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 de vous annoncer la tenue de l'événement suivant :

GROUPE DE TRAVAIL 6

DEUXIÈME 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 24 NOVEMBRE 2025
DE 9H À 18H (UTC +1)

FORMAT : EN PRÉSENTIEL (À L'HUMANITARIUM DU CICR 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.

Créé 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, en particulier la résolution 2 de la XXXIV[e] 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 ». 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.

La première consultation organisée par ce groupe de travail s'est tenue le 15 mai 2025. Elle s'est attachée à identifier les enjeux et les préoccupations juridiques et humanitaires découlant des caractéristiques uniques des activités numériques menées dans les conflits armés. Elle a aussi examiné la manière dont ces questions devraient être traitées afin de maintenir la protection que le DIH accorde aux civils et aux biens de caractère civil, ainsi qu'aux autres personnes et biens protégés dans les conflits armés. La deuxième consultation, qui fait l'objet du présent document, fera avancer cette discussion. Elle se tiendra à Genève dans un format hybride, le 24 novembre 2025.

Pour plus de précisions sur les questions abordées au sein de ce groupe de travail, les participants sont invités à consulter le **document de référence** joint à la présente note de synthèse.

Objectifs

La deuxième consultation prendra appui sur les discussions tenues lors de la première consultation ainsi que sur les points essentiels à retenir de cette dernière. Elle s'attachera à approfondir le débat sur les questions juridiques et humanitaires découlant de l'utilisation des technologies numériques dans les conflits armés. La consultation visera à promouvoir une vision commune ainsi qu'à dégager des pistes de recommandations juridiques et pratiques permettant de mieux protéger la population civile et les biens de caractère civil dans les conflits numérisés.

La consultation visera les objectifs suivants :

- **Faire le point sur les progrès accomplis par le groupe de travail, notamment** :
    - informer les participants des conclusions de la première consultation, compilées dans le rapport intérimaire, ainsi que des enseignements tirés des événements connexes qui ont eu lieu ultérieurement ;
    - présenter les prochaines étapes en vue de l'élaboration des recommandations finales du groupe de travail.

- **Approfondir la discussion autour des enjeux juridiques et humanitaires identifiés afin de parvenir à une vision commune de ces enjeux. En particulier :**
    - faciliter des échanges approfondis sur les questions identifiées lors de la première consultation comme nécessitant un examen plus détaillé, telles que :
        - les implications, du point de vue du DIH, des opérations numériques qui ne causent pas de dommages physiques, comme la mise hors d'état de fonctionner du système pris pour cible ;
        - la protection que confère le DIH aux données civiles et autres contre, par exemple, l'altération, l'endommagement ou la suppression, ou contre leur extraction et leur publication ;
        - la protection spécifique que confère le DIH à certaines catégories de personnes, de biens et d'activités contre les effets des activités numériques menées dans les conflits armés, y compris leurs données et leurs infrastructures numériques ;
        - les limites imposées par le DIH en matière de diffusion d'informations dans le cadre d'activités numériques ;
        - les implications, du point de vue du DIH, de l'utilisation à des fins militaires d'infrastructures numériques civiles et de la participation de civils aux activités numériques menées dans les conflits armés, ainsi que les mesures fondées sur le DIH à même d'atténuer les risques associés de dommages causés aux civils et aux services civils essentiels ;
    - renforcer les mesures concrètes visant à assurer le respect du DIH et à réduire les dommages civils.

Prochaines étapes

Une troisième consultation avec les États est prévue début 2026 en vue de faire progresser les discussions menées lors des deux premières consultations et de parvenir à une compréhension commune des thèmes abordés. Ces consultations prépareront le terrain pour l'élaboration des recommandations du groupe de travail. Tous les États intéressés seront invités à formuler leurs commentaires sur les recommandations du groupe de travail au deuxième trimestre de 2026. Ces recommandations seront ensuite débattues plus avant par les États lors de nouvelles consultations.

Les consultations avec les États seront complétées par des discussions régionales et d'autres événements connexes, qui seront annoncés sur le site web L'humanité dans la guerre.

Participants

- La consultation se déroulera principalement en présentiel, à Genève. Il sera également possible de participer en ligne.
- La consultation est **ouverte à tous les États intéressés**. Pour ce qui est des participants, le choix 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 et des milieux universitaires) pourront également participer à la consultation, sur invitation.
- Les inscriptions sont ouvertes jusqu'au 15 novembre 2025 inclus, à l'adresse https://forms.office.com/e/LuDKik93vY.

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 États de bien vouloir limiter la durée de leurs interventions à **quatre minutes**, afin que tous les participants aient la possibilité de s'exprimer. Au terme de chaque séance, 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 **questions-guides** présentées dans l'ordre du jour ci-après. Certaines questions-guides s'accompagnent d'**exemples de scénarios** qu'il convient de lire avec les questions. Un **document de référence** actualisé est joint à la présente note de synthèse afin d'encadrer et de faciliter les discussions.
- 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 21 novembre 2025, par courrier électronique à l'adresse ihlinitiative@icrc.org, avec en objet la mention « Deuxième 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)
Deuxième série de consultations

24 novembre 2025, de 9h à 18h
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	8h30-9h00
Ouverture de la réunion et introduction	9h00-9h30
Débat d'experts : Principaux enjeux juridiques et humanitaires découlant de l'utilisation des technologies numériques dans les conflits armés	9h30-10h30
Séance 1 : Mesures pratiques visant à assurer le respect du DIH et à protéger les civils lors de l'utilisation de technologies numériques dans les conflits armés	10h30-11h30
Questions-guides 1. Quelles mesures juridiques et opérationnelles votre État a-t-il adoptées, ou envisage-t-il d'adopter, pour assurer le respect du DIH et éviter ou atténuer les dommages causés aux civils dans le cadre des activités numériques menées dans les conflits armés ? En quoi ces mesures – compte tenu des spécificités des opérations numériques – diffèrent-elles de celles qui s'appliquent aux opérations cinétiques, et comment ces spécificités peuvent-elles être prises en compte ? 2. Quelles mesures votre État prend-il, ou envisage-t-il de prendre, pour prévenir et faire cesser les violations du DIH commises par le biais d'activités numériques ou en lien avec celles-ci ? 3. Quelles formes de renforcement des capacités ou de coopération internationale seraient-elles le plus à même d'aider les États à faire mieux respecter le droit ainsi qu'à mettre en commun les mesures pratiques prises dans ce domaine ?	
Pause-café	11h30-12h00

Séance 2 : Protéger les civils, ainsi que les autres personnes et biens protégés, contre les dangers résultant des activités numériques menées dans les conflits armés	12h00-13h00
Questions-guides 1. Quels sont les coûts humains et les implications au regard du DIH des opérations numériques qui causent des dommages non physiques, tels que la mise hors d'état de fonctionner du système pris pour cible ? Prenons le cas d'une opération numérique menée dans le cadre d'un conflit armé contre un bien de caractère civil, par exemple le serveur d'un prestataire de services de transport, d'un prestataire de services internet ou d'une banque. Au moment de l'opération, ce serveur n'est pas utilisé d'une manière qui en fasse un objectif militaire. Suite à l'opération, le bien ciblé ne fournit plus le service qu'il fournit normalement ; cependant, il n'est pas physiquement endommagé. Comment votre État évalue-t-il la licéité de l'opération numérique menée ? Votre évaluation serait-elle différente si des dommages physiques avaient été causés par les effets directs ou indirects prévisibles de cette opération ? 2. Comment assurez-vous la protection, en vertu du DIH, des données civiles et autres contre, par exemple, l'altération, l'endommagement, la suppression ou l'extraction et la publication sans autorisation ? Votre État établit-il une distinction entre différentes catégories de données (médicales, biométriques, financières, etc.) lorsqu'il évalue leur protection en vertu du DIH ? Prenons le cas d'une opération numérique menée, dans le cadre d'un conflit armé, pour supprimer des données civiles (p. ex. données médicales, données de sécurité sociale, comptes bancaires, dossiers fiscaux ou données clients d'entreprises civiles). Comment votre État évalue-t-il la licéité d'opérations numériques de ce type ? Quelles règles du DIH limitent l'altération, l'endommagement ou la destruction de données civiles ou d'autres données protégées en période de conflit armé ? Quelle protection le DIH offre-t-il contre la copie non autorisée, la saisie et la publication potentielle de données civiles ou d'autres données protégées ? 3. Quelles règles du DIH protègent les civils et les biens de caractère civil contre les opérations numériques qui ne peuvent pas être qualifiées d'attaques au regard du DIH ? Par exemple, quelles mesures pratiques faut-il prendre, lorsque des activités numériques sont menées, pour mettre en œuvre l'obligation de veiller constamment à épargner la population civile, les personnes civiles et les biens de caractère civil dans la conduite d'opérations militaires ?	
Pause déjeuner (repas non fourni)	13h00-14h00
Séance 3 : Mettre en œuvre la protection spécifique accordée à certaines catégories de personnes, de biens et d'activités contre les effets de l'utilisation des technologies numériques dans les conflits armés	14h00-15h00
Questions-guides 1. Quelles mesures pratiques votre État prend-il, ou envisage-t-il de prendre, pour faire en sorte que les activités numériques menées dans les conflits armés n'endommagent pas ou ne perturbent pas le fonctionnement des services médicaux, des activités humanitaires ou des biens indispensables à la survie de la population civile, y compris leurs systèmes et leurs données numériques ?	

Et quelles précautions votre État prend-il, ou envisage-t-il de prendre, pour protéger les biens bénéficiant d'une protection spécifique contre les dommages, notamment ceux causés par le biais d'activités numériques ? 2. Concernant la protection spécifique accordée aux structures et personnels de santé, prenons le cas d'une opération numérique menée par une partie à un conflit armé dans le but d'accéder aux serveurs d'un établissement médical situé sur le territoire du camp adverse. La partie concernée collecte les données médicales des membres des forces armées qui sont soignés dans cet établissement, puis encrypte tous les dossiers des patients, les rendant inaccessibles au personnel médical. Dans quelle mesure la protection spécifique des établissements médicaux englobe-t-elle la confidentialité, l'intégrité et la disponibilité des données auxquelles ils accèdent et qu'ils collectent, traitent et conservent pour leurs opérations ? De même, comment cette protection s'applique-t-elle aux données auxquelles le personnel humanitaire a accès et qu'il collecte, traite et conserve, ainsi qu'aux biens que ce personnel utilise à des fins humanitaires ? 3. Quels risques particuliers les activités numériques engendrent-elles en ce qui concerne l'interdiction de la violence sexuelle et/ou l'enrôlement ou l'utilisation illicite d'enfants dans les hostilités ? Quelles mesures pratiques votre État a-t-il adoptées, ou envisage-t-il d'adopter, pour prévenir et gérer ces actes illicites ?	
Séance 4 : Protéger les civils, ainsi que les autres personnes protégées par le DIH, contre la propagation d'informations en violation du DIH dans les conflits armés	15h00-16h00
Questions-guides 1. Quelles limites le DIH impose-t-il à la diffusion d'informations par le biais d'activités numériques dans les conflits armés ? Prenons l'exemple d'une campagne d'information menée par une partie à un conflit armé, consistant à : • mettre en ligne des images de prisonniers de guerre montrant la façon dont ils sont traités ; • élaborer, puis diffuser sur les plateformes de médias sociaux, des messages qui attisent les tensions entre les communautés locales, accroissant ainsi le risque de violence. Quels garde-fous ou mécanismes de surveillance votre État a-t-il mis en place, ou envisagé de mettre en place, pour éviter que les activités numériques n'exposent les personnes privées de liberté à la curiosité publique ? Et comment votre État détermine-t-il si les opérations d'information facilitées par des technologies numériques constituent un acte interdit, par exemple le fait d'inciter ou d'encourager à commettre des violations du DIH, ou de répandre la terreur parmi la population civile ? 2. Comment votre État fait-il face au risque que la diffusion de fausses informations facilitée par des technologies numériques perturbe les services médicaux ou les opérations humanitaires menées dans les conflits armés ?	

Prenons le cas d'une campagne en ligne qui diffuse des images fabriquées et des publications mensongères sur les réseaux sociaux, prétendant qu'un hôpital est un bastion tenu par des combattants. Ces fausses informations exacerbent la méfiance au sein de la population locale et entravent l'accès du personnel médical ; de plus, les employés entrant dans l'hôpital font l'objet de provocations et d'intimidations croissantes. Quelles règles du DIH protègent les services médicaux et les opérations humanitaires contre la désinformation numérique ? Quelles mesures juridiques ou opérationnelles votre État a-t-il adoptées, ou envisage-t-il d'adopter, pour faire face à ces risques ? 3. Quelles autres mesures votre État a-t-il prises, ou envisage-t-il de prendre, pour empêcher que les technologies numériques soient utilisées, y compris dans les médias sociaux, pour diffuser des informations en violation du DIH ?	
Pause-café	16h00-16h30
Séance 5 : Faire face au risque de dommages résultant de l'utilisation à des fins militaires d'infrastructures numériques civiles ainsi que de la participation de civils aux activités numériques dans les conflits armés	16h30-17h30
Questions-guides 1. Quels sont les coûts humains et les implications au regard du DIH de l'utilisation d'infrastructures numériques civiles à des fins militaires ? Quelles mesures fondées sur le DIH faut-il prendre pour atténuer les risques de dommages causés aux civils et aux services civils essentiels qui découlent de cette utilisation ? Prenons l'exemple d'un centre de données commercial situé sur le territoire d'un État partie à un conflit armé, qui héberge des données et des applications militaires, mais aussi des données relatives aux populations civiles et des applications utilisées dans la fourniture de services civils essentiels. • Comment votre État applique-t-il les principes et les règles du DIH, tels que les principes de distinction, de proportionnalité et de précaution, lorsqu'il évalue la conduite d'une opération numérique contre cette infrastructure numérique ? Si une partie particulière de l'infrastructure numérique, telle qu'un serveur en nuage, devient un objectif militaire, comment faut-il prendre en compte, lors de la planification et de la conduite d'une opération numérique, les effets que celle-ci aura sur l'utilisation à des fins civiles de cette partie de l'infrastructure ? • Quelles mesures de précaution l'État menant l'opération numérique peut-il et devrait-il prendre pour protéger la population civile et les services civils essentiels qui dépendent de l'infrastructure numérique prise pour cible ? • Quelles précautions l'État hébergeant le centre de données peut-il et devrait-il prendre pour protéger la population civile et les biens de caractère civil se trouvant sous son contrôle des effets des opérations numériques menées contre le centre de données ? • Quelles précautions l'entreprise qui possède ou exploite le centre de données peut-elle et devrait-elle prendre pour éviter que les opérations numériques dirigées contre les données et les applications militaires portent atteinte aux données civiles hébergées dans les mêmes locaux ?	

2. En quoi les civils peuvent-ils être mis en danger par leur participation à des activités numériques menées dans les conflits armés, et quelles mesures fondées sur le DIH faut-il prendre pour atténuer les risques auxquels ils sont exposés ? Prenons le cas de hackers civils opérant sur le territoire de l'un des belligérants dans le cadre d'un conflit armé, qui mènent des opérations numériques visant à perturber les communications militaires ou à endommager l'infrastructure numérique d'entreprises privées, dans le but d'affaiblir l'économie de l'État ennemi et de saper le moral de sa population. • À quelles obligations juridiques, prévues par le DIH, les hackers civils doivent-ils se conformer lorsqu'ils mènent ce type d'opérations numériques ? • Quelles mesures l'État touché peut-il prendre face à ces opérations numériques ? 3. Quelles mesures pratiques votre État a-t-il prises, ou envisage-t-il de prendre, pour faire en sorte que les civils placés sous sa juridiction ou sous son contrôle – comme les hackers civils, les groupes de hackers ou les employés d'entreprises technologiques menant des activités numériques dans le cadre d'un conflit armé – connaissent et respectent le DIH, et qu'ils soient conscients des risques résultant de leurs actes et bénéficient d'une protection maximale contre ces risques ?	
Observations finales	17h30-18h00