Le pouvoir de l'humanité
XXXIVe Conférence internationale
de la Croix-Rouge et du Croissant-Rouge
28-31 octobre 2024, Genève

Prévenir et réduire les menaces numériques auxquelles font face les personnes touchées par les conflits armés

ÉLÉMENTS POSSIBLES D'UNE RÉSOLUTION

Novembre 2023

FR

Original : anglais

Document établi par le Comité international de la Croix-Rouge en consultation avec
la Fédération internationale des Sociétés de la Croix-Rouge et du Croissant-Rouge

ÉLÉMENTS POSSIBLES D'UNE RÉSOLUTION

Prévenir et réduire les menaces numériques auxquelles font face les personnes touchées par les conflits armés

CONTEXTE

Les éléments proposés pour la résolution relative à la prévention et à la réduction des menaces numériques auxquelles font face les personnes touchées par les conflits armés donnent un aperçu de la teneur possible des différents paragraphes qui la composeront, sans toutefois proposer d'avant-projet de texte. Chaque paragraphe est suivi d'une explication sur les raisons pour lesquelles il serait utile de l'inclure dans la résolution.

Le présent document est envoyé pour consultation aux membres de la Conférence internationale de la Croix-Rouge et du Croissant-Rouge en vue de recueillir leurs premières observations et suggestions et de nous faire une idée du degré d'acceptation et de consensus que suscite l'approche proposée.

Veuillez formuler vos observations et commentaires sur ce document de manière à répondre aux questions suivantes :

- Êtes-vous d'accord avec les différents éléments qu'il est proposé d'inclure dans le préambule et le dispositif du projet de résolution ?
- Y a-t-il des éléments manquants qui devraient être inclus dans la résolution ?

Il ne s'agit pas, à ce stade, de formuler des observations détaillées sur le libellé des éléments possibles de la résolution. Vous aurez tout loisir de le faire ultérieurement, une fois que l'avant-projet de résolution sera disponible.

INTRODUCTION

La disponibilité et la fiabilité des technologies, des infrastructures (notamment pour la connexion à Internet) et des données numériques revêtent une grande importance et peuvent contribuer à sauver des vies dans les situations d'urgence, en particulier dans les conflits armés. Ces ressources numériques peuvent permettre aux personnes de survivre – en les aidant par exemple à savoir où trouver de l'eau, de la nourriture, des couvertures et un abri sûr – ou de contacter et retrouver des proches dont elles avaient perdu la trace. Elles permettent aussi aux gouvernements de fournir des services essentiels à la population et de maintenir un système de gouvernance civile. La confidentialité, la fiabilité et la disponibilité des technologies et des données numériques sont également indispensables au bon fonctionnement des services médicaux – tant militaires que civils – et font partie des caractéristiques clés des opérations humanitaires, y compris celles du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement).

La numérisation des conflits armés fait peser de nouvelles menaces sur la vie, la sécurité et la dignité des civils, du personnel médical, des soldats hors de combat et de ceux qui s'efforcent

de leur apporter protection et assistance. Si les acteurs étatiques et non étatiques ont recours à des moyens et méthodes de guerre numériques pour vaincre leurs adversaires, ces moyens et méthodes sont utilisés également pour mettre hors d'usage des infrastructures et services civils essentiels, pour inciter à la violence contre des populations civiles, le personnel médical ou les soldats hors de combat, et pour perturber les opérations d'assistance médicale et humanitaire ou saper la confiance dans ces opérations. L'usage malveillant des technologies numériques alimente les conflits, mine la confiance et exacerbe les vulnérabilités. Et l'utilisation croissante de l'intelligence artificielle dans ces contextes risque d'aggraver l'ampleur de ces effets ainsi que leur impact.

Le CICR, conjointement avec ses partenaires du Mouvement, est aux avant-postes pour attirer l'attention sur les menaces que la numérisation des opérations militaires fait peser sur les populations civiles, le personnel médical et les soldats hors de combat, et s'emploie à faire mieux connaître et comprendre le droit international humanitaire applicable aux conflits armés, y compris en ce qui concerne les cyberopérations et les opérations d'information.

Le Mouvement a par ailleurs contribué à une meilleure compréhension des enjeux de la protection des données dans le cadre des opérations humanitaires (voir Manuel sur la protection des données dans l'action humanitaire), établi un consensus international sur l'importance de protéger les données dans le contexte du rétablissement des liens familiaux (voir XXXIII^{e} Conférence internationale de la Croix-Rouge et du Croissant-Rouge, résolution 4 intitulée Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles) et convenu de mesures concrètes pouvant être adoptées par les membres du Mouvement pour protéger les données humanitaires (voir Conseil des Délégués de 2022, résolution 12 intitulée La protection des données humanitaires).

Les gouvernements ont quant à eux œuvré dans les enceintes des Nations Unies consacrées aux technologies de l'information et aux télécommunications pour renforcer la sécurité internationale et la protection des droits humains dans l'espace numérique.

Présentée dans le cadre du forum humanitaire unique que constitue la Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale), la résolution proposée vise à attirer l'attention sur les menaces numériques auxquelles font face les populations civiles, le personnel médical et les soldats hors de combat, et à recenser des mesures que les États et les membres du Mouvement pourraient prendre pour prévenir ou réduire ces menaces.

Paragraphes du préambule (PP)

PP 1 :
Ce paragraphe du préambule pourrait *souligner* l'importance que revêtent la disponibilité et la fiabilité des technologies, des infrastructures (notamment pour la connexion à Internet) et des données numériques pour assurer la fourniture de services essentiels – en particulier de services médicaux et humanitaires – à la population civile et pour permettre aux civils de savoir où ils peuvent trouver un abri sûr et des biens indispensables à leur survie, ou comment maintenir le contact avec des proches, en particulier lors d'un conflit armé.

Explication :
Il s'agit d'établir une compréhension commune du rôle important que jouent les technologies, les infrastructures et les données numériques lorsqu'il est question de protéger la vie, la sécurité et la dignité des personnes touchées par un conflit armé.

PP 2 :
Ce paragraphe du préambule pourrait *rappeler* que les États s'emploient à développer leurs capacités numériques à des fins militaires, que ces capacités sont utilisées dans des conflits armés actuels et que la probabilité qu'elles soient utilisées dans des conflits futurs ne fait qu'augmenter ; il pourrait en outre *faire état* de la préoccupation liée au risque que ces

technologies soient utilisées pour infliger des dommages à des civils, des membres du personnel médical, des soldats hors de combat, des biens de caractère civil ou d'autres personnes et biens protégés – ou qu'elles occasionnent de tels dommages de manière incidente – et qu'elles causent des maux superflus et des souffrances inutiles.

Explication :
Il s'agit de prendre acte des avancées militaires dans ce domaine et du coût en vies humaines pouvant résulter de l'utilisation de ces technologies dans les situations de conflit armé.

PP 3 :
Ce paragraphe du préambule pourrait *exprimer* une vive préoccupation quant au coût humain que peuvent avoir les effets directs et indirects des cyberopérations qui impactent les infrastructures, les services et les données civiles indispensables pour assurer la sécurité et la dignité des personnes ainsi que le fonctionnement de la société.

Explication :
Il s'agit de reconnaître le coût humain potentiel des cyberopérations.

PP 4 :
Ce paragraphe du préambule pourrait *exprimer* une vive préoccupation quant à l'ampleur, la rapidité et la portée des opérations d'information numériques ainsi qu'aux dommages qu'elles peuvent causer en incitant à la violence et la haine, en alimentant les tensions et en compromettant la disponibilité et l'intégrité des informations dont les civils ont besoin pour assurer leur sécurité et leur survie en période de conflit armé.

Explication :
Il s'agit de reconnaître le coût humain potentiel des opérations d'information.

PP 5 :
Ce paragraphe du préambule pourrait *exprimer* des inquiétudes quant au fait que des civils, en particulier des individus, des groupes ou des entreprises, puissent mener des cyberopérations ou des opérations d'information en lien avec un conflit armé, et que ces opérations puissent les exposer à des dommages et porter atteinte au principe de distinction.

Explication :
Il s'agit de reconnaître les risques encourus lorsqu'on encourage ou tolère la participation de civils à des cyberopérations ou des opérations d'information menées en lien avec un conflit armé.

PP 6 :
Ce paragraphe du préambule pourrait *exprimer* des inquiétudes quant au risque que des infrastructures numériques civiles, comme les systèmes de communication ou les clouds, soient utilisées à des fins militaires et deviennent ainsi des objectifs militaires, et quant aux conséquences qu'une attaque contre de tels objectifs aurait pour les civils.

Explication :
Il s'agit de reconnaître les dangers liés à l'utilisation de biens civils à des fins militaires, qui risque d'en faire des objectifs militaires et de les exposer ainsi à des dommages.

PP 7 :
Ce paragraphe du préambule pourrait *exprimer* des inquiétudes quant au risque que les cyberopérations, en particulier celles qui ont des effets indiscriminés, menées dans le cadre d'un conflit armé portent atteinte incidemment à des civils par-delà le territoire des parties au conflit, du fait de l'interconnexion mondiale du cyberespace.

Explication :
Il s'agit de reconnaître que les cyberopérations risquent d'avoir des effets qui se propagent et portent atteinte à des civils par-delà les frontières, en particulier lorsque ces attaques frappent sans discrimination.

PP 8 :
Ce paragraphe du préambule pourrait *rappeler* que les entreprises de la tech fournissent toute une palette de produits, de services et d'infrastructures dont dépendent les populations civiles et les gouvernements, *mettre en avant* la responsabilité qui incombe à ces entreprises de respecter les droits des personnes touchées par un conflit armé, et *souligner* l'importance d'associer ces entreprises aux discussions sur la protection des civils contre les menaces numériques dans les situations de conflit armé.

Explication :
Il s'agit de reconnaître le rôle particulier que jouent les entreprises de la tech en tant que fournisseurs de produits, de services et d'infrastructures numériques, y compris lors de conflits armés.

PP 9 :
Ce paragraphe du préambule pourrait *reconnaître* l'importance que revêtent les technologies, les infrastructures (notamment pour la connexion à Internet) et les données numériques pour la conduite d'opérations humanitaires efficaces et efficientes, et *exprimer* de vives inquiétudes quant aux conséquences que les cyberopérations, notamment le piratage de données, et les opérations d'information ciblant des organisations humanitaires risquent d'avoir pour les personnes auxquelles ces organisations viennent en aide, pour les organisations elles-mêmes et pour leur personnel.

Explication :
Il s'agit de reconnaître l'importance que revêtent les technologies (et les données) numériques pour les organisations humanitaires ainsi que les dommages pouvant être causés lorsqu'elles sont prises pour cible.

PP 10 :
Ce paragraphe du préambule pourrait *rappeler* la valeur juridique et protectrice des emblèmes et signaux distinctifs, le cas échéant, qui sont destinés à identifier les unités et moyens de transport sanitaires, le personnel médical et religieux, ainsi que les membres du Mouvement international de la Croix-Rouge et du Croissant-Rouge, et qui, en raison du fait qu'ils sont cités dans les quatre Conventions de Genève et de la pratique en cours depuis plus de 160 ans, sont devenus des signes universellement reconnus de l'aide et de la protection impartiales et neutres en faveur des victimes des conflits armés et autres situations d'urgence, et *saluer* les travaux de recherche et les consultations menés par le CICR, en collaboration avec des établissements universitaires et d'autres composantes du Mouvement, sur la faisabilité d'un « emblème numérique[1] », c'est-à-dire un moyen numérique permettant d'identifier les données et infrastructures numériques des organisations et entités autorisées à utiliser les emblèmes distinctifs reconnus par le droit international humanitaire.

Explication :
Il s'agit de rappeler le rôle joué par les emblèmes distinctifs en vertu du droit international humanitaire et de saluer les consultations et les travaux de recherche menés par le CICR sur la possibilité d'utiliser un « emblème numérique ».

[1] Voir CICR, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions (numérisation des emblèmes de la croix rouge, du croissant rouge et du cristal rouge : avantages, risques et solutions possibles), 3 novembre 2022.

PP 11 :
Ce paragraphe du préambule pourrait *rappeler* et *réaffirmer* la résolution 4 adoptée par la XXXIII[e] Conférence internationale et intitulée « Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles », et *souligner* que les questions abordées dans cette résolution sont importantes également du point de vue de la protection des autres données humanitaires.

Explication :
Il s'agit de rappeler et réaffirmer l'accord conclu lors de la XXXIII[e] Conférence internationale concernant la protection des données dans le cadre de l'action du Mouvement en matière de rétablissement des liens familiaux.

PP 12 :
Ce paragraphe du préambule pourrait *prendre note* de la résolution 12 adoptée par le Conseil des Délégués de 2022 et intitulée « La protection des données humanitaires », et *saluer* les engagements pris par le Mouvement en matière de protection des données humanitaires.

Explication :
Il s'agit de reconnaître les travaux entrepris au sein du Mouvement dans le domaine de la protection des données humanitaires.

PP 13 :
Ce paragraphe du préambule pourrait *exprimer* la conviction qu'aucune disposition du droit international humanitaire, tel qu'applicable aux cyberopérations et aux opérations d'information, ne peut être interprétée comme légitimant ou autorisant tout acte d'agression ou tout autre emploi de la force incompatible avec la Charte des Nations Unies.

Explication :
Il s'agit de rappeler la conviction partagée par les États, telle qu'énoncée dans le préambule du premier Protocole additionnel.

PP 14 :
Ce paragraphe du préambule pourrait *souligner* le fait que les personnes, au même titre que les organisations médicales et humanitaires, font face à des menaces numériques dans les situations d'urgence autres que les conflits armés, *appeler* les États à prendre appui sur cette résolution pour mettre en place des mesures efficaces visant à assurer leur protection conformément aux cadres juridiques applicables, et *demander* au Mouvement de prendre des mesures appropriées pour assurer en tout temps la cybersécurité et la protection des données.

Explication :
Il s'agit de rappeler que les menaces numériques ne concernent pas uniquement les situations de conflit armé et que les États et les composantes du Mouvement doivent mettre en place des mesures de protection également en dehors de ces situations.

Paragraphes du dispositif (OP)

OP 1 :
Ce paragraphe du dispositif pourrait *souligner* la volonté démontrée par tous les membres de la Conférence internationale de protéger les civils, les biens de caractère civil et les autres personnes et biens bénéficiant d'une protection particulière contre les menaces numériques dans les situations de conflit armé.

Explication :
Il s'agit d'exprimer l'objectif humanitaire commun consistant à protéger les civils et les biens de caractère civil contre les menaces numériques dans les situations de conflit armé.

OP 2 :
Ce paragraphe du dispositif pourrait *réaffirmer* l'importance fondamentale des obligations qui incombent à toutes les parties aux conflits armés au titre du droit international humanitaire et d'autres branches du droit international, si applicables, en particulier le droit international des droits humains, s'agissant de protéger les civils, les biens de caractère civil et les autres personnes et biens bénéficiant d'une protection particulière contre les cyberopérations et les opérations d'information dans les situations de conflit armé.

Explication :
Il s'agit de réaffirmer le cadre juridique existant applicable aux cyberopérations et aux opérations d'information dans les situations de conflit armé.

OP 3 :
Ce paragraphe du dispositif pourrait *appeler* tous les États et toutes les parties aux conflits armés à veiller à ce que le droit international humanitaire soit appliqué de manière à garantir une protection adéquate aux civils, au personnel médical, aux soldats hors de combat, aux infrastructures et aux données civiles, ainsi qu'aux autres personnes et biens bénéficiant d'une protection particulière au sein de nos sociétés de plus en plus numérisées ; *demander* à ce que les règles applicables soient respectées ; et *inviter instamment* tous les États et autres acteurs qui s'emploient à renforcer leurs capacités dans le domaine de la cybernétique ou des technologies de l'information à prendre les mesures d'ordre législatif, administratif et pratique nécessaires au niveau national pour s'acquitter de leurs obligations juridiques.

Explication :
Il s'agit d'appeler tous les États et toutes les parties aux conflits armés à mettre en place une protection adéquate contre les menaces numériques et à veiller au respect des règles juridiques applicables.

OP 4 :
Ce paragraphe du dispositif pourrait *appeler* tous les États et les parties aux conflits armés à respecter en particulier le principe de distinction, un principe cardinal consacré par le droit international humanitaire, en vue de protéger les civils des dangers des hostilités, notamment lorsqu'ils mènent des cyberopérations ou des opérations d'information ; *souligner* en particulier que les cybercapacités assimilables à des armes et de nature à frapper sans discrimination sont interdites ; *insister* sur le fait qu'il est interdit de diriger des attaques directes contre des civils ou des biens de caractère civil, de se livrer à des actes ou des menaces de violence dont le but principal est de répandre la terreur parmi la population civile, de lancer des attaques indiscriminées ou disproportionnées, d'attaquer, de détruire, d'enlever ou de mettre hors d'usage des biens indispensables à la survie de la population, de recourir à la perfidie ou de faire un usage abusif des emblèmes, signaux, drapeaux, uniformes et insignes spécifiquement protégés, y compris lors de l'utilisation de moyens et méthodes de guerre numériques ; et *rappeler* aux États et aux parties aux conflits qu'il faut veiller en tout temps à épargner la population civile et les biens de caractère civil et prendre toutes les précautions pratiquement possibles pour éviter, ou du moins réduire autant que possible, les dommages causés incidemment aux civils et pour protéger la population civile et les biens de caractère civil soumis à leur autorité contre les effets des attaques, y compris lorsqu'ils utilisent des moyens et méthodes de guerre numériques.

Explication :
Il s'agit de réaffirmer certaines des règles de base du DIH qui protègent les civils contre les menaces numériques dans les situations de conflit armé.

OP 5 :

Ce paragraphe du dispositif pourrait *appeler* les États et les parties aux conflits armés à s'acquitter de l'obligation qui leur incombe au titre du droit international humanitaire de respecter et protéger en toutes circonstances le personnel médical ainsi que les unités et moyens de transport sanitaires, y compris lors de cyberopérations et d'opérations d'information.

Explication :
Il s'agit de réaffirmer le fait que le personnel médical ainsi que les unités et moyens de transport sanitaires bénéficient d'une protection juridique internationale spécifique contre les menaces numériques dans les situations de conflit armé.

OP 6 :
Ce paragraphe du dispositif pourrait *appeler* les États et les parties aux conflits armés à respecter l'obligation qui leur incombe au titre du droit international humanitaire d'autoriser et de faciliter dans les situations de conflit armé la conduite d'activités humanitaires impartiales, y compris celles menées à l'aide de moyens numériques, et de respecter et protéger les activités et le personnel humanitaires, y compris lors de cyberopérations et d'opérations d'information.

Explication :
Il s'agit de réaffirmer le fait que les organisations humanitaires impartiales bénéficient d'une protection juridique internationale spécifique contre les menaces numériques dans les situations de conflit armé.

OP 7 :
Ce paragraphe du dispositif pourrait *rappeler* que lorsque les parties à un conflit armé encouragent la participation de civils à un conflit armé, y compris à travers des moyens numériques, les civils en question risquent de perdre leur protection juridique contre les attaques, ou d'être perçus comme ayant perdu cette protection, et *appeler* les parties à en tenir compte et à prendre toutes les précautions possibles pour éviter d'exposer des civils à des dommages.

Explication :
Il s'agit de reconnaître les risques encourus lorsqu'on encourage des civils à participer aux hostilités, et d'appeler les parties à prendre toutes les précautions possibles pour protéger les civils.

OP 8 :
Ce paragraphe du dispositif pourrait *mettre en avant* le fait que les acteurs non étatiques, y compris les civils et les groupes armés non étatiques, qui mènent des cyberopérations en lien avec un conflit armé doivent, quel que soit leur statut, se conformer au droit international humanitaire, *réaffirmer* la volonté des États de prendre des mesures pour faire en sorte que les acteurs non étatiques agissant sur instruction, sous la direction ou sous le contrôle d'un État, ou à partir de son territoire, ne mènent pas d'opérations qui violent le droit international humanitaire et pour qu'ils répriment toute violation de ce droit, et *encourager* le CICR et les Sociétés nationales de la Croix-Rouge et du Croissant-Rouge à redoubler d'efforts pour œuvrer à la diffusion du droit international humanitaire.

Explication :
Il s'agit de réaffirmer le rôle premier des États s'agissant de faire respecter le droit international humanitaire par les acteurs non étatiques, et de reconnaître le rôle statutaire du Mouvement s'agissant de faire mieux connaître ce droit.

OP 9 :
Ce paragraphe du dispositif pourrait *rappeler* que les entreprises de la tech qui opèrent dans des contextes de conflit armé, ou qui fournissent des services en rapport avec de tels contextes, devraient être au fait et tenir compte des implications que leurs opérations ont au regard du droit international humanitaire, s'assurer que leurs employés respectent les obligations qui leur

incombent et prendre des mesures appropriées pour protéger leur personnel ainsi que les civils qui dépendent de leurs produits et services contre tout dommage éventuel.

Explication :
Il s'agit d'amener les entreprises de la tech à prendre conscience des implications de leurs opérations dans les situations de conflit armé et à prendre des mesures pour protéger la population civile.

OP 10 :
Ce paragraphe du dispositif pourrait *encourager* les États à dissocier, c'est-à-dire séparer physiquement ou techniquement, dans la mesure du possible, les infrastructures numériques utilisées à des fins militaires des infrastructures civiles, sachant que l'utilisation d'infrastructures civiles à des fins militaires risque d'en faire un objectif militaire, ce qui pourrait porter atteinte aux civils qui se servent de ces mêmes infrastructures.

Explication :
Il s'agit d'encourager les États à dissocier, dans la mesure du possible, les infrastructures numériques utilisées à des fins militaires de celles utilisées à des fins civiles.

OP 11 :
Ce paragraphe du dispositif pourrait *encourager* tous les membres du Mouvement à tenir compte, dans le cadre de leur travail, des menaces numériques et des dommages pouvant en résulter, leur *demander instamment* de renforcer leur préparation et leur capacité à faire face aux menaces numériques auxquelles sont exposés les civils, par exemple en améliorant leur capacité à détecter ces menaces et à déployer des activités de protection en faveur de la population civile, et *inviter* les États à soutenir le Mouvement dans ces efforts.

Explication :
Il s'agit d'encourager le Mouvement à renforcer sa capacité à faire face aux menaces numériques et d'inviter les États à soutenir ces efforts et les investissements qu'ils impliquent.

OP 12 :
Ce paragraphe du dispositif pourrait *se féliciter* des résultats des recherches et des tests en cours sur un emblème numérique, et *encourager* le CICR à proposer, en consultation avec les États et les composantes du Mouvement, une solution technique, globale et durable, et à formuler des propositions pour que les États puissent l'incorporer dans le droit international humanitaire.

Explication :
Il s'agit d'inviter le CICR à poursuivre ses travaux sur un emblème numérique, en étroite collaboration avec les États et le Mouvement.

OP 13 :
Ce paragraphe du dispositif pourrait *engager* les composantes du Mouvement à prendre des mesures appropriées, dans les limites de leurs mandats, leurs capacités et leurs besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de cybersécurité et de protection des données ; pour appliquer les meilleures pratiques de gouvernance des données à l'ensemble des données humanitaires ; pour observer les normes et les meilleures pratiques pertinentes lors du traitement de données personnelles, en tenant compte du Manuel sur la protection des données dans l'action humanitaire ; et pour se conformer à la législation en vigueur et aux cadres applicables en matière de protection des données personnelles, et *exprimer* le soutien des États à l'égard de ces mesures.

Explication :
Il s'agit d'engager le Mouvement à prendre des mesures appropriées en matière de cybersécurité et de protection des données pour protéger les populations auxquelles il vient en aide.

OP 14 :
Ce paragraphe du dispositif pourrait *rappeler* que les composantes du Mouvement doivent traiter des données personnelles pour pouvoir s'acquitter de leurs mandats respectifs, notamment au titre du droit international humanitaire, lorsqu'il s'applique, et des Statuts du Mouvement, et que ce traitement est nécessaire et justifié par des motifs importants d'intérêt public ainsi que par les intérêts vitaux des personnes, et *engager instamment* les États et le Mouvement à coopérer pour veiller à ce que les données personnelles ne soient pas sollicitées ni utilisées à des fins incompatibles avec la nature humanitaire de l'action du Mouvement, conformément à l'article 2 des Statuts du Mouvement et notamment à son alinéa 5, ou d'une manière susceptible de nuire à la confiance des personnes auxquelles il vient en aide ou à l'indépendance, l'impartialité et la neutralité des opérations du Mouvement.

Explication :
Il s'agit de rappeler l'importance que revêt le traitement des données dans le cadre de l'action humanitaire menée par le Mouvement et d'engager les États à coopérer pour permettre aux membres du Mouvement de s'acquitter de leurs mandats respectifs.

OP 15 :
Ce paragraphe du dispositif pourrait *inviter* le CICR à continuer d'évaluer les menaces numériques dans les situations de conflit armé ainsi que la protection accordée aux civils face à ces menaces, notamment au titre du droit international humanitaire, et à faire rapport à la XXXV^{e} Conférence internationale sur ce sujet.

Explication :
Il s'agit d'inviter le CICR à faire rapport à la prochaine Conférence internationale au sujet de la présente résolution.