Première consultation sur le respect du DIH dans l'utilisation des technologies de l'information et de la communication dans les conflits armés

Intervention de la France

15 juin

Session 1 : L'utilisation des TICs dans les conflits armés actuels et leur coût humain

Mesdames et Messieurs,

La France remercie le CICR et les Etats co-présidant ce groupe de travail – le Luxembourg, le Mexique et la Suisse – pour cette première consultation. Parmi tous les groupes de l'initiative mondiale pour le DIH, celui-ci est sans doute un de ceux qui a le plus grand potentiel pour faire progresser nos réflexions sur ce que signifie faire respecter le DIH au XXIe siècle, dans la continuité de l'importante résolution adoptée à l'unanimité lors de la 34e Conférence internationale du mouvement de la Croix-Rouge et du Croissant-Rouge.

Tout d'abord, il nous semble important de rappeler que la France reconnait la pleine applicabilité du droit international, en particulier du droit international humanitaire, au cyberespace et aux technologies de l'information et de la communication.

La France a établi dans plusieurs documents de doctrine les modalités de la mise en œuvre du DIH dans le cyberespace. D'abord, dans son rapport sur le Droit international appliqué aux opérations dans le cyberespace (2019) puis, dans le Manuel de droit des opérations militaires du Ministère des armés (2023).

Ensuite, il est indéniable que des attaques cyber peuvent violer le droit international humanitaire et avoir à ce titre des impacts sur civils et les personnels de santé et humanitaires qui se mobilisent à leur service. Nous estimons par ailleurs très important d'évoquer les conséquences déstabilisatrices de la désinformation et nous remercions les co-parrains d'avoir prévu une séquence à cet effet.

Dès lors, si le DIH s'applique pleinement au cyberespace, l'immédiateté de l'action dans ce milieu, l'hyper-connexion et l'interdépendance des réseaux nous oblige à une réflexion juridique poussée sur la manière dont ce corpus juridique doit se décliner.

En France, les moyens cyber ont été intégrés dans la manœuvre opérationnelle grâce à un processus de ciblage numérique spécifique, directement placé sous la responsabilité du chef d'état-major des armées. Il bénéficie alors du soutien d'experts et de conseillers juridiques opérationnels spécialisés. La mise en œuvre du DIH dans une cyber opération repose donc sur deux éléments :

- D'une part, une planification longue et spécifique à l'opération afin de recueillir toutes les informations nécessaires pour l'identification de la nature du système visé et donc ainsi, garantir le respect du principe de distinction.

- D’autre part, un choix du ou des moyens les plus adaptés pour conduire une opération dans le domaine cyber et ainsi limiter les dommages incidents aux personnes et biens protégés.

Je vous remercie.

Session 2: Protéger les civils et autres personnes et objets protégés des dangers resultant d’activités usant de TICs dans les conflits armés

Pour la France l’application des principes cardinaux du droit international humanitaire que sont la distinction, la proportionnalité et la précaution, aux activités usant des technologies de l'information et de la communication ne fait aucun doute.

De notre point de vue, les cyberopérations qui, sans créer de dommage physique, ont pour effet de rendre inopérants des systèmes, peuvent être qualifiées d'attaques au sens de l'article 49 du protocole additionnel I aux Convention de Genève. La France considère en effet qu’une cyberopération constitue une attaque dès lors que les équipements ou les systèmes visés ne rendent plus le service pour lesquels ils ont été mis en place. Et ce, que cela soit de manière temporaire ou définitive, réversible ou irréversible. Si les effets sont temporaires et/ou réversibles, l’attaque sera caractérisée dès lors qu’une intervention de l’adversaire est nécessaire pour rendre l’infrastructure ou le système de nouveau opérant.

Toutefois, conformément au principe de distinction, ces cyberopérations ne peuvent viser que des systèmes numériques qui auront pu être préalablement identifiés comme des objectifs militaires. Toute opération à l'encontre de systèmes qui ne seraient pas des objectifs militaires est illicite.

Par ailleurs, la France considère que les opérations menées dans le cyberespace doivent également prendre en compte la protection spéciale dont bénéficient certains biens au regard du DIH, tels que les unités sanitaires, les biens de secours humanitaires, les biens indispensables à la survie de la population civile, les installations contenant des forces dangereuses ou l'environnement naturel. Toute opération dirigée à l'encontre des services informatiques et équipements nécessaires au fonctionnement de ces entités doit faire l'objet d'une précaution renforcée. Nous devons réfléchir aux moyens de mieux protéger les systèmes numériques des biens spécialement protégés. La proposition du CICR de créer un emblème numérique est une piste intéressante. Nous devons poursuivre la réflexion sur les modalités techniques nécessaires à l’efficacité d’un tel emblème.

Enfin, concernant le statut des données, la position française est le résultat de deux types de considérations. D'une part, un constat de réalité, qui est de reconnaitre l’importance des données et la dépendance numérique actuelle. Et d'autre part, des considérations juridiques issues de la règle bien établie que tout bien qui n’est pas militaire doit être présumé comme étant civil.

Ainsi, nous considérons que les données de contenu comme les données bancaires ou médicales sont des biens protégés. La protection renforcée dont bénéficient certains biens

(comme les unités sanitaires ou les biens indispensables à la survie de la population) s'étend aux données nécessaires au fonctionnement des équipements et systèmes informatiques de ces derniers.

Je vous remercie.

Session 3 : Protéger les civils et autres personnes protégées contre la diffusion d'informations en violation du DIH pendant les conflits armés

Je voudrais ici traiter deux sujets.

Les images des conflits contemporains nous parviennent en nombre dans le monde connecté dans lequel nous vivons. Elles permettent de rendre compte des situations de conflits quasiment en temps réel pour certains. Ces images sont des sources de preuves et d'informations qui pourront s'avérer utiles pour l'établissement des responsabilités des auteurs de violations.

Toutefois, l'utilisation des nouvelles technologies de l'information et de la communication pose au moins deux questions dans les situations de conflits armés.

1/ D'abord, elle pose, avec une acuité nouvelle, la question de la diffusion d'images de personnes privées de liberté. L'utilisation croissante des TICs dans les conflits armés nécessite de réfléchir à la protection des personnes privées de liberté contre la curiosité publique.

En droit international humanitaire, alors que tout individu doit *a minima* être protégé contre les atteintes à sa dignité, la protection contre la curiosité publique qui est accordée aux prisonniers de guerre permet d'une part de préserver l'honneur et la dignité de ces individus, mais également de les protéger contre les risques de représailles.

A ce titre, la France soutient pleinement les commentaires de la troisième convention de Genève qui ont été réalisés en 2020 par le CICR et qui ont pleinement identifié cette problématique et y ont apporté des éclairages utiles.

2/ Ensuite, je veux évoquer la question de la désinformation. Le CICR et d'autres organisations humanitaires nous alertent sur la manière dont des fausses informations diffusées sur internet et les réseaux sociaux peuvent entraver leur capacité d'action sur le terrain et mettre en danger la vie de leurs personnels, par exemple en remettant en cause leur neutralité.

Tous les Etats ont un rôle à jouer pour contribuer à la défense de l'espace humanitaire et au respect des principes humanitaires. Les Etats doivent s'abstenir de toute attaque informationnelle contre les organisations humanitaires. Plus encore, ils doivent aider à les prévenir, en menant des actions de sensibilisation auprès de certains publics comme les journalistes par exemple. La France s'engage aussi, dans ses relations diplomatiques, pour attirer l'attention de ses partenaires sur l'importance du respect de la neutralité des acteurs humanitaires.

Je vous remercie.

Session 4: Le risque de préjudice découlant de l'utilisation militaire des infrastructures TIC civiles et de l'implication de civils dans les activités TIC pendant les conflits armés.

Je voudrais rappeler un point évoqué plus en détail dans le cadre du groupe de travail sur la protection des infrastructures civiles : en droit des conflits armés, en dehors des objectifs militaires par nature, les biens normalement affectés à un usage civil doivent être présumés comme tels et ne pas être pris pour cible. Cette présomption est levée au cas par cas, si et seulement si les deux conditions cumulatives de l'article 52§2 du PA I sont satisfaites.

La France l'a déjà souligné aux côtés d'autres États, les "biens duaux" n'existent pas juridiquement et il est essentiel de s'en tenir à l'approche binaire du DIH positif. Toutefois, l'expression de bien dual permet justement de souligner que si le bien est juridiquement un objectif militaire licite, il fournit un service ou demeure utilisé par des civils. Cet état de fait implique d'apprécier avec les plus grandes exigence et rigueur les incidences de sa destruction ou neutralisation sur les civils, particulièrement compte tenu des caractéristiques intrinsèques au cyberespace. Ces effets ne doivent pas être disproportionnés par rapport à l'avantage militaire direct et concret attendu de l'attaque.

En ce qui concerne les personnes civiles, leurs actions dans des contextes de conflit armé sont susceptibles, si commises à grande échelle, de fragiliser la protection qui leur est due. Dans le monde actuel, la disponibilité plus grande des technologies de l'information et de la communication auprès des personnes civiles implique qu'il est souvent plus facile pour un civil de fournir des informations utiles aux belligérants. Cela soulève des questions liées aux enjeux la participation directe des hostilités de ces civils. En effet, les civils peuvent perdre la protection qui leur est normalement octroyée et être ciblés lorsqu'ils participent directement aux hostilités et pendant toute la durée de cette participation.

Si aucune disposition n'interdit expressément aux Etats d'inviter ou d'inciter la population civile majeure à participer directement aux hostilités, cette pratique crée néanmoins un climat propice à la confusion des civils avec les combattants.

Il nous semble ainsi fondamental que les incidences de cette participation soient pleinement comprises par la population. De fait, la formation, en temps de paix, au DIH auprès d'un large public (militaire et civil) est essentielle. La formation au DIH est une priorité des autorités françaises, avec l'adoption d'une nouvelle stratégie humanitaire de la République française pour les années 2023-2027, qui vise à promouvoir et renforcer le respect du DIH.

Enfin, nous souhaiterions conclure en saluant, à nouveau, les travaux conduits par le CICR lors de la 34ème conférence du mouvement, en octobre dernier, qui ont permis l'adoption de la résolution portant sur la protection des 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 doit nous permettre de bâtir sur ce succès pour aller plus loin.

Je vous remercie.