Humanity In War

1er avril 2026

DOCUMENT DE TRAVAIL POUR LA QUATRIÈME 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 numériques sont devenues indispensables à la vie des êtres humains à travers le monde. Dans notre monde numérisé et connecté, les services essentiels pour la population civile, tout comme la capacité à être en lien avec ses proches et à poursuivre 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 des dommages, ou en portant moins atteinte aux civils ou aux biens de caractère civil que les opérations cinétiques, leur utilisation dans les conflits contemporains a aussi donné lieu à des activités numériques préjudiciables affectant la population et les infrastructures civiles, y compris par-delà les frontières internationales.

Le groupe de travail a souligné la nécessité impérative de protéger la population civile et de préserver la dignité humaine dans les conflits actuels et futurs. À cette fin, il faut absolument veiller à ce que les technologies numériques soient utilisées d'une manière conforme au droit international humanitaire (DIH) dans les conflits armés et renforcer le respect du DIH, afin d'éviter que nos

infrastructures, nos réseaux et nos moyens de communication soient mis hors d'état de fonctionner, que nos données soient effacées et nos sociétés paralysées.

Le groupe de travail a également formulé les recommandations pratiques ci-après, visant notamment à :

- protéger la population, les données et les 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 diffusion d'informations en violation du DIH ;
- réduire au minimum le risque de dommages causés à la population civile du fait de l'utilisation d'infrastructures numériques civiles à des fins militaires et éviter que les civils – qu'il s'agisse de hackers ou d'employés d'entreprises technologiques – participant à des activités numériques ne violent le DIH ou ne se mettent eux-mêmes involontairement en danger.

Pour promouvoir le respect du DIH lorsque des activités numériques sont menées, le groupe de travail a souligné l'importance de :

- reconnaître que, dans les zones en proie à un conflit, il est essentiel que les civils, les gouvernements et les acteurs humanitaires puissent compter sur des technologies numériques fiables, et que les activités numériques peuvent avoir un coût humain, en termes de souffrances infligées, de blessures ou de destruction, même sans forcément causer de dommage physique, 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, et à prendre des mesures pratiques, individuelles ou collectives, 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, afin de parvenir à une compréhension commune permettant de protéger les civils ;
- promouvoir la transparence en diffusant publiquement les positions nationales 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 de renforcer la capacité des États à mettre en œuvre et à appliquer le DIH aux activités numériques.

Résultats

1. Protéger la population, les données et les infrastructures civiles contre les dommages découlant des 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 gravement porter atteinte aux civils ainsi qu'aux autres personnes et biens protégés, notamment lorsque des services civils essentiels, tels que l'électricité, l'eau, l'assainissement, les télécommunications, la santé, les services humanitaires et d'urgence ou les services financiers, sont perturbés, même en l'absence de dommages physiques.

Lorsque des activités numériques sont menées dans une situation de conflit armé ou en lien avec un conflit armé, le DIH doit être respecté en tout temps, notamment les principes d'humanité, de nécessité militaire, de distinction, de proportionnalité et de précaution.

Les opérations numériques dont on peut attendre qu'elles causent la mort ou des blessures à des personnes, ou qu'elles endommagent ou détruisent des biens, constituent des attaques au sens du DIH. Cela inclut les opérations susceptibles de mettre des équipements ou des systèmes hors d'usage et qui nécessitent une action (remplacement, réinstallation ou réparation) pour rétablir leur fonctionnement. Ces opérations numériques doivent être menées conformément à 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 indispensables au fonctionnement des services civils essentiels et des activités humanitaires. La manière dont les données sont traitées pendant 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. Supprimer, manipuler, refuser l'accès ou divulguer ces données sans autorisation peut perturber des services essentiels et exposer des individus et des communautés à de graves dangers.

Plusieurs principes et règles de DIH offrent une protection à la population civile ainsi qu'aux données et infrastructures civiles contre les dangers découlant des activités numériques menées dans les conflits armés, notamment :

- le principe selon lequel une partie à un conflit armé ne devra 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 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 ;
- l'obligation de veiller en permanence à épargner la population civile, les personnes civiles et les biens de caractère civil dans la conduite des opérations militaires ;
- les règles protégeant les biens du pillage, de la saisie et de la destruction.

Les activités de collecte d'informations ne sont pas interdites en tant que telles par le DIH, même lorsqu'elles impliquent d'accéder aux données.

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, il est essentiel que les États et les parties aux conflits armés s'emploient à :

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

b) fonder les opérations numériques, y compris les procédures de choix des objectifs, sur l'ensemble des informations raisonnablement disponibles et activement recherchées auprès de sources pertinentes, notamment des données et renseignements fiables, avec l'aide de conseils juridiques, comme l'exige le DIH ; et, dans toute la mesure du 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 de l'infrastructure numérique ;

c) veiller, lorsque les infrastructures numériques constituent un objectif militaire au regard du DIH mais continuent d'être utilisées à des fins civiles, à prendre en compte tous les effets raisonnablement prévisibles, directs et indirects, pouvant être causés incidemment à la population civile, ainsi qu'aux données et infrastructures civiles du fait de la perte totale ou partielle de leur usage civil, notamment l'impact sur les services civils essentiels qu'elles fournissent ou facilitent, conformément aux principes et aux 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) appliquer des limites géographiques, temporelles et systémiques appropriées (« cloisonnement ») dans la conduite des opérations numériques afin d'éviter, ou au moins de réduire au minimum le risque de causer incidemment des dommages civils ;

f) surveiller en permanence les opérations numériques et garantir la capacité de les adapter ou d'y mettre un terme afin d'éviter des dommages civils involontaires ou excessifs. Lorsque cela est pratiquement possible, incorporer des protections 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 dans les réseaux ou infrastructures civils ou dans ceux d'États tiers.

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 de l'infrastructure numérique civile à des fins militaires posent des problèmes spécifiques pour leur protection.

Lorsque l'infrastructure numérique civile, y compris l'infrastructure fournie par les entreprises technologiques, est utilisée à des fins militaires, cela ne signifie pas que toute utilisation fait de cette infrastructure, ou d'une partie de cette infrastructure, 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 les civils et les biens de caractère civil situés à proximité physique ou connectés numériquement à de telles cibles ou qui en dépendent, à des dommages incidents.

Le DIH interdit d'attaquer des biens de caractère civil, y compris les infrastructures numériques civiles. Cependant, l'utilisation à des fins militaires peut faire de ces infrastructures, ou de parties de celles-ci, des objectifs militaires.

En cas d'attaque menée contre ces objectifs militaires, les États et les parties au conflit armé doivent respecter l'interdiction de lancer des attaques indiscriminées ou disproportionnées ainsi que le principe de précaution, notamment lorsque la population civile dépend de ces infrastructures numériques pour la fourniture de services essentiels. Lorsque cela est pratiquement possible, ils doivent veiller à ce que les attaques ne visent que les éléments ou fonctions des infrastructures numériques utilisés à des fins militaires en épargnant ceux qui sont destinés à un usage civil.

Pour protéger la population civile contre les effets des attaques, les États et les parties au conflit armé doivent, dans toute la mesure du possible, prendre toutes les précautions nécessaires pour protéger les civils et les biens de caractère civil placés sous leur contrôle contre les dangers résultant des opérations militaires.

Pour réduire au minimum le risque de dommages à la population civile résultant de l'utilisation des infrastructures numériques civiles à des fins militaires dans les conflits armés, et en plus des mesures présentées dans le Résultat 1 ci-dessus, il est essentiel que les États et les parties au conflit armé sous le contrôle desquels ces infrastructures sont placées s'emploient à :

a) allouer les ressources financières et techniques appropriées et prendre des mesures en matière de planification, de conception et de configuration avant et pendant les conflits armés ;

b) séparer, dans la mesure du possible, physiquement ou techniquement les éléments des infrastructures numériques qui sont utilisés à des fins militaires de ceux destinés à un usage civil, notamment en segmentant le réseau ou en appliquant d'autres mesures de configuration appropriées. Cela inclut, lorsque cela est possible, de séparer les données utilisées à des fins militaires de celles destinées à un usage civil, par exemple au niveau du stockage, de la gestion ou des dispositions relatives au 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 aux activités numériques menées dans les conflits armés sur le territoire d'un État ou sous sa juridiction ou son contrôle

Dans les conflits armés contemporains, la participation de civils aux activités numériques menées dans les conflits armés s'est amplifiée. Dans certains cas, les États ont toléré, facilité ou encouragé le fait que des civils se livrent à 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 lorsqu'ils mènent des activités numériques dans le contexte d'un conflit armé ou en lien avec un tel conflit.

Les États et les parties aux conflits armés sont responsables des violations du DIH commises par des civils, notamment des hackers ou des employés d'entreprises technologiques, dont les activités numériques menées dans un conflit armé leur sont imputables. Les États doivent agir avec la diligence requise pour prévenir les violations du DIH commises par des civils sur leur territoire ou sous leur juridiction ou leur contrôle par le biais d'activités numériques ou facilitées par celles-ci et, si elles se produisent, les faire cesser, conformément aux obligations qui leur incombent en vertu du DIH. Les États s'engagent à faire connaître le DIH auprès des civils dans leurs pays respectifs. Ils ne doivent pas encourager ou aider des civils à violer le DIH, y compris par le biais d'activités numériques.

Dans certaines circonstances bien précises, la participation de civils à des activités numériques peut constituer une participation directe aux hostilités, ce qui fait perdre aux civils la protection dont ils bénéficient contre les attaques, mais uniquement tant que leur implication équivaut à une participation directe. En cas de doute, le DIH exige qu'un individu soit considéré comme étant protégé 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.

Pour réduire au minimum les risques liés à la participation de civils aux activités numériques dans les conflits armés, il est essentiel que les États et les parties au conflit armé s'emploient à :

a) prendre des mesures concrètes pour informer les civils pouvant être amenés à participer à des activités numériques dans le cadre d'un conflit armé ou en lien avec celui-ci des risques juridiques et pratiques qu'ils encourent de ce fait. Pour ce faire, ils peuvent échanger des informations sur les règles du DIH à travers les réseaux sociaux, des applications dédiées, la radio ou d'autres moyens de communication de masse, ou élaborer des modèles de codes de conduite conforme au DIH que les civils menant des activités numériques devraient suivre ;

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 résultant 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 les enfants prennent part aux hostilités par le biais d'activités numériques, par exemple en proposant des programmes d'enseignement et de sensibilisation destinés aux enfants et à ceux 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 les faisant appliquer ; enfin, en fixant un âge minimum pour l'accès aux outils numériques pouvant constituer 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 entreprises technologiques sont de plus en plus nombreuses à fournir des produits et services de cybersécurité ou d'autres produits et services numériques aux parties à un conflit armé. Dans ces situations, les civils et les biens de caractère civil qui dépendent de ces produits et services ou qui y sont associés peuvent être exposés à des dangers.

Parallèlement, 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 dans les conflits armés. C'est pourquoi leur interruption, leur dégradation ou leur emploi abusif peuvent avoir des conséquences humanitaires importantes. Ces produits et services numériques civils, ainsi que le personnel civil qui les fournit, sont protégés en vertu du DIH.

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

a) être conscientes que la fourniture de produits et de services numériques aux parties à un conflit armé comporte à la fois des risques juridiques et pratiques ;

b) comprendre et évaluer les risques de dommages causés aux civils et aux biens de caractère civil et prendre des mesures pour les réduire au minimum, qu'il s'agisse du personnel ou des biens appartenant à ces entreprises, ou du fait de leur proximité physique, de leur connexion numérique ou de leur dépendance vis-à-vis des infrastructures ou des services visés. Cela inclut, dans la mesure du possible, de 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 participer à des violations du DIH, de les faciliter ou de s'en rendre complice, y compris en fournissant des produits ou des services numériques aux parties à un conflit armé, et prendre les mesures appropriées si de tels actes devaient néanmoins être commis.

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

Le secteur de la santé et les organisations humanitaires impartiales sont particulièrement vulnérables aux activités numériques menées dans les conflits armés. Du fait de la dépendance croissante des services médicaux et des activités humanitaires à l'égard 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 et de leur personnel, et compromettre la fourniture d'une aide essentielle.

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, conformément au DIH, y compris contre les dommages découlant des 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, leurs systèmes informatiques et de communication.

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

Les parties à un conflit armé doivent par ailleurs prendre toutes les mesures pratiquement possibles, dans les circonstances qui prévalent et compte tenu des ressources disponibles, pour protéger les services médicaux et les activités humanitaires contre tout dommage, y compris ceux causés par des activités numériques menées par des tiers tels que des cybercriminels et d'autres acteurs non étatiques et non imputables à une partie à un conflit armé.

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 lors d'activités numériques menées dans les conflits armés. Cette protection inclut leurs données et les infrastructures numériques indispensables à leur fonctionnement.

Les activités numériques peuvent être utilisées pour commettre ou faciliter des actes de violence sexuelle ou pour enrôler ou utiliser des enfants dans les hostilités. 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.

Pour assurer la protection des services médicaux, des activités humanitaires et des autres personnes, biens ou activités spécialement protégés contre les dommages découlant des activités numériques menées dans les conflits armés, il est essentiel que les États et les parties aux conflits armés s'emploient à :

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 leur engagement à respecter et protéger les services médicaux et les activités humanitaires, y compris les données, les systèmes informatiques et de communication de ces services et activités, et à faciliter leurs opérations dans l'environnement numérique, ainsi qu'à respecter la protection spéciale des 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) dans la mesure du possible, soutenir et faciliter 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 de politique générale nationaux pertinents qui traitent des comportements en ligne pouvant constituer ou faciliter des violations du DIH relatives 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 ;

e) intégrer des normes spécifiques dans la doctrine militaire, les procédures opérationnelles normalisées et les règles d'engagement afin de prévenir et faire cesser les violations commises

ou facilitées dans le cadre d'activités numériques, notamment la violence sexuelle ainsi que l'enrôlement et l'utilisation d'enfants dans les hostilités. Les mesures possibles consistent à réglementer l'emploi de dispositifs numériques personnels dans des contextes opérationnels, limiter la mise en commun d'images ou d'informations sensibles, interdire l'utilisation de technologies numériques pour enrôler ou impliquer des enfants dans les hostilités, et sensibiliser les enfants et les personnes qui prennent soin d'eux aux risques associés.

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 diffuser 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 accroître fortement la vitesse, l'ampleur et la portée des informations préjudiciables.

Les États doivent s'abstenir de propager des informations en violation du DIH et prendre toutes les mesures pratiquement possibles pour éviter que cela se produise, y compris par le biais des technologies numériques. Cela comprend la diffusion 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 dans la population civile.

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

Pour remédier au problème de la diffusion d'informations en violation du DIH, il est essentiel que les États et les parties au conflit armé s'emploient à :

a) prendre toutes les mesures pratiquement possibles pour évaluer, prévenir et atténuer le risque que les opérations d'information nuisent 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 des informations qui déshumanisent l'adversaire ou propagent la haine envers la population civile, y compris par le biais de technologies numériques, et prendre les mesures appropriées pour s'assurer que leurs forces armées, les autres autorités publiques ou les personnes agissant en leur nom ne se livrent pas à ces pratiques ;

c) aider, dans la mesure du possible, les prestataires de services médicaux et les organisations humanitaires impartiales à se doter des capacités permettant d'améliorer la résilience face à la désinformation et aux autres activités d'information préjudiciables, notamment en renforçant leur capacité à recueillir, vérifier et diffuser des informations correctes ; 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 les zones où se déroulent les opérations ;

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. Cela peut consister à mettre en place les cadres juridiques et de politique générale appropriés et promouvoir l'adoption par les entreprises technologiques de mesures de protection et de pratiques permettant de détecter, d'évaluer et de traiter les informations préjudiciables dans les situations de conflit armé ;

e) renforcer la résilience de la société face aux activités 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 attendu que ces mesures risqueraient de porter préjudice à la population civile. Lorsque des restrictions sont justifiées par une nécessité militaire impérieuse, prendre des mesures d'atténuation pour limiter le plus possible les effets néfastes sur les civils.

7. Mesures transversales pour renforcer la mise en œuvre du DIH en rapport avec les activités numériques

Il est essentiel que les États, dans le cadre de la mise en œuvre de leurs obligations au titre du DIH en rapport avec les activités numériques, s'emploient, y compris en prenant des mesures d'application en temps de paix, à :

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

b) mettre des conseillers juridiques qualifiés à la disposition des unités et commandements militaires en charge 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 constituant de nouvelles armes ou de nouveaux moyens ou méthodes de guerre, notamment en testant, évaluant, vérifiant et validant rigoureusement ces capacités, 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 de faire cesser les violations du DIH commises par le biais d'activités numériques ou facilitées par celles-ci, par des personnes ou sur un territoire placé sous leur juridiction ou leur contrôle ;

e) prendre toutes les mesures pratiquement possibles pour prévenir ou limiter la prolifération, la réaffectation ou l'utilisation abusive des outils et capacités numériques lorsqu'il y a un risque clair qu'ils contribuent à des violations du DIH ;

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 et d'autres dispositions d'ordre pratique pour réduire les risques et, s'il y a lieu, le signalement volontaire d'incidents numériques importants ayant incidemment causé des dommages civils, afin d'améliorer la compréhension collective et l'atténuation des risques ;

g) favoriser la transparence et la compréhension commune en élaborant et en diffusant publiquement les positions nationales sur les modalités d'application du droit international, y compris le DIH, aux activités numériques, ainsi qu'en échangeant les enseignements tirés et les pratiques recommandées visant à réduire au minimum les dommages civils ;

h) appuyer le renforcement des capacités aux niveaux bilatéral, régional et mondial afin de renforcer la capacité des États à mettre en œuvre et à appliquer le DIH aux 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 d'ordre pratique adaptées au contexte ;

j) encourager la coopération entre les entreprises technologiques et les organisations humanitaires impartiales afin d'améliorer la préparation et la riposte face aux menaces numériques touchant les personnes et les biens protégés, notamment par l'échange d'informations et l'appui à la 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 dans les cadres nationaux et la pratique opérationnelle afin de renforcer la mise en œuvre du DIH, notamment pour recenser les risques numériques et y faire face.