



## **Power of humanity**

**34th International Conference  
of the Red Cross and Red Crescent**

28–31 October 2024, Geneva

# **Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés**

DOCUMENT DE RÉFÉRENCE

Septembre 2024

**FR**

IC34/24/9.2  
Original : anglais  
Pour information

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

## DOCUMENT DE RÉFÉRENCE

---

# Protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques menées dans les conflits armés

---

### RÉSUMÉ

La résolution vise à protéger les civils ainsi que les autres personnes et biens protégés dans les situations de conflit armé contre les dangers résultant des activités numériques. Elle cherche à établir une compréhension commune des perspectives ouvertes par le fait de disposer de technologies numériques fiables durant un conflit armé et des dangers que représente leur utilisation à des fins militaires, ainsi qu'à recenser des mesures concrètes pour faire face à ces dangers. La résolution appelle les États et les composantes du Mouvement international de la Croix-Rouge et du Croissant-Rouge (Mouvement) à prendre des mesures dans ce sens.

La disponibilité et la fiabilité des technologies numériques ouvrent des perspectives dans les domaines social, économique, du développement ainsi que de l'information et de la communication. Dans les situations de conflit armé, les technologies numériques peuvent contribuer à sauver des vies et à améliorer les conditions d'existence. Elles 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. Dans le même temps, l'utilisation des technologies numériques à des fins militaires pendant un conflit armé peut présenter de nouvelles menaces pour la vie, la sécurité et la dignité des civils ainsi que des autres personnes et biens protégés. Les cyberopérations et les opérations d'information dirigées contre des civils et d'autres personnes et biens protégés sont particulièrement préoccupantes, notamment celles qui visent les structures médicales et les opérations humanitaires.

Pour faire face à ces dangers, la résolution rappelle le consensus des États autour du fait que le droit international humanitaire (DIH) s'applique uniquement aux situations de conflit armé, reconnaissant la nécessité d'examiner plus avant de quelle manière et dans quelles circonstances le DIH s'applique à l'utilisation des technologies numériques. La résolution rappelle ensuite un certain nombre de règles et principes cardinaux du DIH relatifs à la protection des populations civiles, exige leur mise en œuvre effective et invite les États à respecter l'obligation qui leur incombe de respecter et protéger en toutes circonstances le personnel médical ainsi que les unités et moyens de transport sanitaires (c'est-à-dire les véhicules) et d'autoriser et faciliter, ainsi que de respecter et protéger, les activités de secours humanitaires. La résolution propose également d'inviter les États et les composantes du Mouvement à saluer les travaux de recherche menés par le Comité international de la Croix-Rouge (CICR) – en consultation avec des experts externes et d'autres composantes du Mouvement – sur la possibilité d'utiliser un emblème numérique et encourage la poursuite des travaux dans ce domaine.

La résolution rappelle en outre la responsabilité qui incombe aux composantes du Mouvement de prendre des mesures appropriées, dans les limites de leurs mandats, possibilités et besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de sécurité numérique et de protection des données.

## 1) INTRODUCTION

Le fait de disposer de technologies numériques fiables ouvre des perspectives dans les domaines social, économique, du développement ainsi que de l'information et de la communication et peut contribuer à sauver des vies et à améliorer les conditions d'existence. Pendant un conflit armé, les technologies 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. Les technologies numériques peuvent également permettre aux organisations humanitaires d'acheminer plus efficacement l'aide humanitaire et aux belligérants, par exemple, d'alerter efficacement la population civile et de mieux assurer sa protection et sa reconnaissance. Parallèlement, l'utilisation des technologies numériques à des fins militaires pendant un conflit armé engendre de nouvelles menaces pour la vie, la sécurité et la dignité des civils ainsi que des autres personnes et biens protégés.

Conjointement avec ses partenaires du Mouvement, le CICR a joué un rôle de premier plan dans les travaux de recherche et les consultations d'experts portant sur le coût humain potentiel de certaines activités numériques, notamment les cyberopérations et les opérations d'information menées dans les conflits armés. Conscient des enjeux et conformément à son mandat, le CICR s'emploie à faire mieux comprendre et mieux connaître le DIH, y compris en ce qui concerne les nouveaux moyens et méthodes de guerre. Les États ont œuvré dans les enceintes des Nations Unies consacrées aux technologies numériques dans le contexte de la sécurité internationale et de la protection des droits humains. Depuis 2019, le Mouvement met davantage l'accent sur les risques liés à la protection des données dans les opérations humanitaires, notamment le piratage de données.

Présentée dans le cadre du forum humanitaire unique de la Conférence internationale de la Croix-Rouge et du Croissant-Rouge (Conférence internationale), la résolution proposée vise à attirer l'attention sur la nécessité de protéger les civils, ainsi que les autres personnes et biens protégés, contre le coût humain potentiel des activités numériques, et à recenser des mesures que les États et les membres du Mouvement peuvent prendre pour prévenir ou réduire les dommages causés aux civils.

## 2) CONTEXTE

C'est la première fois qu'une résolution de la Conférence internationale aborde la question de l'utilisation des capacités numériques dans les conflits armés, en particulier les cyberopérations et les opérations d'information. Elle s'appuiera sur les résolutions de la Conférence internationale et du Conseil des Délégués qui portaient sur la protection des données ainsi que sur les rapports établis par le CICR en collaboration avec des experts du monde entier sur la protection des civils contre les menaces numériques.

En ce qui concerne la protection des données humanitaires, la résolution proposée s'inspirera de la résolution intitulée « [Rétablir les liens familiaux tout en respectant la vie privée, y compris en ce qui concerne la protection des données personnelles](#) », adoptée à la XXXIII<sup>e</sup> Conférence internationale en 2019, ainsi que des mesures convenues par les composantes du Mouvement dans la résolution intitulée « [La protection des données humanitaires](#) », adoptée au Conseil des Délégués de 2022. Le « [Manuel sur la protection des données dans l'action humanitaire](#) » peut également présenter un intérêt dans ce contexte.

S'agissant des dangers présentés par l'utilisation des technologies numériques dans les conflits armés et des mesures pratiques que les États et les organisations humanitaires devraient envisager, le CICR souhaite attirer l'attention des délégations en particulier sur le rapport 2023 du [Conseil consultatif mondial sur les menaces numériques dans les conflits armés](#). Créé par le CICR, ce conseil réunit un groupe mondial de responsables des questions politiques, juridiques, militaires et technologiques. Son rapport présente quatre principes

directeurs et 25 recommandations concrètes à l'intention des belligérants, des États, des entreprises technologiques et des organisations humanitaires afin de prévenir ou d'atténuer les menaces numériques qui pèsent sur les populations civiles<sup>1</sup>. La résolution proposée abordant également les travaux de recherche menés par le CICR sur la possibilité d'un emblème numérique, le rapport intitulé « [Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions](#) » et la vidéo « [Digital Emblem | Explained](#) » peuvent présenter un intérêt particulier.

### 3) ANALYSE/PROGRÈS RÉALISÉS

Dans les régions touchées par un conflit armé ou d'autres situations d'urgence, les populations dépendent souvent de la disponibilité et de la fiabilité des technologies numériques pour accéder aux biens et aux services essentiels à leur survie et à leur bien-être. Les technologies numériques permettent aux gouvernements de fournir des services essentiels à la population et de maintenir un système de gouvernance civile. La confidentialité, l'intégrité et la disponibilité des technologies numériques, ainsi que des données sur lesquelles elles reposent, sont également indispensables au bon fonctionnement des services médicaux – tant militaires que civils – et revêtent une importance croissante dans les opérations humanitaires, y compris celles menées par le Mouvement. Parallèlement, les technologies numériques sont également utilisées de nos jours comme moyen ou méthode de guerre, en particulier sous la forme de cyberopérations et d'opérations d'information. Cette réalité soulève des questions et des enjeux considérables pour la protection des populations touchées par les conflits et pour une action humanitaire fondée sur des principes.

#### A) Dangers résultant d'activités numériques auxquels la population civile est exposée

Sur la base de ce qui a été observé dans les conflits armés contemporains et des recherches et consultations évoquées plus haut, quatre types de dangers résultant d'activités numériques semblent particulièrement pertinents, en raison de leur probabilité et de leurs conséquences négatives potentielles sur les civils.

##### **Cyberopérations**

Plus notre quotidien est régi par les technologies numériques, plus grand est le risque que des cyberopérations menées dans le cadre d'un conflit armé infligent des dommages aux populations civiles. Les cyberopérations peuvent mettre hors service ou endommager physiquement des installations industrielles, des réseaux de communication et d'autres éléments de l'infrastructure essentielle d'un État, d'une manière qui pourrait directement ou indirectement causer des dommages, des blessures ou la mort de civils, notamment en empêchant le bon fonctionnement de services essentiels. Les cyberopérations conçues pour manipuler des informations à des fins cognitives pourraient avoir des conséquences similaires, notamment par le vol, la fuite, la manipulation ou la suppression de données. En raison de l'interconnectivité propre au cyberspace, il existe un risque réel que les cyberopérations – si elles sont conçues dans ce but ou ne sont pas correctement mises à l'essai ou contrôlées – portent atteinte sans discrimination à des systèmes informatiques largement utilisés et des infrastructures civiles connectées bien au-delà de la zone de conflit, causant directement ou indirectement des dommages, des blessures ou la mort de civils et contribuant à aggraver les conflits.

##### **Opérations d'information**

Les opérations d'information font depuis longtemps partie des conflits armés. Elles sont autorisées dans certaines circonstances, par exemple pour prévenir les civils d'attaques

---

<sup>1</sup> D'autres publications du CICR peuvent présenter un intérêt : [The Potential Human Cost of Cyber Operations](#), (Le coût humain potentiel des cyberopérations), 2019 ; [Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts](#) (Éviter les dommages civils causés par des cyberopérations militaires dans les conflits armés), 2021 ; [Harmful Information: Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence](#) (Informations malveillantes : mésinformation, désinformation et discours de haine dans les conflits armés et autres situations de violence), 2021.

militaires ou pour tromper l'adversaire, conformément au droit international. La numérisation a accru l'ampleur, la vitesse de propagation et la portée de ces opérations – et aujourd'hui, le recours à l'intelligence artificielle et à d'autres technologies émergentes peut conduire à amplifier ces phénomènes. Les opérations d'information essaient dans d'innombrables écosystèmes et plateformes d'information, déformant les faits, influençant les croyances et les comportements, alimentant les tensions et accroissant le risque de dommages causés aux civils en attisant la méfiance et en propageant la haine en ligne et hors ligne. Les femmes, les enfants et les minorités vulnérables sont particulièrement exposés à ces risques. Par ailleurs, des informations préjudiciables peuvent avoir un impact sur la vie des personnes, leur sécurité et leur dignité, et contribuer à l'escalade de la violence. Elles peuvent aussi compromettre la disponibilité, l'intégrité et la fiabilité des informations essentielles dont les civils ont besoin pour leur sécurité et leur survie en période de conflit.

### **Participation des civils aux cyberopérations et aux opérations d'information**

Il y a longtemps que des civils – en tant qu'individus, groupes ou entreprises – sont amenés à assumer des fonctions militaires pendant un conflit armé et à participer à l'effort de guerre. Avec la numérisation des sociétés, les types d'opérations qu'ils peuvent mener et le nombre d'acteurs civils participant à un conflit armé sont en augmentation. Cette évolution engendre des risques pour la population civile qui ne sont pas suffisamment pris en compte : la multiplication des technologies numériques encourageant la participation de civils aux hostilités les expose à un risque accru de dommages. Plus l'infrastructure ou les services numériques sont utilisés indifféremment par des civils et des militaires, plus les infrastructures civiles risquent d'être attaquées.

### **Activités numériques dirigées contre des structures médicales et des organisations humanitaires**

Cela fait plusieurs années que le CICR s'inquiète toujours davantage du fait que l'essor de la numérisation rend les structures médicales vulnérables aux cyberopérations et aux dommages causés incidemment par de telles opérations dirigées contre d'autres cibles. De même, la désinformation véhiculée par des moyens numériques en vue de nuire à la mission primordiale des services médicaux engendre de nouveaux dangers, menaçant la sécurité du personnel médical. Le coût humain potentiel de ces activités numériques est particulièrement élevé dans les situations de conflit armé et d'urgence, où la fourniture de services médicaux revêt un caractère vital.

Compte tenu de l'ampleur des besoins et de la capacité de réponse humanitaire insuffisante, les activités numériques dirigées contre les organisations humanitaires risquent d'avoir des conséquences dévastatrices pour les populations dont la survie dépend de la protection et de l'assistance fournies par ces organisations. Ces dernières années, des composantes du Mouvement ont été victimes de ce type d'opérations qui revêtent différentes formes : cyberopérations visant à perturber ou détruire l'infrastructure numérique des organisations humanitaires, opérations consistant à pirater leurs systèmes pour exfiltrer des données ou encore opérations de désinformation qui, en ternissant leur réputation, entravent leur action.

Pour les acteurs médicaux et humanitaires, le piratage de données risque non seulement de mettre en danger des vies et des moyens d'existence, mais aussi d'éroder la confiance que leur accordent les civils et les parties aux conflits armés, compromettant leur accès aux personnes touchées ainsi que la sécurité de leur personnel.

## **B) Une réponse collective du Mouvement et des États parties aux Conventions de Genève**

Pour répondre aux dangers évoqués ci-dessus, la résolution proposée poursuit deux objectifs principaux.

Premièrement, dans les paragraphes du préambule, elle vise à établir une compréhension commune du coût humain potentiel des activités numériques menées dans les conflits armés. La résolution met particulièrement l'accent sur le risque que les cyberopérations perturbent les technologies numériques intégrées à des infrastructures civiles et des services essentiels ou utilisées par ces infrastructures et services, sur les opérations d'information incitant à la violence et à la haine en violation du DIH, sur les dangers spécifiques que ces activités numériques font peser sur les services médicaux et les opérations humanitaires, y compris leurs données, et sur les enjeux et les risques qu'il y a à encourager ou tolérer la participation de civils à des activités numériques dans un conflit armé.

Deuxièmement, dans les paragraphes du dispositif, la résolution rappelle le consensus des États autour du fait que le DIH s'applique uniquement aux situations de conflit armé, reconnaissant la nécessité d'examiner plus avant de quelle manière et dans quelles circonstances le DIH s'applique à l'utilisation des technologies numériques, ce qui est sans préjudice de la possibilité d'établir, à l'avenir, de nouvelles obligations contraignantes, le cas échéant. La résolution reconnaît également que les caractéristiques propres à l'environnement numérique soulèvent des questions quant à la manière dont certains principes et certaines règles du DIH s'appliquent dans ce contexte et que les avis des États divergent sur ces questions. Elle repose cependant aussi sur des points d'accord importants. La résolution rappelle les principes cardinaux du DIH relatifs à la protection des populations civiles, exige leur mise en œuvre effective et invite les parties au conflit à respecter l'obligation qui leur incombe de respecter et protéger en toutes circonstances le personnel médical ainsi que les unités et moyens de transport sanitaires (c'est-à-dire les véhicules), et d'autoriser et faciliter, ainsi que de respecter et protéger, les activités de secours et le personnel humanitaires. En outre, la résolution encourage toutes les composantes du Mouvement à intégrer la protection des civils ainsi que des autres personnes et biens protégés dans les conflits armés dans leurs activités opérationnelles, politiques et juridiques, et à prendre des mesures appropriées, dans les limites de leurs mandats, capacités et besoins opérationnels respectifs, pour renforcer leur capacité à assurer un niveau adéquat de sécurité numérique et de protection des données dans tous les aspects de leur action. Sur ces questions, la résolution appelle à une collaboration avec les États, qu'elle invite à soutenir ces efforts.

Les travaux de recherche menés par le CICR sur la possibilité d'utiliser un emblème numérique, c'est-à-dire un moyen numérique d'identifier les données et infrastructures numériques des organisations et entités autorisées à utiliser les emblèmes distinctifs reconnus par le DIH, pourraient contribuer à renforcer la protection des activités médicales et humanitaires contre les dangers résultant des activités numériques. À cet égard, la résolution vise à saluer le travail accompli jusqu'à présent par le Mouvement, en consultation avec les États et les spécialistes. Elle invite à poursuivre les travaux dans ce domaine.

#### **4) INCIDENCES EN TERMES DE RESSOURCES**

En adoptant la résolution, les États et les composantes du Mouvement s'engagent à prendre des mesures appropriées, dans les limites de leurs mandats, capacités et activités respectifs, afin de renforcer la protection des civils ainsi que des autres personnes et biens protégés dans les situations de conflit armé. La résolution attend également des composantes du Mouvement qu'elles prennent des mesures appropriées pour renforcer leur capacité à assurer un niveau adéquat de sécurité numérique et de protection des données. Elle encourage en outre le CICR à poursuivre ses travaux de recherche et à continuer d'éprouver la faisabilité technique d'un emblème numérique, ainsi qu'à consulter les États et les composantes du Mouvement sur les voies juridiques et diplomatiques pour son emploi possible.

La mise en œuvre de ces engagements est susceptible d'avoir des incidences en termes de ressources pour les États et les composantes du Mouvement, en fonction du degré d'avancement de leurs législations, politiques, programmes et activités existants.

## **5) MISE EN ŒUVRE ET SUIVI**

Le succès de la résolution dépendra de la mise en œuvre par les États et les composantes du Mouvement des mesures convenues dans leurs législations, politiques, programmes et activités. Les États sont censés agir dans le cadre de la mise en œuvre du DIH et des politiques relatives à la protection

des populations civiles. Quant aux composantes du Mouvement, elles devraient mettre en œuvre les parties pertinentes de la résolution dans le cadre des efforts déployés pour assurer la sécurité des données et la protection des données personnelles, selon leurs moyens et en fonction des besoins, et promouvoir la diffusion du DIH.

Tous les membres de la Conférence internationale sont invités à rendre compte à la prochaine Conférence internationale des progrès réalisés dans la mise en œuvre de la résolution.

## **6) CONCLUSION ET RECOMMANDATIONS**

En cette année marquant le 75<sup>e</sup> anniversaire de l'adoption des quatre Conventions de Genève, la résolution vise à prendre en compte les réalités changeantes des conflits armés. Elle cherche à établir une compréhension commune du coût humain potentiel des activités numériques menées dans les conflits armés et à recenser des moyens concrets pour y faire face. Elle appelle les États et les composantes du Mouvement à prendre des mesures à cet effet, dans les limites de leurs responsabilités respectives.

L'adoption de la résolution marquera une étape importante dans les efforts internationaux en cours pour faire en sorte que l'utilisation des technologies numériques améliore le bien-être des personnes. Elle mettra spécifiquement l'accent sur les besoins de protection des personnes touchées par les conflits armés. Adoptée dans le cadre unique de la Conférence internationale et privilégiant l'aspect humanitaire de la protection des civils et des acteurs médicaux et humanitaires dans les situations de conflit armé, la résolution se démarquera des efforts intergouvernementaux déployés dans les enceintes multilatérales, tout en les complétant.