XXXIVe Conférence internationale a également souligné les dommages que l'utilisation de technologies numériques par les parties aux conflits armés peut causer aux civils, en particulier lorsqu'elle vise ou affecte incidemment les infrastructures civiles critiques et les services essentiels, ainsi que le préjudice qui peut être causé aux organisations humanitaires impartiales, menaçant leur accès aux populations touchées[8].

III. L'UTILISATION DES TECHNOLOGIES NUMÉRIQUES DANS LES CONFLITS ARMÉS : QUESTIONS JURIDIQUES ET HUMANITAIRES DÉCOULANT DU DIH

Les traités de DIH existants et le droit coutumier protègent les civils et les biens de caractère civil contre les dangers résultant des activités numériques menées dans les conflits armés. Comme le réitère la résolution sur le numérique, « dans les situations de conflit armé, les règles et principes du DIH – notamment le principe de distinction, l'interdiction de lancer des attaques indiscriminées ou disproportionnées, l'obligation, lors de la conduite des opérations militaires, d'épargner la population civile, les personnes civiles et les biens de caractère civil et de prendre toutes les précautions pratiquement possibles en vue d'éviter et, en tout cas, de réduire au minimum les dommages causés incidemment aux civils, l'interdiction d'encourager ou d'inciter à commettre des violations du DIH, et l'interdiction de se livrer à des actes ou menaces de violence dont le but principal est de répandre la terreur parmi la population civile – contribuent à protéger les civils ainsi que les autres personnes et biens protégés, notamment contre les risques résultant des activités numériques »[9].

Sur la base des éléments ci-dessus, les questions juridiques essentielles qui reflètent les préoccupations humanitaires les plus pressantes sont proposées ci-après pour un examen plus approfondi.

[7] Groupe de travail à composition non limitée sur la sécurité du numérique et de son utilisation, *projet de rapport final,* A/AC.292/2025/CRP.1, 2025, par. 15, 16 et 21.
[8] Résolution sur le numérique, par. 7 et 14 du préambule.
[9] Résolution sur le numérique, par. 4.

I. PROTÉGER LES CIVILS, AINSI QUE LES AUTRES PERSONNES ET BIENS PROTÉGÉS, CONTRE LES DANGERS RÉSULTANT DES ACTIVITÉS NUMÉRIQUES MENÉES DANS LES CONFLITS ARMÉS

La protection des populations civiles contre les effets des opérations numériques menées dans les conflits armés et la notion d'attaque en DIH

Les opérations numériques peuvent mettre hors service ou endommager physiquement des installations industrielles, des réseaux de communication et d'autres éléments de l'infrastructure essentielle d'un État. Ces opérations peuvent également causer, directement ou indirectement, des dommages, des blessures ou la mort de civils, notamment en empêchant le bon fonctionnement de services essentiels. Ces risques sont décuplés par l'interconnectivité de l'espace numérique. Si les opérations numériques causant des dommages matériels ont fait l'objet d'une attention particulière, les utilisations récentes des technologies numériques, y compris dans les conflits armés, ont montré que même si elles ne causent pas de dommages physiques, les opérations numériques peuvent gravement perturber les infrastructures civiles et interrompre la fourniture de services essentiels. En l'occurrence, cela constitue l'un des principaux risques numériques pour les civils dans les conflits armés.

Les règles du DIH régissant la conduite des hostilités ont pour objet d'assurer le respect et la protection de la population civile et des biens de caractère civil[10]. La plupart des règles découlant des principes et règles régissant la conduite des hostilités, notamment les 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 ou activités définies par le DIH comme des « attaques », c'est-à-dire « des actes de violence contre l'adversaire, que ces actes soient offensifs ou défensifs »[11]. C'est pourquoi la question de l'interprétation de la notion d'« attaque » en ce qui concerne l'utilisation des technologies numériques dans les conflits armés, en particulier les opérations numériques qui mettent hors service des biens de caractère civil sans causer de dommages physiques, est essentielle, car elle détermine l'applicabilité de ces règles et le degré de protection des civils et des autres personnes et biens protégés contre les dangers résultant de ces opérations.

Il est bien établi que la notion de violence dans la définition de l'« attaque » au sens du DIH peut renvoyer soit aux moyens utilisés, soit aux conséquences ou aux effets produits. Une opération qui a des effets violents peut être qualifiée d'attaque, même si les moyens utilisés ne sont pas violents en eux-mêmes[12].

Il est également largement admis qu'une opération numérique dont on peut attendre qu'elle cause la mort ou des blessures à une personne, ou qu'elle endommage ou détruise un bien, constitue une attaque au sens du DIH[13]. Il est communément admis que cela inclut les opérations qui causent des dommages par leurs effets directs et indirects prévisibles, par

---

[10] Protocole additionnel I du 8 juin 1977, art. 48 et titres de la Partie IV et section I.

[11] Protocole additionnel I, art. 49.1. Quelques règles du DIH s'appliquent à toutes les opérations militaires, y compris celles menées dans le cadre d'activités numériques. Voir, par exemple, Protocole additionnel I, art. 48, 51.1 et 57.1.

[12] Y. Sandoz, C. Swinarski et B. Zimmermann (dir.), Commentaire des Protocoles additionnels du 8 juin 1977 aux Conventions de Genève du 12 août 1949, CICR, Genève/Martinus Nijhoff, Leiden, 1987 (ci-après CICR, Commentaire des Protocoles additionnels), le par. 1881 à propos de l'art. 49.1 du Protocole additionnel I stipule qu'« il y a attaque chaque fois qu'une personne est directement mise en danger par une mine posée », ce qui est une interprétation cohérente avec l'approche fondée sur les conséquences. Un autre exemple généralement accepté est que l'utilisation d'un agent chimique ou biologique constituerait une attaque en raison des effets violents qu'il provoque, même si les moyens de diffusion de ces agents ne sont pas forcément violents.

[13] CICR, *Le droit international humanitaire et les défis posés par les conflits armés contemporains*, 2015, p. 49-50.

exemple lorsque des patients placés en unités de soins intensifs décèdent du fait d'une opération numérique contre un réseau électrique qui prive l'hôpital d'électricité[14].

Il importe en outre que les États examinent plus avant quelles règles du DIH limitent les opérations numériques qui compromettent le fonctionnement des systèmes numériques sans nécessairement causer des dommages matériels ou la destruction d'un bien ou encore des blessures ou la mort d'une personne, et se posent notamment la question de savoir si ces opérations peuvent être qualifiées d'« attaques » au sens du DIH.

Sous l'angle de la guerre contemporaine, il est essentiel, pour la protection des civils et des biens de caractère civil contre les activités numériques menées dans les conflits armés, de reconnaître comme une attaque au sens du DIH une opération numérique qui met un bien hors service sans causer de dommages physiques. Une interprétation restrictive de la notion d'attaque, qui exclurait certaines activités numériques de la protection offerte par les règles fondamentales du DIH relatives à la conduite des hostilités, serait difficilement conciliable avec l'objet et la finalité du DIH et avec la nécessité de garantir l'efficacité durable de son cadre de protection au gré de l'évolution des moyens et méthodes de guerre. À cet égard, il faut absolument que les États parviennent à dégager une acception commune pour protéger les civils et les biens de caractère civil contre les effets de l'utilisation malveillante des technologies numériques dans les conflits armés.

Les données civiles et la notion de biens de caractère civil au sens du DIH

Les données civiles – telles que les données médicales, biométriques, humanitaires, 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 suscite des préoccupations croissantes. La suppression ou l'altération des données civiles peut rapidement entraîner la paralysie des services publics et des entreprises privées et nuire bien davantage aux civils que la destruction de certains biens de caractère civil. En outre, le vol ou la fuite de données civiles peut exposer les individus et les communautés à de graves risques de préjudice.

S'agissant des données appartenant à certaines catégories de personnes et de biens bénéficiant d'une protection particulière au titre du DIH, les règles de protection sont suffisamment générales. Par exemple, l'obligation de respecter et de protéger le personnel, les unités et les moyens de transport sanitaires, le personnel et les biens humanitaires, ainsi que les biens indispensables à la survie de la population civile, s'étend à leurs données[15]. Il est cependant tout aussi important de mieux comprendre dans quelle mesure les données civiles sont protégées par les règles existantes du DIH[16], en particulier si les données constituent des biens au sens du DIH, auquel cas les opérations numériques menées contre des données (visant à les endommager ou à les supprimer) seraient alors régies par les principes de distinction, de proportionnalité et de précaution.

---

[14] CICR, *Document de position sur le droit international humanitaire et les cyberopérations pendant les conflits armés*, 2019, p. 9. Pour obtenir un aperçu des positions adoptées par les États, voir le Cyber Law Toolkit, « Attack (International Humanitarian Law) », à l'adresse https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law).

[15] Voir la section suivante du présent document intitulée « Protection spéciale prévue par le DIH pour les personnes, les biens et les activités ».

[16] Celles-ci comprennent les principes et les règles du DIH relatives à la conduite des hostilités. D'autres règles pertinentes peuvent inclure la protection des biens culturels, la protection des biens contre la saisie et la destruction et l'interdiction du pillage.

À cet égard, certains États ont estimé que la protection des biens civils s'étendait à tous les types de données civiles ; d'autres semblent établir une différence entre les « données de contenu » et les autres données, d'autres encore estimant que les données numériques ne peuvent généralement pas être considérées comme des biens au sens du DIH[17].

Des discussions plus approfondies entre les États sont nécessaires pour parvenir à une compréhension commune de cette question cruciale. D'un point de vue humanitaire, affirmer qu'une opération conçue pour supprimer ou altérer des données civiles (ou dont on peut s'attendre à ce qu'elle produise de tels effets) ne serait pas interdite par le DIH, alors que nous vivons dans un monde toujours plus dépendant des données, semble difficilement conciliable avec l'objet et le but du DIH. En toute logique, le remplacement des fichiers et documents sur papier par des fichiers numériques sous la forme de données ne doit pas diminuer le niveau de protection qui est conféré par le DIH aux informations stockées dans les données.

Protection spéciale prévue par le DIH pour les personnes, les biens et les activités

Certaines règles du DIH accordent une protection spéciale à certaines catégories de personnes, de biens et d'activités, au-delà de l'interdiction des attaques, notamment en ce qui concerne les activités numériques.

Par exemple, les belligérants doivent respecter et protéger le personnel et les installations médicales en tout temps[18], y compris l'obligation de ne pas indûment entraver le fonctionnement des services médicaux et de prendre toutes les mesures possibles pour les protéger contre les dommages ou les ingérences de personnes privées non imputables aux parties au conflit armé[19]. De même, le personnel humanitaire et les biens utilisés pour les opérations humanitaires doivent être respectés et protégés[20] et les parties à un conflit armé doivent autoriser et faciliter les activités humanitaires impartiales menées dans les conflits armés, sous réserve de leur droit de contrôle[21]. Qu'il s'agisse des services médicaux ou du personnel et des biens humanitaires, la protection spéciale s'étend aux communications et aux données[22].

Pour renforcer la protection des services médicaux et des activités humanitaires contre les risques numériques, les discussions approfondies pourraient porter sur la mise en pratique de cette protection. L'une des pistes à suivre est l'action menée par le CICR pour élaborer un emblème numérique, c'est-à-dire un moyen d'identifier l'infrastructure et les données numériques des organisations et entités habilitées à arborer les emblèmes distinctifs reconnus par le DIH[23]. Prenant note des travaux en cours du CICR en concertation avec les États et les composantes du Mouvement, la résolution sur le numérique encourage la

---

[17] Pour un aperçu des positions adoptées par les États, voir le Cyber Law Toolkit, « Data as a military objective » : https://cyberlaw.ccdcoe.org/wiki/Military_objectives#Qualification_of_data_as_a_military_objective_under_IHL.

[18] Voir, par exemple, la Première Convention de Genève du 12 août 1949, art. 19 ; la Deuxième Convention de Genève du 12 août 1949, art. 12 ; la Quatrième Convention de Genève du 12 août 1949, art. 18 ; le Protocole additionnel I, art. 12 ; le Protocole additionnel II du 8 juin 1977, art. 11 ; l'étude du CICR sur le DIH coutumier, à l'adresse https://ihl-databases.icrc.org/fr/customary-ihl/rules, règles 25, 28 et 29.

[19] CICR, Commentaire des Protocoles additionnels, par. 517 sur l'art. 12 du Protocole additionnel I, et CICR, *Commentaire de la Première Convention de Genève : Convention (I) pour l'amélioration du sort des blessés et des malades dans les forces armées en campagne*, 2e éd., CICR, Genève / Cambridge University, Cambridge, 2016 (ci-après Commentaire du CICR de la Première Convention de Genève, 2016), par. 1799 sur l'art. 19.

[20] Protocole additionnel I, art. 70.4 et 71.2 ; étude du CICR sur le DIH coutumier, règles 31 et 32.

[21] Voir la Quatrième Convention de Genève, art. 23 ; le Protocole additionnel I, art. 70.2 ; le Protocole additionnel II, art. 18.2 ; l'étude du CICR sur le DIH coutumier, règle 55.

[22] CICR, Commentaire de la Première Convention de Genève, 2016, par. 1804 sur l'art. 19.

[23] Le projet d'emblème numérique est un projet indépendant que le CICR mène en consultation et en interaction avec les États et les composantes du Mouvement. La discussion au sein de ce groupe de travail ne sera pas centrée sur ce projet.

poursuite des travaux et des consultations, notamment l'étude des voies juridiques et diplomatiques pouvant conduire à l'emploi d'un emblème numérique[24].

En outre, les activités numériques qui « détruisent, enlèvent ou mettent hors d'usage » des biens indispensables à la survie de la population civile, tels que les installations d'eau potable et les ouvrages d'irrigation, entrent dans le champ d'application de la protection spéciale conférée à ces biens par le DIH, qu'elles puissent ou non être qualifiées d'attaques[25]. Cette protection spéciale s'étend aux infrastructures numériques qui sont elles-mêmes « indispensables » au fonctionnement de ces biens. Il convient d'examiner plus avant les mesures visant à mettre ces protections en pratique.

Enfin, les règles du DIH interdisent la violence sexuelle et accordent des protections particulières à certaines catégories de personnes, notamment, mais pas exclusivement, les femmes, les personnes âgées, les personnes handicapées et les enfants (par exemple, contre leur enrôlement ou leur utilisation illicite dans les hostilités)[26]. Il convient d'approfondir le débat, entre autres, sur les mesures pratiques visant à garantir le respect de ces règles, y compris lorsque les violences sont facilitées par les technologies numériques.

II. PROTÉGER LES CIVILS, AINSI QUE LES AUTRES PERSONNES PROTÉGÉES, CONTRE LA PROPAGATION D'INFORMATIONS EN VIOLATION DU DIH DANS LES CONFLITS ARMÉS

Les États et les groupes armés non étatiques diffusent des informations numériques à des fins diverses, notamment dans le cadre d'opérations d'information ou d'opérations psychologiques. Certaines opérations visent à réduire le risque de porter atteinte aux personnes dans les conflits armés, par exemple en avertissant les civils par des moyens efficaces avant une attaque ou en les orientant vers des lieux sûrs. D'autres visent à semer la confusion ou à causer des dommages, à tromper un adversaire ou à soutenir les objectifs militaires ou politiques d'une partie au conflit. Dans les conflits armés contemporains, les technologies numériques sont utilisées pour diffuser des informations en violation du DIH. Les informations diffusées par le biais des technologies numériques peuvent contribuer à la violence ou l'encourager, causer des dommages psychologiques durables, compromettre l'accès aux services essentiels et perturber les opérations des organisations humanitaires, au risque de saper la confiance dans ces organisations.

[24] Résolution sur le numérique, par. 15 du préambule et par. 12 du dispositif.
[25] Ces biens comprennent notamment « les denrées alimentaires et les zones agricoles qui les produisent, les récoltes, le bétail, les installations et réserves d'eau potable et les ouvrages d'irrigation ». Protocole additionnel I, art. 54.2 ; Protocole additionnel II, art. 14 ; Étude du CICR sur le DIH coutumier, règle 54. Voir aussi CICR, Le droit international humanitaire et les défis posés par les conflits armés contemporains, 2024, p. 49-50.
[26] Quatrième Convention de Genève, art. 27.2 ; Protocole additionnel I, art. 76.1 et 77.1 et art. 2 ; Protocole additionnel II, art. 4.3.c ; étude du CICR sur le DIH coutumier, règles 134 à 138.

Le DIH contient plusieurs règles spécifiques qui imposent des limites à la diffusion d'informations, y compris par des moyens numériques, en particulier les suivantes :

- Les responsables civils et militaires d'une partie à un conflit armé ne doivent pas encourager les violations du DIH, y compris sur les plateformes numériques[27]. La résolution sur le numérique réaffirme en outre l'interdiction d'encourager ou d'inciter à commettre des violations du DIH par des moyens numériques[28].
- Les prisonniers de guerre et les autres personnes protégées par le DIH doivent être protégés contre la curiosité publique[29]. La diffusion publique par les autorités de données, d'images et de vidéos de prisonniers de guerre et d'autres personnes privées de liberté, à quelques rares exceptions près, violerait cette règle, et les États doivent également assurer une protection contre la diffusion par des entités privées[30].
- Les menaces de violence dont le but principal est de répandre la terreur parmi la population civile sont interdites par le DIH[31].
- Les fausses informations diffusées par les parties à un conflit armé pour perturber les interventions médicales ou humanitaires sont incompatibles avec l'obligation de respecter et de protéger le personnel médical et humanitaire et ses activités[32].
- La propagation d'informations visant à recruter des enfants, ou la propagande destinée à enrôler des personnes protégées dans les territoires occupés, dans les forces armées, est illégale[33].

Compte tenu des risques susmentionnés de préjudice porté aux civils et aux autres personnes protégées en vertu du DIH, il convient de poursuivre le débat afin de parvenir à une compréhension commune de la manière dont le DIH s'applique à la diffusion d'informations, en garantissant la protection effective de toutes les personnes et de tous les biens protégés par le DIH.

III. LE RISQUE DE DOMMAGES RÉSULTANT DE L'UTILISATION À DES FINS MILITAIRES D'INFRASTRUCTURES NUMÉRIQUES CIVILES ET LA PARTICIPATION DE CIVILS AUX ACTIVITÉS NUMÉRIQUES DANS LES CONFLITS ARMÉS

L'utilisation d'infrastructures numériques civiles à des fins militaires et ses effets sur la protection conférée par le DIH

À l'exception de certains réseaux militaires, le cyberespace est majoritairement civil. Toutefois, l'interconnexion des réseaux civils et militaires et l'utilisation de l'infrastructure numérique civile par les militaires posent des problèmes spécifiques pour sa protection.

Si des infrastructures numériques civiles – notamment celles fournies par des entreprises technologiques – sont utilisées à des fins militaires (on parlera alors d'infrastructures « à double usage »), elles risquent de devenir des objectifs militaires au sens du DIH et, donc,

[27] Quatrième Convention de Genève, art. 1 commun ; étude du CICR sur le DIH coutumier, règle 139.
[28] Résolution sur le numérique, par. 4.
[29] Voir, par exemple, la Troisième Convention de Genève du 12 août 1949, art. 13 et la Quatrième Convention de Genève, art. 27.
[30] Pour un débat plus approfondi sur ce thème, voir, par exemple, CICR, Commentaire de la Troisième Convention de Genève *: Troisième Convention relative au traitement des prisonniers de guerre, 2e éd.*, CICR, Genève, 2020 (ci-après CICR, Commentaire de la troisième Convention de Genève, 2020), par. 1623-1632.
[31] Protocole additionnel I, art. 51.2 ; Protocole additionnel II, art. 13.2 ; Étude du CICR sur le DIH coutumier, règle 2.
[32] À ne pas confondre avec les critiques ou l'expression de la colère des autorités ou des bénéficiaires à l'égard des services médicaux ou des organisations humanitaires, qui n'ont rien d'illégal à première vue.
[33] En ce qui concerne le recrutement d'enfants, voir l'étude du CICR sur le DIH coutumier, règle 136 et les obligations au titre du Protocole facultatif à la Convention relative aux droits de l'enfant, concernant l'implication d'enfants dans les conflits armés, du 25 mai 2000. S'agissant des personnes protégées dans les situations d'occupation, voir la Quatrième Convention de Genève, art. 51.

de perdre leur protection contre les attaques[34]. Le cas échéant, des dommages incidents risquent d'être causés aux civils et biens de caractère civil situés à proximité physique ou connectés numériquement à de telles cibles, ou qui en dépendent.

Toutefois, toutes les utilisations militaires ne transforment pas un bien civil en objectif militaire au sens du DIH ; c'est le cas seulement lorsque l'utilisation répond aux critères d'un objectif militaire tels que définis par le DIH. De plus, même si un belligérant considère qu'une personne civile ou un bien de caractère civil a perdu sa protection en raison de sa participation à des opérations numériques, toute attaque reste soumise à l'interdiction des attaques aveugles et disproportionnées et à l'obligation de prendre toutes les précautions possibles. En outre, certains biens spécialement protégés ne peuvent pas être attaqués ou peuvent faire l'objet de limitations plus strictes, même s'ils correspondent à la définition d'un objectif militaire.

Pour protéger les populations civiles et les services civils essentiels qui dépendent de l'infrastructure numérique, il convient de poursuivre la discussion afin de déterminer à quel moment l'utilisation militaire d'une infrastructure numérique essentiellement civile en fait un objectif militaire, et d'identifier et de mettre en œuvre d'autres mesures de protection possibles. Par exemple, le CICR a appelé les États, autant que faire se peut, à segmenter – c'est-à-dire séparer physiquement ou techniquement – les infrastructures numériques (ou des parties de celles-ci) utilisées à des fins militaires de celles destinées à un usage civil[35]. Il importe également de faire respecter toute protection spéciale conférée par le DIH.

La participation de civils aux activités numériques dans les conflits armés

Dans les conflits armés actuels, plusieurs tendances posent des risques pour les civils : les hackers civils mènent des opérations numériques qui prennent de plus en plus souvent pour cible des biens de caractère civil ; les parties à un conflit armé encouragent les civils à collecter des informations pertinentes sur le plan militaire par des moyens numériques, ce qui les expose à des attaques ; et les entreprises technologiques civiles qui fournissent des services et des infrastructures numériques aux forces armées risquent de perdre leur protection juridique.

Le DIH s'appuie sur le principe cardinal de la distinction. La participation croissante de civils dans les opérations numériques et l'utilisation des infrastructures numériques civiles à des fins militaires risquent d'éroder la protection que ce principe fondamental est censé fournir aux civils, notamment contre le risque d'être identifié à tort comme des cibles légitimes.

Les individus et les groupes, notamment les hackers et les employés d'entreprises technologiques, qui mènent des activités numériques dans le contexte de conflits armés sont tenus de respecter les limites définies par le DIH dans le cadre de telles activités[36] et doivent

---

[34] Les biens à double usage peuvent devenir des objectifs militaires s'ils répondent, en l'occurrence, à la définition de l'art. 52.2 du Protocole additionnel I : « 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 ».

[35] Par exemple, lorsqu'il s'agit de décider où conserver des données militaires – sur un cloud commercial non segmenté, un segment de cloud commercial ou au sein d'une infrastructure numérique militaire dédiée – les planificateurs et opérateurs militaires devraient éviter d'utiliser le cloud commercial non segmenté. Voir CICR, Le droit international humanitaire et les défis posés par les conflits armés contemporains, 2024, p. 63-64.

[36] En ce qui concerne les hackers civils intervenant dans le contexte de conflits armés, ces limites ont été résumées dans CICR, « 8 règles destinées aux « hackers civils » en temps de guerre et 4 obligations des États pour limiter leur action » : https://blogs.icrc.org/law-and-policy/fr/2024/01/12/8-regles-destinees-aux-hackers-civils-en-temps-deguerre-4-obligations-des-etats-pour-limiter-leur-action/. Sur la pertinence du DIH pour les entreprises privées, voir plus généralement la brochure du CICR intitulée *« Private Businesses and Armed Conflict: An Introduction to Relevant Rules of International Humanitarian Law,* 2024.

être conscients des risques qu'ils encourent. À titre exceptionnel, la participation de civils à des activités numériques peut constituer une « participation directe aux hostilités », ce qui signifie qu'un civil perd sa protection contre les attaques pendant la durée de cette participation. Toutefois, le DIH exige qu'en cas de doute, un individu soit considéré comme un civil et protégé en tant que tel[37].

La responsabilité des États dans la diffusion du DIH et les moyens de prévenir et de faire cesser les violations du DIH

En ce qui concerne la participation de civils à des activités numériques dans un conflit armé, il convient de noter que les États se sont engagés à respecter et à faire respecter le DIH. Si des hackers civils, des entreprises privées ou d'autres personnes ou entités privées agissent sur instruction, sur les directives ou sous le contrôle d'un État, ce dernier est responsable, au regard du droit international, de tout comportement de ces personnes qui ne serait pas conforme aux obligations juridiques internationales de l'État, y inclus en matière de DIH[38].

Même si la conduite des civils n'est pas imputable à une partie à un conflit armé, les États sont néanmoins tenus de veiller au respect du DIH. Au minimum, les parties à un conflit armé ne doivent pas encourager ou aider des civils impliqués dans des activités numériques à violer le DIH[39], par exemple en les encourageant à diriger des opérations numériques contre des biens de caractère civil. En outre, les États doivent faire connaître le DIH, prévenir et faire cesser les violations de ce droit, enquêter sur les crimes de guerre, y compris ceux commis par la population civile, et en poursuivre les auteurs[40].

[37] Protocole additionnel I, art. 50.1. S'il existe un risque que des enfants se retrouvent impliqués dans des hostilités au travers d'activités numériques et soient considérés comme participant directement aux hostilités, les belligérants ont l'obligation supplémentaire d'empêcher la participation d'enfants âgés de moins de 15 ans ou de moins de 18 ans, selon le cadre juridique applicable.
[38] Au regard du droit international public, un État est responsable du comportement de personnes, de groupes ou d'entités privés – y compris les hackers civils ou les groupes de hackers – s'ils sont « habilités par la loi de cet État à exercer des prérogatives de puissance publique », ou s'ils « agissent en fait sur les instructions de l'État ou sur ses directives ou sous son contrôle ». Voir la Commission du droit international, « La responsabilité de l'État pour fait internationalement illicite », 2001, art. 5 et 8.
[39] CICR, Commentaire de la Troisième Convention de Genève, 2020, par. 191 sur l'article premier.
[40] CICR, Commentaire de la Troisième Convention de Genève, 2020, par. 183 sur l'article premier.