Humanity In War

Dans le cadre de l'Initiative mondiale visant à revitaliser l'engagement politique en faveur du droit international humanitaire (Initiative mondiale en faveur du DIH), **le Ghana, le Luxembourg, le Mexique, la Suisse et le Comité international de la Croix-Rouge (CICR)** ont le plaisir d'annoncer la tenue de l'événement suivant :

GROUPE DE TRAVAIL 6

TROISIÈME CONSULTATION AVEC LES ÉTATS SUR LE THÈME « VEILLER À CE QUE LES TECHNOLOGIES NUMÉRIQUES SOIENT UTILISÉES D'UNE MANIÈRE CONFORME AU DIH DANS LES CONFLITS ARMÉS »

À l'intention des responsables gouvernementaux spécialisés dans le DIH, la cybersécurité ou les cyberopérations militaires en poste dans les capitales, ainsi que des représentants des missions permanentes à Genève

LUNDI 16 FÉVRIER 2026

DE 10H À 14H (UTC+1)

FORMAT : EN PRÉSENTIEL (À GENÈVE) ET EN LIGNE (SUR ZOOM)

Contexte

L'utilisation croissante des technologies numériques dans les conflits armés pose d'importantes questions humanitaires et juridiques. S'il est généralement 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.

Œuvrant dans le cadre de l'Initiative mondiale en faveur du DIH, le groupe de travail sur le numérique prend appui sur les discussions mondiales autour de l'utilisation des technologies numériques, ainsi que sur les progrès réalisés à ce jour, notamment les rapports du Groupe de travail des Nations Unies à composition non limitée sur la sécurité du numérique et de son utilisation et ceux 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, les positions nationales et communes sur le cyberdroit et le droit international, ainsi que la résolution 2 de la XXXIVe Conférence internationale de la Croix-Rouge et du Croissant-Rouge, 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 ». Il vient compléter les discussions multilatérales, y compris celles du futur Mécanisme mondial concernant les progrès du numérique dans le contexte de la sécurité internationale et la promotion d'un comportement responsable des États en matière d'utilisation du numérique. Ce groupe de travail s'inscrit dans le cadre des efforts actuellement déployés pour parvenir à une compréhension commune des limites que le DIH impose aux activités numériques dans les conflits armés en vue de protéger les civils.

Tenues respectivement le 15 mai et le 24 novembre 2025, les première et deuxième consultations avec les États du groupe sur le numérique ont reconnu les graves conséquences humaines que peut générer l'utilisation des technologies numériques dans les conflits armés et a souligné la nécessité impérative de protéger les personnes et de préserver la dignité humaine. Elles ont réaffirmé que le DIH reste le cadre juridique fondamental pour la protection des civils et des autres personnes et biens protégés contre les dangers résultant de l'utilisation des technologies numériques dans les conflits armés internationaux et non internationaux.

Lors de ces deux consultations, les participants ont examiné les conséquences humanitaires et juridiques de l'utilisation des technologies numériques dans les conflits armés et envisagé des mesures pratiques pour garantir le respect du DIH et renforcer la protection des civils dans ce contexte.

La troisième consultation prendra appui sur ces discussions et sur les principales observations formulées à cette occasion, s'attachant à faire progresser la compréhension commune des moyens de veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés en vue de protéger les populations civiles.

Objectifs

La troisième consultation visera les objectifs suivants :

- **Consolider la prise de conscience émergente** de la manière dont les principes et les règles du DIH protègent les civils, ainsi que les autres personnes et biens protégés, des dangers résultant des activités numériques menées dans les conflits armés. Si les États ont largement réaffirmé la nécessité de faire respecter et de renforcer ces protections, certaines questions nécessitent un examen plus approfondi afin de favoriser une vision commune. Conformes à l'objectif de

protection de la population civile à l'ère du numérique que poursuit le groupe de travail, les principales observations formulées par les coprésidents et le CICR pourront servir de base pour guider la discussion, recueillir d'autres avis et aider à évaluer les dispositifs permettant de parvenir à une compréhension commune des limites que le DIH impose à l'utilisation des technologies numériques dans les conflits armés.

- **Recueillir les points de vue et les pratiques des États** sur les mesures juridiques, opérationnelles et politiques qu'ils ont prises ou envisagé de prendre pour veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés, notamment par le biais de la législation, de la pratique militaire, de la diffusion du DIH, du dialogue avec le secteur technologique et des mesures visant à prévenir et faire cesser les violations du DIH.
- **Identifier les domaines nécessitant une réflexion et un dialogue plus approfondis**, en vue de la formulation des projets de recommandations à soumettre aux États, avant de les inclure dans les résultats globaux de l'Initiative mondiale en faveur du DIH.

Prochaines étapes

À la suite des trois premières séries de consultations, les États assurant la coprésidence du groupe de travail ainsi que le CICR formuleront des recommandations concrètes, qui seront présentées à l'ensemble des États pour un examen plus approfondi :

- Le **1er avril 2026**, une première version des recommandations de chaque groupe de travail sera envoyée à toutes les missions permanentes à Genève et publiée sur le site web L'humanité dans la guerre.
- La **quatrième série de consultations** se tiendra **du 4 au 6 mai 2026**, dans un **format hybride**. Au cours de ces rencontres, tous les États seront invités à faire part de leurs commentaires sur la première version des recommandations. La discussion se déroulera dans l'ordre des groupes de travail.
- Le **1er juin 2026**, une deuxième version des recommandations de chaque groupe de travail sera envoyée à tous les États et publiée sur le site web L'humanité dans la guerre.
- La **cinquième série de consultations** se tiendra **du 22 au 26 juin 2026**, dans un **format hybride**. Tous les États seront invités à faire part de leurs commentaires finaux sur les recommandations. À l'issue de ces consultations, les coprésidents et le CICR finaliseront les recommandations de chaque groupe de travail, en vue de les présenter à l'ensemble des États au cours du second semestre de 2026.

Participants

- La consultation se tiendra dans un format hybride permettant la participation en présentiel ou en ligne.
- La consultation sera **ouverte à tous les États intéressés**. Le choix des participants devrait se porter de préférence sur des responsables gouvernementaux spécialisés dans le DIH, la cybersécurité ou les cyberopérations militaires en poste dans les capitales, ainsi que sur des représentants des missions permanentes à Genève.
- D'autres représentants disposant d'une expertise spécifique dans le domaine concerné (p. ex. membres d'organisations internationales, de la société civile, des milieux

universitaires ainsi que des représentants du secteur technologique) pourront également participer à la consultation, sur invitation.

- Les inscriptions pourront se faire jusqu'au **vendredi 13 février 2026** inclus, au moyen du formulaire prévu à cet effet.

Modalités d'organisation

- Les langues de travail seront **l'anglais, l'arabe, le chinois, l'espagnol, le français et le russe.** Des services d'interprétation simultanée seront fournis.
- Nous prions les participants de bien vouloir limiter la durée de leurs interventions à **quatre minutes**, afin que chacun ait la possibilité de s'exprimer. Au terme de la consultation, et une fois que tous les participants souhaitant s'exprimer auront pu le faire, les États et les autres participants auront l'occasion de débattre des idées proposées par d'autres intervenants.
- Pour préparer leurs interventions, les participants sont priés de se reporter aux **principales observations formulées par les coprésidents du groupe de travail et par le CICR pour veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés** ainsi qu'aux **questions-guides** présentées dans l'ordre du jour ci-après. Le document de référence du groupe de travail peut également être consulté pour délimiter plus précisément la portée de la discussion.
- Étant donné les difficultés techniques inhérentes aux réunions hybrides, nous encourageons les délégations présentes dans la salle à faire leurs déclarations en personne et, dans tous les cas, à accorder toute leur attention aux délégations prenant la parole à distance.
- Tout au long de la consultation, les discussions devront rester **inclusives, constructives, non politisées et orientées vers la recherche de solutions**. Si, lors des consultations, les participants sont encouragés à faire part de la pratique en vigueur dans leur pays, ils sont priés de s'abstenir d'évoquer des situations spécifiques ou la pratique d'autres États.
- Afin de faciliter le travail des interprètes, nous invitons les participants à transmettre le texte de leurs déclarations d'ici au vendredi **13 février 2026**, par courrier électronique à l'adresse ihlinitiative@icrc.org, avec en objet la mention « Troisième consultation du groupe de travail sur le numérique ». Nous encourageons également les participants à envoyer le texte intégral de leurs déclarations par courrier électronique à l'issue de la réunion. **Sauf demande expresse de confidentialité, ces déclarations seront publiées sur le site L'humanité dans la guerre.**
- La consultation sera enregistrée, mais l'enregistrement ne sera pas rendu public.

Ordre du jour

Veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés (groupe de travail sur le numérique) Troisième série de consultations

16 février 2026, de 10h à 14h
Humanitarium (CICR), 17 avenue de la Paix, 1202 Genève

** Les horaires indiqués ci-dessous sont sujets à modification en fonction du nombre de déclarations.*

Enregistrement et café / Login et connexion	9h30-10h00
Ouverture de la réunion et introduction	10h00-10h10
Séance 1 – Principales observations formulées par les coprésidents du groupe de travail et le CICR pour veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés	10h10-12h00
Principales observations Reconnaissant le coût humain des activités numériques menées dans les conflits armés ainsi que les dommages et perturbations qu'elles peuvent causer aux sociétés, et soulignant la nécessité impérative de protéger les populations civiles et de préserver la dignité humaine, il faut absolument veiller à ce que les technologies numériques soient utilisées de manière conforme au DIH dans les conflits armés et renforcer le respect du DIH. Les États et les parties à un conflit armé prendront des mesures pratiques, individuelles ou collectives, pour atténuer les risques encourus par la population civile et faire en sorte que les activités numériques menées dans le contexte du conflit en question ne portent pas atteinte aux protections conférées par le DIH. **Protéger la population civile, les personnes civiles et les biens de caractère civil contre les dangers résultant des activités numériques menées dans les conflits armés** Dans la conduite d'activités numériques liées à 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 une personne, ou qu'elles endommagent ou détruisent un bien, y compris en le mettant hors d'usage, constituent des attaques au sens du DIH et doivent être menées conformément à l'ensemble des règles et principes du DIH sur la conduite des hostilités, notamment l'interdiction de lancer des attaques directes contre des civils et des biens à caractère civil, des attaques indiscriminées ou disproportionnées, ainsi que l'obligation de prendre toutes les précautions pratiquement possibles en vue d'éviter ou au moins de réduire au minimum les dommages causés incidemment aux civils. 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, l'obligation de constamment veiller à épargner la population civile, les personnes civiles et les biens de caractère civil dans la conduite des opérations militaires, et les règles protégeant les biens contre la saisie et la destruction, offrent une protection supplémentaire contre les dangers découlant des activités numériques. **Protection des données**	

Les données sont au cœur de la transformation numérique mondiale et indispensables au fonctionnement des services civils essentiels. La manière dont les données sont traitées pendant les conflits armés a une incidence sur la vie des personnes et leur dignité. En vertu du DIH, les données sont protégées par :

- les principes et règles régissant la conduite des hostilités, notamment la distinction qui exige que les opérations militaires ne visent que les données constituant un objectif militaire et interdit les attaques touchant sans distinction des données civiles et militaires, ainsi que les principes et règles de proportionnalité et de précaution,
- 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,
- 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, et
- 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.

Infrastructures numériques civiles utilisées à des fins militaires

Les États et les parties à un conflit armé doivent avoir conscience du risque de dommages civils découlant de l'utilisation à des fins militaires des infrastructures numériques civiles dans les conflits armés et s'efforcer de réduire ce risque.

Lorsque cette utilisation transforme une infrastructure numérique civile, ou des parties de celle-ci, en objectif militaire, toute attaque menée contre cet objectif militaire demeure soumise aux interdictions relatives aux attaques indiscriminées ou disproportionnées, ainsi qu'à l'obligation de prendre toutes les précautions pratiquement possibles.

L'évaluation de la licéité de telles opérations doit prendre en compte tous les effets directs et indirects prévisibles qui pourraient être causés incidemment à des personnes civiles et des biens de caractère civil, y compris à l'utilisation civile des infrastructures numériques. Toutes les précautions pratiquement possibles doivent être prises pour épargner la population civile et les services civils essentiels qui dépendent des infrastructures numériques. Toutes les précautions pratiquement possibles doivent être prises quant au choix des moyens et méthodes de guerre en vue d'éviter et, en tout cas, de réduire au minimum les pertes en vies humaines dans la population civile, les blessures aux personnes civiles et les dommages aux biens de caractère civil qui pourraient être causés incidemment. Cela implique notamment de ne viser que les éléments ou fonctions des infrastructures numériques utilisés à des fins militaires en épargnant ceux qui sont destinés à un usage civil.

Les États et les parties à un conflit armé doivent, dans toute la mesure du possible, prendre toutes les précautions nécessaires pour protéger la population civile et les biens de caractère civil placés sous leur contrôle contre les dangers résultant des opérations militaires. Cela inclut, si les circonstances le permettent, de séparer physiquement ou techniquement les éléments des infrastructures numériques qui sont utilisés à des fins militaires de ceux destinés à un usage civil.

La participation de civils aux activités numériques dans les conflits armés

Les civils, notamment les hackers et les employés d'entreprises technologiques, sont tenus de respecter le DIH lorsqu'ils opèrent dans le contexte d'un conflit armé ou en lien avec un tel conflit.

Les États doivent veiller au respect du DIH par les civils dont les activités numériques menées dans un conflit armé leur sont imputables, faire connaître le DIH aux civils sur lesquels ils exercent une autorité, y compris les hackers et les employés d'entreprises technologiques, et prendre les mesures nécessaires pour les informer des risques juridiques et pratiques associés à la conduite d'activités numériques dans le contexte d'un conflit armé. Les États doivent agir avec la diligence requise pour prévenir les violations du DIH commises par des civils par le biais d'activités numériques ou facilitées par celles-ci et, si elles se produisent, les faire cesser. Ils ne doivent pas encourager ou aider des civils à violer le DIH, y compris par le biais d'activités numériques.

Les États et les parties à un conflit armé doivent 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 civils en question doivent, dans la mesure du possible, être intégrés dans les forces armées. Les enfants ne doivent pas être autorisés à prendre part aux hostilités.

Produits et services fournis par les entreprises technologiques dans les conflits armés

Les entreprises technologiques fournissent toute une gamme de produits et de services numériques civils dont dépendent la population civile, les gouvernements et les organisations humanitaires, notamment dans les conflits armés, et ces biens de caractère civil, de même que les employés civils qui fournissent ces services numériques, sont protégés par le DIH.

Les entreprises technologiques doivent 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. Elles doivent comprendre et évaluer les risques de dommages causés aux civils et aux biens de caractère civil et s'efforcer de les réduire au minimum, qu'ils émanent de membres du personnel ou de biens appartenant à ces entreprises, ou de leur proximité physique, de leur connexion numérique ou de leur dépendance vis-à-vis de l'infrastructure ou des services visés. Cela inclut, dans la mesure du possible, de séparer physiquement ou techniquement les services et produits utilisés pour soutenir les opérations militaires de ceux qui sont destinés à un usage civil.

Les entreprises technologiques doivent prendre des mesures pour empêcher leur personnel de participer à des violations du DIH ou s'en rendre complice, y compris en fournissant des produits ou des services numériques aux parties à un conflit armé, tout comme elles doivent prendre les mesures appropriées si de tels actes devaient néanmoins être commis.

Questions-guides pour la discussion

1. Avez-vous des commentaires à formuler concernant les principales observations exposées ci-dessus ? Certaines questions nécessitent-elles un débat plus approfondi ?
2. Y a-t-il d'autres éléments ou mesures de protection qui devraient être pris en compte pour mieux protéger les civils, ainsi que les autres personnes et biens protégés, contre les dangers résultant des activités numériques menées dans les conflits armés ?

Pause	12h00-12h30

Séance 2 – Principales observations formulées par les coprésidents du groupe de travail et le CICR pour veiller à ce que les technologies numériques soient utilisées d'une manière conforme au DIH dans les conflits armés (suite)	12h30-13h55
Principales observations **Protéger les services médicaux, les activités humanitaires et les autres personnes, biens et activités spécialement protégés** 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 effets 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 comme l'exige le DIH. Cette protection est essentielle pour préserver la confiance dans le travail des services médicaux et des organisations humanitaires impartiales. Les États et les parties à un conflit armé doivent par ailleurs prendre toutes les mesures pratiquement possibles 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. Dans l'environnement numérique, tout comme dans le monde physique, il est important que la protection spécifique que confère le DIH aux services médicaux et aux activités humanitaires soit clairement identifiable et visible, afin qu'elle puisse être respectée. Un des moyens permettant de signaler cette protection serait un « emblème numérique », en cours d'élaboration. Les États et les autres parties prenantes concernées sont encouragées à continuer de dialoguer avec le CICR pour explorer les voies juridiques, techniques et diplomatiques conduisant à la mise en œuvre de cet emblème. La protection spécifique accordée aux biens indispensables à la survie de la population civile, aux ouvrages et installations contenant des forces dangereuses, aux biens culturels et à la protection civile doit être respectée, y compris dans la conduite d'opérations numériques dans les conflits armés. Cela comprend aussi bien les données que les infrastructures numériques indispensables à leur fonctionnement. Le DIH interdit la violence sexuelle et l'enrôlement ou l'utilisation d'enfants dans les hostilités, y compris quand ces actes sont commis dans le cadre d'activités numériques ou encouragés ou facilités par ces activités. **Propagation d'informations en violation du DIH** Les États doivent s'abstenir d'utiliser les technologies numériques pour propager des informations en violation du DIH et prendre toutes les mesures pratiquement possibles pour éviter que cela se produise. 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 États et les parties à un conflit armé ne doivent pas diffuser des informations qui déshumanisent l'adversaire ou propagent la haine envers la population civile, y compris par le biais de technologies numériques. 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.	

Mesures visant à garantir le respect du DIH

Les États doivent adopter des mesures nationales visant à garantir que les technologies numériques sont utilisées d'une manière conforme au DIH dans les conflits armés. Cela comprend la diffusion des 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, ainsi que l'intégration des principes et règles du DIH et de leur application aux activités numériques dans la législation nationale, la doctrine militaire, les procédures opérationnelles, les règles d'engagement et la formation, selon que de besoin. Des conseils juridiques spécialisés devraient être fournis, le cas échéant, aux unités et commandements militaires en charge des activités numériques. Conformément aux obligations qui incombent aux États en vertu du droit international, il convient de déterminer, dans l'étude, la mise au point, l'acquisition ou l'adoption de capacités numériques fonctionnant comme une nouvelle arme, un nouveau moyen ou une nouvelle méthode de guerre, si leur emploi serait interdit, dans certaines circonstances ou en toutes circonstances, par le droit international.

Intégrer des approches tenant compte de l'âge et du genre dans les cadres nationaux contribue au respect des obligations inscrites dans le DIH, notamment pour faire face aux risques numériques.

Pour protéger les civils et les autres personnes protégées contre la diffusion d'informations en violation du DIH, le dialogue avec les acteurs pertinents, notamment le secteur technologique, peut favoriser le respect du droit applicable. Cela inclut d'encourager les entreprises technologiques à adopter des mesures de protection et des pratiques qui réduisent 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.

Il est essentiel que chaque État adopte toutes les mesures nécessaires, qu'elles soient législatives, réglementaires ou autres, et prenne, 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 sa juridiction ou son contrôle.

On pourra renforcer encore la transparence, la confiance et une compréhension commune en élaborant et en diffusant publiquement les opinions et positions nationales sur les modalités d'application du droit international, y compris le DIH, à l'utilisation des technologies numériques, et en échangeant les enseignements tirés et les pratiques recommandées visant à réduire au minimum le risque de dommages causés aux civils par des activités numériques. Dans la mesure du possible, des efforts seront déployés pour 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 scrupuleusement le DIH aux activités numériques.

Questions-guides pour la discussion

1. Avez-vous des commentaires à formuler concernant les principales observations exposées ci-dessus ? Certaines questions nécessitent-elles un débat plus approfondi ?
2. Y a-t-il d'autres éléments ou mesures de protection qui devraient être pris en compte pour mieux protéger les civils, ainsi que les autres personnes et biens protégés, contre les dangers résultant des activités numériques menées dans les conflits armés ?

Observations finales	13h55-14h00