Humanity In War

1er juin 2026

DOCUMENT DE TRAVAIL POUR LA CINQUIÈME CONSULTATION AVEC LES ÉTATS

Groupe de travail 6 – VEILLER À CE QUE LES TECHNOLOGIES NUMÉRIQUES SOIENT UTILISÉES D'UNE MANIÈRE CONFORME AU DIH DANS LES CONFLITS ARMÉS

CO-PRÉSIDÉ par le Ghana, le Luxembourg, le Mexique, la Suisse et le Comité international de la Croix-Rouge

Présentation générale

Les technologies de l'information et de la communication (ou technologies numériques) jouent aujourd'hui un rôle déterminant dans la vie des êtres humains à l'échelle mondiale. Dans notre monde numérisé et connecté, les services essentiels pour la population civile, tout comme la capacité à rester en lien avec ses proches et à favoriser le développement économique, dépendent de l'intégrité et de l'accessibilité des technologies numériques. Dans les zones touchées par un conflit, il est crucial de disposer de technologies numériques fiables pour permettre aux civils d'avoir accès aux biens et aux services essentiels, aux gouvernements de fournir des services, ainsi que pour soutenir les services médicaux et les activités humanitaires, notamment celles du Mouvement international de la Croix-Rouge et du Croissant-Rouge. Si les capacités numériques peuvent permettre aux belligérants d'atteindre des objectifs militaires sans nécessairement causer de dommages, ou en portant moins atteinte aux civils et aux biens de caractère civil que dans le cadre d'opérations cinétiques, leur utilisation dans les conflits contemporains a aussi donné lieu à des activités numériques préjudiciables affectant la population, les données et les infrastructures civiles, y compris par-delà les frontières internationales. Les disparités au niveau des capacités technologiques et de la résilience face aux cyber-risques peuvent venir encore aggraver ces menaces, notamment en réduisant la capacité des États et des autres acteurs concernés à prévenir, atténuer et gérer les dommages résultant d'activités numériques menées dans les conflits armés.

Le groupe de travail a souligné la nécessité impérieuse de protéger la population civile et de préserver la dignité humaine dans les conflits actuels et futurs. À cette fin, il est essentiel de garantir et de renforcer le respect du droit international humanitaire (DIH) dans l'utilisation qui est faite des technologies numériques en période de conflit armé, ce afin de protéger les infrastructures, les communications, les données et les réseaux civils contre les activités numériques préjudiciables menées dans les conflits armés.

Les États sont tenus d'utiliser les technologies numériques d'une manière conforme au droit international, en particulier à la Charte des Nations Unies, qui prévoit notamment l'obligation de régler les différends internationaux par des moyens pacifiques ainsi que l'interdiction de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies. Aucune disposition du DIH ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies. En aucun cas l'application du DIH ne légitime ni n'encourage les conflits armés.

Le groupe de travail a en outre recensé les bonnes pratiques et formulé les recommandations pratiques ci-après, visant notamment à :

- protéger la population civile, ainsi que les données et infrastructures civiles, contre les activités numériques préjudiciables ;
- protéger les services médicaux et les activités humanitaires contre les menaces numériques, et veiller au respect de l'interdiction de la violence sexuelle et de l'enrôlement et de l'utilisation d'enfants dans les hostilités, y compris par des moyens numériques ;
- remédier au problème de la propagation d'informations en violation du DIH ;
- réduire au minimum le risque de dommages à la population civile découlant de l'utilisation d'infrastructures numériques civiles à des fins militaires, et éviter que les civils participant à des activités numériques – qu'il s'agisse de hackers ou d'employés d'entreprises technologiques – ne portent atteinte au DIH ou ne se mettent eux-mêmes involontairement en danger.

Le groupe de travail a également souligné l'importance des éléments suivants si l'on veut renforcer la protection accordée par le DIH dans le cadre des activités numériques :

- reconnaître que, dans les zones en proie à un conflit, il est essentiel que les civils, les pouvoirs publics et les acteurs humanitaires puissent compter sur des technologies numériques fiables, et que les activités numériques peuvent avoir un coût humain même sans forcément causer de dommages physiques, un constat qui met en avant la nécessité de préserver l'humanité et la dignité humaine dans la guerre ;
- s'engager à promouvoir et préciser l'application du DIH aux activités numériques, ainsi qu'à prendre toutes les mesures individuelles et collectives nécessaires pour atténuer les risques encourus par la population civile et faire en sorte que les activités numériques ne portent pas atteinte aux protections conférées par le DIH ;
- poursuivre l'étude et l'examen des modalités d'application du DIH aux activités numériques, sur la base des débats menés au sein du groupe de travail ainsi que du présent document, en vue de renforcer et de promouvoir une compréhension commune permettant de protéger les civils ;

- encourager la transparence en diffusant publiquement les positions des États sur l'application du droit international – notamment du DIH – aux activités numériques, ainsi qu'en partageant les enseignements tirés et les pratiques recommandées en matière d'atténuation des dommages causés aux civils ;
- favoriser le renforcement des capacités aux niveaux bilatéral, régional et mondial afin que les États soient mieux à même de mettre en œuvre et d'appliquer le DIH dans le cadre des activités numériques.

Résultats

1. Protéger la population civile, ainsi que les données et infrastructures civiles, contre les dommages résultant d'activités numériques menées dans les conflits armés

Les conflits armés contemporains montrent que les activités numériques peuvent poser des risques pour la population civile ainsi que pour les données et les infrastructures civiles. Ces activités peuvent avoir de graves répercussions sur les civils ainsi que les autres personnes et biens protégés, notamment lorsque les services essentiels – c'est-à-dire les services indispensables à la survie des populations civiles, ainsi que l'ensemble des systèmes interdépendants dont elles dépendent pour subvenir à leurs besoins fondamentaux – se trouvent perturbés, même en l'absence de dommages physiques. Les services essentiels comprennent par exemple l'approvisionnement en électricité et en eau, l'assainissement, la production et la distribution de nourriture, les télécommunications, les soins de santé, l'éducation, les services humanitaires et d'urgence ou encore les services financiers.

Lorsque des activités numériques sont menées dans le contexte d'un conflit armé et en rapport avec celui-ci, il est impératif de respecter en tout temps le DIH, notamment (sans s'y limiter) les principes d'humanité, de nécessité militaire, de distinction, de proportionnalité et de précaution.

Les opérations numériques dont on peut raisonnablement attendre qu'elles causent des décès ou des blessures, ou qu'elles endommagent ou détruisent des biens, constituent des attaques au sens du DIH. Cela inclut les opérations raisonnablement susceptibles de mettre des systèmes numériques hors d'usage et de nécessiter une action pour rétablir leur fonctionnement. Ces opérations numériques doivent être menées dans le respect de l'ensemble des principes et règles du DIH qui régissent la conduite des hostilités, notamment l'interdiction des attaques contre les civils et les biens de caractère civil, des attaques sans discrimination et des attaques disproportionnées, ainsi que le principe de précaution.

Les données sont au cœur d'un monde toujours plus numérisé et jouent un rôle central dans le fonctionnement des services civils essentiels et des activités humanitaires. La manière dont les données sont traitées dans les conflits armés a une incidence sur la vie des personnes et leur dignité. Les données médicales, biométriques, financières et humanitaires, entre autres, font partie intégrante de la prestation de services publics et sociaux. Le fait de supprimer, manipuler ou divulguer de telles données sans autorisation, ou d'en refuser l'accès, peut perturber des services essentiels et exposer des personnes et des communautés à de graves dangers. Il importe de noter que les activités de collecte d'informations ne sont pas interdites en tant que telles par le DIH, même lorsqu'elles impliquent d'accéder à des données.

Plusieurs principes et règles du DIH protègent la population civile, ainsi que les données et infrastructures civiles, contre les dangers résultant d'activités numériques menées dans les conflits armés, notamment :

- le principe selon lequel le droit des parties à un conflit armé de choisir leurs moyens et méthodes de guerre n'est pas illimité, et qu'une partie à un conflit armé ne pourra recourir qu'aux moyens et méthodes de guerre qui sont nécessaires à l'affaiblissement des forces militaires de l'ennemi ;
- les principes et règles qui régissent la conduite des hostilités, notamment les principes de distinction, de proportionnalité et de précaution ainsi que l'interdiction connexe des attaques contre les civils et les biens de caractère civil, des attaques sans discrimination et des attaques disproportionnées ;
- l'obligation de veiller constamment, lors de la conduite des opérations militaires, à épargner la population civile, les personnes civiles et les biens de caractère civil ;
- les règles protégeant les biens du pillage, de la saisie et de la destruction.

Les mesures suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour renforcer la protection de la population civile, ainsi que des données et infrastructures civiles, contre les dommages résultant d'activités numériques menées dans les conflits armés :

a) établir et appliquer des procédures rigoureuses pour les opérations numériques afin de garantir leur conformité au DIH, notamment en vérifiant que les cibles constituent bien des objectifs militaires et ne jouissent pas d'une protection spéciale, et en évaluant, en évitant ou du moins en réduisant au minimum le risque de causer incidemment des dommages civils ;

b) fonder les opérations numériques, y compris les procédures de sélection des cibles, sur l'ensemble des informations raisonnablement disponibles et activement recherchées auprès de sources pertinentes, notamment des données et renseignements fiables, en s'appuyant également sur des conseils juridiques, comme l'exige le DIH, et, dans toute la mesure possible, faire appel à des experts de la cybersécurité et d'autres spécialistes techniques pertinents concernant la structure, l'interconnectivité et la dépendance des civils vis-à-vis des infrastructures numériques ;

c) veiller, lorsque des infrastructures numériques constituent un objectif militaire au regard du DIH mais continuent de remplir des fonctions civiles, à prendre en compte tous les dommages raisonnablement prévisibles, directs et indirects, pouvant être causés incidemment à la population, aux données et aux infrastructures civiles du fait de la perte totale ou partielle de leur usage civil, ainsi que les répercussions sur les services civils qu'elles fournissent ou facilitent, conformément aux principes et règles de proportionnalité et de précaution dans la planification et la conduite des attaques ;

d) veiller, dans la mise en œuvre de l'obligation de prendre toutes les précautions pratiquement possibles dans le choix des moyens et méthodes de guerre, à choisir les moyens et méthodes dont on peut attendre qu'ils causent le moins de dommages collatéraux aux civils, notamment en déterminant précisément si des moyens et méthodes numériques ou d'autres moyens et méthodes non cinétiques réduiraient le risque de dommages civils par rapport aux solutions cinétiques possibles ;

e) imposer des limites géographiques, temporelles et systémiques appropriées (« cloisonnement ») dans la conduite des opérations numériques afin d'éviter, ou du moins de réduire au minimum, le risque de causer incidemment des dommages civils ;

f) surveiller en permanence les opérations numériques et maintenir la capacité à les adapter ou y mettre un terme pour éviter des dommages civils involontaires ou excessifs. Lorsque cela est pratiquement possible, incorporer des mesures de protection techniques, telles que des coupe-circuit, permettant de stopper, limiter ou isoler des opérations numériques lorsqu'elles risquent de se propager au-delà de la cible visée, notamment à des infrastructures ou réseaux civils ou à ceux d'États tiers ;

g) prendre toutes les mesures appropriées pour faire en sorte que les activités numériques reposant sur l'intelligence artificielle ou d'autres technologies émergentes, ou rendues possibles par celles-ci, soient conduites d'une manière conforme au DIH ainsi qu'aux mesures décrites ci-dessus.

2. Réduire au minimum le risque de dommages à la population civile découlant de l'utilisation d'infrastructures numériques civiles à des fins militaires dans les conflits armés

À l'exception de certains réseaux militaires, l'environnement numérique est majoritairement civil. Toutefois, l'interconnexion entre les réseaux civils et militaires et l'utilisation d'infrastructures numériques civiles à des fins militaires posent des problèmes spécifiques pour leur protection.

Lorsqu'une infrastructure numérique civile, y compris fournie par des entreprises technologiques, est utilisée à des fins militaires, cela ne signifie pas systématiquement que cette infrastructure, en tout ou en partie, devienne un objectif militaire au sens du DIH. Néanmoins, l'utilisation à des fins militaires peut accroître le risque que cette infrastructure soit attaquée, exposant ainsi à des dommages incidents les civils et les biens de caractère civil situés à proximité de cette infrastructure, qui y sont connectés numériquement ou qui en dépendent.

Le DIH interdit d'attaquer des biens de caractère civil, y compris les infrastructures numériques civiles. Mais leur utilisation à des fins militaires peut faire de telles infrastructures, en tout ou en partie, des objectifs militaires, uniquement tant que les critères prévus par le DIH sont remplis. Cette analyse exige une attention particulière et une évaluation au cas par cas.

En cas d'attaque menée contre de tels objectifs militaires, les États et les parties aux conflits armés doivent respecter l'interdiction de lancer des attaques sans discrimination ou disproportionnées ainsi que le principe de précaution, notamment lorsque la population civile dépend de ces infrastructures numériques pour la fourniture de services essentiels. Toutes les précautions pratiquement possibles doivent être prises pour faire en sorte que les attaques menées n'affectent que les composantes ou fonctions des infrastructures numériques qui sont utilisées à des fins militaires, ainsi que pour éviter ou du moins réduire au minimum les dommages causés aux infrastructures qui remplissent des fonctions civiles.

Afin de protéger la population civile contre les effets des attaques, les États et les parties aux conflits armés doivent, dans la mesure du possible, prendre toutes les précautions nécessaires pour protéger les civils et les biens de caractère civil se trouvant sous leur contrôle contre les dangers découlant des opérations militaires.

Outre les mesures décrites sous le résultat 1 ci-dessus, les mesures suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour réduire au minimum le risque de dommages à la population civile découlant de l'utilisation d'infrastructures numériques civiles à des fins militaires dans les conflits armés :

a) allouer des ressources financières et techniques suffisantes et prendre des mesures en matière de planification, de conception et de configuration avant et pendant les conflits armés en vue de réduire au minimum l'exposition des civils et des infrastructures numériques civiles aux effets des activités numériques menées dans les conflits armés ;

b) séparer physiquement ou techniquement, dans toute la mesure possible, les composantes des infrastructures numériques qui sont utilisées à des fins militaires de celles qui remplissent des fonctions civiles, notamment en segmentant le réseau ou en appliquant d'autres mesures de configuration appropriées. Séparer, dans toute la mesure possible, les données utilisées à des fins militaires de celles répondant à des besoins civils, par exemple au niveau des dispositifs de stockage, de gestion ou de contrôle des accès ;

c) renforcer la résilience des infrastructures et services numériques civils essentiels, notamment en prévoyant des redondances, en planifiant des interventions d'urgence et en adoptant d'autres mesures visant à réduire le risque de causer incidemment des dommages civils.

3. Réduire au minimum les risques liés à la participation de civils se trouvant sur le territoire d'un État, sous sa juridiction ou sous son contrôle à des activités numériques menées dans les conflits armés

Dans les conflits armés contemporains, les civils participent de plus en plus souvent à des activités numériques menées dans les conflits armés. Dans certains cas, les États ont toléré, facilité ou encouragé le fait que des civils conduisent des activités numériques contre l'adversaire, y compris des activités susceptibles de toucher des civils ou des biens de caractère civil.

Lorsque des civils sont trop proches des hostilités, ils risquent de subir des dommages. Beaucoup n'ont sans doute pas conscience des risques encourus, des conséquences juridiques potentielles de leurs actes ou des règles du DIH qu'ils doivent respecter.

Les civils – qu'il s'agisse de hackers ou d'employés d'entreprises technologiques – sont tenus de respecter le DIH et les autres corps de droit applicables lorsqu'ils mènent des activités numériques dans le contexte d'un conflit armé et en rapport avec celui-ci.

Lorsque des civils (y compris des hackers et des employés d'entreprises technologiques) mènent des activités numériques dans un conflit armé imputables à des États ou des parties aux conflits armés, le droit international tient ces derniers pour responsables des violations du DIH commises par ces civils. Les États doivent prendre toutes les mesures appropriées pour prévenir les violations du DIH commises par le biais d'activités numériques menées par des civils se trouvant sur leur territoire, sous leur juridiction ou sous leur contrôle, ou facilitées par ces activités, et pour réprimer de telles violations si elles se produisent. Les États veillent en outre à diffuser le DIH aussi largement que possible afin de le faire connaître à leur population civile. Ils ne doivent pas encourager, favoriser ou faciliter la commission de violations du DIH par des civils, y compris par le biais d'activités numériques.

Les civils sont protégés contre les attaques sauf s'ils participent directement aux hostilités, et pendant la durée de cette participation. Dans certaines circonstances bien précises, la participation de civils à des activités numériques peut constituer une participation directe aux hostilités. Afin d'éviter que des

civils ne soient pris pour cible par erreur ou de façon arbitraire, les parties aux conflits armés doivent prendre toutes les précautions pratiquement possibles pour déterminer si un individu est une personne civile et, dans l'affirmative, s'il participe directement aux hostilités, y compris par le biais d'activités numériques. En cas de doute, le DIH exige que ladite personne soit considérée comme étant protégée contre les attaques.

Les enfants ne doivent pas être autorisés à prendre part aux hostilités dans les conflits armés, y compris par le biais d'activités numériques.

Les mesures suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour réduire au minimum les risques liés à la participation de civils à des activités numériques menées dans les conflits armés :

a) prendre les mesures appropriées pour informer les civils pouvant être amenés à participer à des activités numériques dans le contexte d'un conflit armé et en rapport avec celui-ci des risques juridiques et pratiques qu'ils encourent de ce fait. Notamment, partager des informations sur les règles du DIH à travers les médias sociaux, des applications dédiées, la radio ou d'autres moyens de communication de masse, ou élaborer des modèles de codes de conduite respectueux du DIH à l'intention des civils menant des activités numériques ;

b) s'abstenir, dans la mesure du possible, d'impliquer des civils dans des opérations numériques constituant une participation directe aux hostilités, afin de les protéger contre les dangers découlant des opérations militaires. Lorsqu'une telle participation se produit néanmoins, les intégrer autant que possible dans les forces armées ;

c) prendre toutes les mesures pratiquement possibles pour éviter que des enfants participent aux hostilités par le biais d'activités numériques, par exemple en proposant des programmes d'enseignement et de sensibilisation destinés aux enfants et aux personnes qui prennent soin d'eux ; en adaptant la législation nationale et les politiques interdisant l'enrôlement et l'utilisation d'enfants de manière à englober les moyens de communication en ligne, et en assurant leur application ; enfin, en fixant un âge minimum pour l'accès aux outils numériques susceptibles de permettre une participation directe aux hostilités, le cas échéant.

4. Protéger les produits et services numériques civils fournis par des entreprises technologiques dans les conflits armés

Les produits et services numériques fournis par des entreprises technologiques sont largement utilisés par la population civile, les gouvernements et les organisations humanitaires impartiales, y compris en période de conflit armé. C'est pourquoi leur perturbation, leur dégradation ou leur utilisation abusive peuvent avoir d'importantes conséquences humanitaires. Ces produits et services numériques, de même que le personnel civil qui les fournit, sont protégés en vertu du DIH.

Parallèlement, les entreprises technologiques sont de plus en plus nombreuses à fournir des produits ou services numériques, par exemple en matière de cybersécurité, à des parties aux conflits armés, ce qui peut entraîner la perte de la protection que leur confère le DIH. Dans de tels cas, les civils et les biens de caractère civil qui dépendent de ces produits et services peuvent eux aussi être exposés à certains risques.

Afin de renforcer la protection des produits et services numériques civils fournis par des entreprises technologiques dans les conflits armés, ces dernières devraient :

a) prendre dûment en considération le fait que fournir des produits et services numériques à des parties aux conflits armés implique des risques à la fois juridiques et pratiques ;

b) comprendre et évaluer les risques de dommages causés aux civils et aux biens de caractère civil (y compris à leur propre personnel et à leurs biens) et prendre des mesures pour réduire ces risques au minimum, qu'ils soient liés à une proximité physique, à une connexion numérique ou à une dépendance vis-à-vis des infrastructures ou des services en question. Dans la mesure du possible, séparer physiquement ou techniquement les infrastructures, services et produits utilisés pour soutenir les opérations militaires de ceux qui sont destinés à un usage civil ;

c) prendre des mesures pour empêcher leur personnel de mener, de faciliter ou de participer de quelque manière que ce soit à des activités constituant des violations du DIH, y compris en fournissant des produits ou services numériques à des parties aux conflits armés, et prendre les mesures qui s'imposent si de telles situations devaient toutefois survenir.

5. Protéger les services médicaux, les activités humanitaires et les autres personnes, biens et activités bénéficiant d'une protection spéciale contre les dommages résultant d'activités numériques menées dans les conflits armés

Le secteur de la santé et les organisations humanitaires impartiales sont particulièrement vulnérables face aux activités numériques menées dans les conflits armés. Les services médicaux et humanitaires étant de plus en plus dépendants de systèmes interconnectés et de données numériques, toute perturbation des infrastructures ou des services numériques peut avoir une incidence directe sur des opérations médicales vitales, compromettre des données sensibles, entraver le travail des organisations humanitaires impartiales ainsi que de leur personnel, et mettre en péril la fourniture de l'assistance.

Conformément au DIH, le personnel médical ainsi que les unités et moyens de transport sanitaires, de même que le personnel et les biens humanitaires, doivent être respectés et protégés en tout temps, y compris contre les dommages résultant d'activités numériques. Les activités numériques menées dans les conflits armés ne doivent pas perturber indûment le fonctionnement des services médicaux et des activités humanitaires, y compris leurs données et leurs systèmes numériques et de communication.

La confidentialité des données médicales et humanitaires doit être respectée en vertu du DIH. Cette protection est essentielle pour préserver la confiance dans le travail des services médicaux et des organisations humanitaires impartiales.

Les parties aux conflits armés doivent par ailleurs prendre toutes les mesures pratiquement possibles, dans les circonstances qui prévalent et compte tenu des ressources à leur disposition, pour éviter que les services médicaux et les activités humanitaires ne subissent des dommages, y compris par le biais d'activités numériques menées par des tiers – tels que des cybercriminels et d'autres acteurs non étatiques – et non imputables à une partie au conflit armé, conformément au DIH et aux autres dispositions applicables du droit international.

Certains autres biens et activités bénéficiant d'une protection spéciale en vertu du DIH, notamment les biens indispensables à la survie de la population civile, les ouvrages et installations contenant des forces dangereuses, les biens culturels et la protection civile, peuvent aussi être exposés à de graves risques du fait d'activités numériques. La protection spéciale qui leur est accordée doit être respectée, y compris

dans le cadre d'activités numériques menées dans les conflits armés. Cette protection s'étend à leurs données et aux infrastructures numériques indispensables à leur fonctionnement.

Les activités numériques peuvent en outre être utilisées pour commettre ou faciliter des actes de violence sexuelle ou pour enrôler ou utiliser des enfants dans les hostilités. Or le DIH interdit la violence sexuelle et l'enrôlement ou l'utilisation d'enfants dans les hostilités, y compris quand ces actes sont commis par le biais d'activités numériques ou encouragés ou facilités par ces activités.

Les mesures suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour protéger les services médicaux, les activités humanitaires et les autres personnes, biens et activités bénéficiant d'une protection spéciale contre les dommages résultant d'activités numériques menées dans les conflits armés :

a) appuyer les discussions et les efforts déployés pour rendre la protection spéciale conférée par le DIH aux services médicaux et aux activités humanitaires identifiable et visible dans l'environnement numérique, notamment en créant un « emblème numérique », et continuer de dialoguer avec le CICR pour explorer les voies juridiques, techniques et diplomatiques conduisant à sa mise en œuvre ;

b) réaffirmer explicitement l'engagement à respecter et protéger les services médicaux et les activités humanitaires, y compris leurs données et leurs systèmes numériques et de communication, à faciliter leurs opérations dans l'environnement numérique, ainsi qu'à respecter la protection spéciale conférée aux biens indispensables à la survie de la population civile, notamment leurs données et les infrastructures numériques indispensables à leur fonctionnement. Ces engagements devraient figurer dans la législation et les politiques nationales ainsi que dans la doctrine et la pratique militaires ;

c) soutenir et faciliter, dans la mesure du possible, l'élaboration de mesures adéquates de cybersécurité et de protection des données pour les prestataires de services médicaux et les organisations humanitaires impartiales, et contribuer à renforcer leur résilience face aux menaces numériques qui pèsent sur leurs systèmes et leurs opérations ;

d) renforcer les cadres juridiques et politiques nationaux pertinents qui régissent les comportements en ligne pouvant constituer ou faciliter des violations du DIH – notamment (sans s'y limiter) les cadres relatifs à la violence sexuelle et à l'enrôlement ou l'utilisation d'enfants dans les conflits armés – et assurer une mise en œuvre et une coordination efficaces entre les autorités compétentes. Plus particulièrement, afin de prévenir l'enrôlement et l'utilisation illicites d'enfants, déployer davantage d'efforts au niveau des gouvernements pour sensibiliser les enfants et les personnes qui prennent soin d'eux aux risques associés ;

e) intégrer des mesures de protection spécifiques dans la doctrine, les procédures opérationnelles standards et les règles d'engagement militaires afin de prévenir et de traiter les violations commises par le biais d'activités numériques ou facilitées par de telles activités, y compris la violence sexuelle ainsi que l'enrôlement ou l'utilisation d'enfants dans les hostilités. Dans la mesure du possible, réglementer l'emploi de dispositifs numériques personnels dans les contextes opérationnels, limiter la diffusion d'images ou d'informations sensibles, et interdire l'utilisation de technologies numériques aux fins de l'enrôlement ou l'utilisation illicites d'enfants dans les hostilités.

6. Remédier au problème de la propagation d'informations en violation du DIH

Dans les conflits armés contemporains, les technologies numériques sont de plus en plus utilisées pour propager des informations susceptibles de violer le DIH. Si les opérations d'information font depuis longtemps partie de la guerre et ne sont pas en soi illicites, l'utilisation des technologies numériques – en particulier sur les plateformes de médias sociaux ou les applications de messagerie, ou lorsqu'elles sont couplées à l'intelligence artificielle et à d'autres technologies émergentes – peut fortement accroître l'ampleur, la portée et la vitesse de propagation des informations préjudiciables.

Les États et les parties aux conflits armés doivent s'abstenir de propager des informations en violation du DIH, y compris au moyen de technologies numériques, et prendre toutes les mesures pratiquement possibles pour éviter que cela se produise. Il s'agit notamment de ne pas propager d'informations qui incitent ou encouragent à commettre des violations du DIH, exposent des personnes privées de liberté à des insultes ou à la curiosité publique, ou dont le but premier est de répandre la terreur parmi la population civile. Dans certaines circonstances bien précises, la diffusion d'informations peut constituer ou faciliter un acte de perfidie.

Les services médicaux et les activités humanitaires doivent être protégés contre la désinformation numérique ayant pour effet de perturber leur travail dans les conflits armés. Ces actes entravent en effet indûment le personnel médical et humanitaire et ses activités, et sont incompatibles avec l'obligation de les respecter et les protéger.

Les mesures suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour remédier au problème de la propagation d'informations en violation du DIH :

a) prendre toutes les mesures pratiquement possibles pour évaluer, prévenir et atténuer le risque que des opérations d'information – y compris celles reposant sur l'intelligence artificielle ou d'autres technologies émergentes, ou rendues possibles par celles-ci – ne portent atteinte à la population civile et aux autres personnes protégées, notamment en compromettant leur sécurité, leur dignité ou leur accès aux services essentiels ;

b) ne pas diffuser d'informations qui déshumanisent l'adversaire ou propagent la haine envers la population civile, y compris au moyen de technologies numériques, et prendre les mesures appropriées pour s'assurer que les forces armées, les autres autorités publiques et les personnes agissant en leur nom ne se livrent pas à de telles pratiques ;

c) aider, dans la mesure du possible, les prestataires de services médicaux et les organisations humanitaires impartiales à accroître leur résilience face à la désinformation et aux autres opérations d'information préjudiciables, notamment en renforçant leur capacité à recueillir, vérifier et diffuser des informations correctes dans le cadre de leurs activités médicales ou humanitaires ; en renforçant leur préparation et leur planification d'urgence en cas d'exposition à des informations préjudiciables ; et en encourageant l'élaboration de réponses adaptées au contexte face aux informations préjudiciables qui touchent les civils dans leurs zones d'intervention ;

d) dialoguer avec les acteurs concernés, y compris le secteur technologique, afin de réduire le risque que des plateformes en ligne ou d'autres services numériques soient utilisés pour inciter ou encourager à commettre des violations du DIH, ou faciliter ces actes, ou pour infliger, de quelque manière que ce soit, des dommages aux civils et aux biens de caractère civil. Notamment, mettre en place les cadres juridiques et politiques appropriés et promouvoir l'adoption par les entreprises technologiques de mesures de protection et de pratiques

permettant de détecter, d'évaluer et de gérer les informations préjudiciables dans les situations de conflit armé ;

e) s'employer à renforcer la résilience de la société face aux opérations d'information préjudiciables, notamment en favorisant la mise à disposition d'informations fiables, en protégeant les journalistes et les médias lorsque le DIH et tout autre droit applicable l'exigent, et en promouvant des mesures de préparation qui renforcent la capacité de la population civile à accéder à des informations fiables dans les conflits armés ;

f) s'abstenir de bloquer l'accès des civils à Internet ou à d'autres services numériques, à moins que cela soit justifié par d'impérieuses nécessités militaires, car ces mesures risquent de porter préjudice à la population civile. Lorsque de telles restrictions doivent toutefois être imposées, prendre des mesures d'atténuation pour limiter autant que possible les effets néfastes sur les civils.

7. Mesures transversales visant à renforcer la mise en œuvre du DIH dans le cadre des activités numériques

Les mesures transversales suivantes, qui relèvent à la fois de dispositions législatives existantes et de bonnes pratiques, sont particulièrement importantes pour renforcer la mise en œuvre du DIH dans le cadre des activités numériques, y compris en temps de paix :

a) diffuser les connaissances sur le DIH auprès des forces armées et de la population au sens large, en particulier des personnes susceptibles de participer à des activités numériques, ainsi qu'intégrer les principes et règles du DIH et leur application aux activités numériques dans la législation nationale et la doctrine, les procédures opérationnelles standards, les règles d'engagement, les codes de conduite et les programmes de formation militaires, selon qu'il convient ;

b) mettre des conseillers juridiques qualifiés à la disposition des unités et commandements militaires chargés des activités numériques, en particulier lors de la planification et de la conduite de ces opérations ;

c) procéder à un examen de la licéité des capacités numériques pouvant servir de nouvelles armes, de nouveaux moyens ou de nouvelles méthodes de guerre au moment où elles sont étudiées, mises au point, acquises ou adoptées, pour s'assurer que leur emploi – dans certaines circonstances ou en toutes circonstances – ne serait pas interdit par le droit international. Cet examen consistera notamment à tester, évaluer et vérifier rigoureusement ces capacités numériques avant de les valider, afin de mieux comprendre leur fonctionnement, leur propagation et leurs effets potentiels sur les systèmes civils ;

d) adopter toutes les mesures nécessaires, qu'elles soient législatives, réglementaires ou autres, et prendre, s'il y a lieu, des sanctions pénales afin de prévenir et réprimer les violations du DIH commises par le biais d'activités numériques menées par des personnes se trouvant sur le territoire d'un État, sous sa juridiction ou sous son contrôle, ou facilitées par ces activités ;

e) prendre les mesures appropriées lors de la conception, de la mise au point et du déploiement des capacités numériques afin de réduire le risque qu'elles se propagent involontairement ou qu'elles soient détournées, transformées ou utilisées abusivement d'une manière susceptible de constituer des violations du DIH ou d'y contribuer, notamment en adoptant des mesures de cybersécurité appropriées, telles que le cryptage, ainsi que des mesures techniques, telles que

des coupe-circuit intégrés, afin de limiter leur propagation ou leur réutilisation sans autorisation ;

f) favoriser l'échange volontaire d'informations et les mesures de renforcement de la confiance visant à réduire les risques pour les infrastructures numériques civiles, y compris les échanges de bonnes pratiques entre États, la mise en place de canaux de communication ainsi que d'autres mesures pratiques de réduction des risques et, s'il y a lieu, l'établissement de mécanismes de signalement volontaire des incidents numériques graves ayant causé incidemment des dommages civils, afin de renforcer la compréhension collective et l'atténuation des risques ;

g) encourager la transparence et la compréhension commune en élaborant et en diffusant publiquement des prises de position des États sur la façon dont le droit international, y compris le DIH, s'applique aux activités numériques, notamment au travers de déclarations nationales ou conjointes, ainsi qu'en partageant les enseignements tirés et les pratiques recommandées en vue de réduire au minimum les dommages civils ;

h) favoriser le renforcement des capacités aux niveaux bilatéral, régional et mondial afin que les États soient mieux à même de mettre en œuvre et d'appliquer le DIH dans le cadre des activités numériques ;

i) encourager la coopération entre les États, les entreprises technologiques, les organisations humanitaires impartiales et la société civile afin d'utiliser les technologies numériques de manière à renforcer la protection des civils, notamment en élaborant des orientations ou des dispositions pratiques adaptées au contexte ;

j) encourager la coopération entre les entreprises technologiques et les organisations humanitaires impartiales afin d'améliorer la préparation et la réponse aux menaces numériques touchant les personnes et les biens protégés, notamment par l'échange d'informations et le soutien en matière de cybersécurité, tout en respectant les principes humanitaires de neutralité, d'impartialité et d'indépendance ;

k) intégrer des approches tenant compte de l'âge, du genre et du handicap éventuel dans les cadres nationaux et la pratique opérationnelle afin de renforcer la mise en œuvre du DIH, y compris en identifiant et en gérant les risques numériques.