



## **Power of humanity**

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

28–31 October 2024, Geneva

# **Proteggere i civili e altre persone e beni protetti dal potenziale costo umano delle attività ICT durante i conflitti armati**

RISOLUZIONE

Ottobre 2024

**IT**

**34IC/24/R2**  
**Originale: Inglese**  
**Adottata**

**RISOLUZIONE**

---

**Proteggere i civili e altre persone e beni protetti  
dal potenziale costo umano delle attività ICT  
durante i conflitti armati**

---

La 34a Conferenza Internazionale della Croce Rossa e della Mezzaluna Rossa (Conferenza Internazionale),

*riconoscendo* che un mondo sempre più digitalizzato e connesso offre opportunità nei settori sociale, economico, dello sviluppo, umanitario e delle tecnologie dell'informazione e della comunicazione, e può contribuire a salvare e migliorare vite umane, anche in situazioni di conflitto armato,

*sottolineando* l'importanza della connettività e delle tecnologie dell'informazione e della comunicazione (*information and communication technologies - ICT*) per la fornitura di una varietà di beni e servizi, compresi i servizi sanitari per la popolazione civile, per le operazioni umanitarie, per consentire ai civili di cercare e ricevere informazioni in un formato accessibile sui luoghi sicuri e i beni essenziali per la loro sopravvivenza, e per mantenere o ristabilire i legami familiari, anche in situazioni di conflitto armato,

*ricordando* che l'uso delle ICT nei futuri conflitti è sempre più probabile, e rilevando che le ICT sono già state utilizzate nei conflitti armati in diverse regioni,

*ricordando* la ratifica universale delle Convenzioni di Ginevra del 1949, e sottolineando la responsabilità primaria degli Stati nello sviluppo del diritto internazionale umanitario (DIU),

*riconoscendo* la Risoluzione 76/19 dell'Assemblea Generale delle Nazioni Unite e il lavoro degli Stati nell'ambito dell' *Open-Ended Working Group on Security of and in the Use of Information and Communication Technologies (OEWG)* per il periodo 2021-2025, e che la Prima Commissione dell'Assemblea Generale delle Nazioni Unite, in particolare l'OEWG 2021-2025, costituisce un forum intergovernativo centrale per studiare come il diritto internazionale si applichi all'uso delle ICT da parte degli Stati,

*ricordando* che la funzione della Conferenza Internazionale è contribuire al rispetto e allo sviluppo del DIU,

*esprimendo* preoccupazione per il fatto che l'uso doloso delle capacità ICT da parte delle parti in conflitto possa causare danni alla popolazione civile e ad altre persone e beni protetti, anche attraverso i confini internazionali, in particolare quando è diretto contro, o incidentalmente colpisce, le ICT che fanno parte di beni di carattere civile, inclusi oggetti indispensabili alla sopravvivenza della popolazione civile, opere e installazioni contenenti forze pericolose o infrastrutture critiche civili,

*esprimendo* ulteriore preoccupazione per il fatto che la mancanza di capacità adeguate di individuare e difendersi dalle attività ICT dolose possa rendere gli Stati e le componenti del Movimento Internazionale della Croce Rossa e della Mezzaluna Rossa (Movimento) più vulnerabili,

*notando* la portata, la velocità e la diffusione delle attività ICT dolose, in particolare attraverso le piattaforme dei social media, ed *esprimendo preoccupazione* per il fatto che ciò possa causare, istigare o amplificare danni alla popolazione civile o ad altre persone e beni protetti durante un conflitto armato, compreso quando le ICT sono utilizzate per reclutare bambini nelle forze armate,

*riconoscendo* che donne, uomini, ragazze e ragazzi di diverse età, con disabilità e provenienze differenti, possono essere colpiti in modo diverso dai conflitti armati, e che tali differenze devono essere considerate nell'attuazione e applicazione del DIU, al fine di garantire una protezione adeguata per tutti,

*riconoscendo* che l'intelligenza artificiale e altre tecnologie emergenti possono offrire benefici umanitari, sociali, economici o di sviluppo per la popolazione civile, ma *notando* al contempo con preoccupazione che l'uso di tali tecnologie nelle attività ICT dolose può amplificarne ulteriormente portata, velocità e danni,

*notando* che le ICT possono consentire o essere utilizzate per incoraggiare i civili a condurre o sostenere attività ICT nei conflitti armati, ed esprimendo preoccupazione per il fatto che i civili potrebbero non essere consapevoli dei rischi connessi o dei limiti e delle implicazioni giuridiche applicabili alla loro condotta,

*ricordando* che le aziende tecnologiche private forniscono una gamma di prodotti, servizi e infrastrutture ICT su cui fanno affidamento popolazioni civili, governi e organizzazioni umanitarie, anche durante i conflitti armati, *sottolineando* l'importanza della disponibilità e integrità di tali prodotti, servizi e infrastrutture per le popolazioni civili, e *ribadendo* l'importanza per le aziende tecnologiche private di considerare i bisogni di tutte le persone colpite dai conflitti armati, in conformità con le leggi applicabili,

*riconoscendo* che le ICT sono essenziali per delle operazioni umanitarie efficienti ed efficaci, ed *esprimendo* profonda preoccupazione per l'impatto che le attività ICT dolose possono avere sulle organizzazioni umanitarie, comprese le violazioni dei dati e la disinformazione che le prendono di mira, interrompendone le operazioni di soccorso, minando la fiducia nei loro riguardi, incluso nelle componenti del Movimento, mettendo a rischio la sicurezza e l'incolumità del loro personale, delle sedi e dei beni, e in ultima analisi il loro accesso e la loro capacità di svolgere attività umanitarie,

*ricordando* il valore giuridico e protettivo degli emblemi distintivi e dei segnali, e prendendo atto delle ricerche in corso sullo scopo, i parametri e la fattibilità di un emblema digitale condotte dal Comitato Internazionale della Croce Rossa (CICR), in collaborazione con istituzioni accademiche e altre componenti del Movimento,

*riaffermando* la Risoluzione 4, “*Restoring Family Links while respecting privacy, including as it relates to personal data protection*”, adottata dalla 33a Conferenza Internazionale, e *sottolineando* che le questioni affrontate in tale risoluzione sono rilevanti anche per la protezione di altri dati umanitari,

*prendendo atto* della Risoluzione 12, “*Safeguarding humanitarian data*”, adottata dal Consiglio dei Delegati nel 2022, e *accogliendo con favore* gli impegni del Movimento sulla protezione dei propri dati umanitari, anche per quanto riguarda il rafforzamento delle capacità, e *sottolineando* l'importanza della riservatezza, integrità e disponibilità dei dati per le operazioni umanitarie,

*ricordando* che gli Stati non devono adottare misure non conformi al diritto internazionale nell'uso delle ICT, in particolare alla Carta delle Nazioni Unite, compreso l'obbligo di risolvere le controversie internazionali con mezzi pacifici e il divieto della minaccia o dell'uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, o in qualsiasi altro modo incompatibile con gli scopi delle Nazioni Unite, *riaffermando* la convinzione che nulla nel DIU possa essere interpretato come legittimazione o autorizzazione di qualsiasi atto di aggressione o altro uso della forza incompatibile con la Carta delle Nazioni Unite, e *sottolineando* che il richiamo al DIU non legittima né incoraggia in alcun modo i conflitti,

*riconoscendo* che le specificità dell'ambiente ICT sollevano questioni su come i principi e le regole del DIU si applichino alle attività ICT in situazioni di conflitto armato e che gli Stati hanno espresso una diversità di opinioni su tali questioni, *sottolineando* la necessità di continuare le discussioni,

*sottolineando* che le persone e le infrastrutture critiche, così come le organizzazioni e il personale sanitario e umanitario, rischiano costantemente di subire danni causati dalle attività ICT, e *esortando* gli Stati a basarsi su questa risoluzione per adottare misure efficaci per la loro protezione, in linea con i quadri giuridici applicabili e con le loro attuali capacità in materia di ICT,

1. *esprime* l'impegno condiviso di tutti i membri della Conferenza Internazionale a proteggere la popolazione civile e altre persone e beni protetti in situazioni di conflitto armato, anche contro i rischi derivanti da attività ICT dolose;
2. *ricorda* che il DIU si applica solo alle situazioni di conflitto armato – inclusi i principi giuridici internazionali consolidati di umanità, necessità, proporzionalità e distinzione – e solo alle condotte che si verificano nel contesto di tale conflitto e sono associate allo stesso;
3. *riconosce* la necessità di ulteriori studi su come e quando tali principi si applicano all'uso delle ICT, *sottolinea* che il richiamo a tali principi non legittima né incoraggia in alcun modo i conflitti, ed *esorta* gli Stati a trovare un'intesa comune in tal senso;
4. *ribadisce* che, in situazioni di conflitto armato, le regole e i principi del DIU – tra cui il principio di distinzione, il divieto di attacchi indiscriminati e sproporzionati, l'obbligo di risparmiare la popolazione civile, i civili e i beni di carattere civile durante le operazioni militari, e di adottare tutte le precauzioni possibili per evitare, o comunque minimizzare, i danni incidentali ai civili, il divieto di incoraggiare o incitare a violazioni del DIU, e il divieto di atti o minacce di violenza il cui scopo principale sia diffondere il terrore tra la popolazione civile – servono a proteggere le popolazioni civili e altre persone e beni protetti, anche contro i rischi derivanti dalle attività ICT;

5. *esorta* le parti in conflitto a proteggere, in conformità con i loro obblighi giuridici internazionali, le infrastrutture critiche civili che forniscono servizi in diversi Stati, incluse le infrastrutture tecniche essenziali per la disponibilità generale o l'integrità di internet, compresi i cavi sottomarini e le reti di comunicazione orbitali;
6. *esorta* inoltre le parti in conflitto a rispettare e proteggere il personale sanitario, le unità e i trasporti, in conformità con i loro obblighi giuridici internazionali, anche in relazione alle attività ICT;
7. *esorta* gli Stati e le parti in conflitto a consentire e facilitare attività umanitarie imparziali durante i conflitti armati, incluse quelle che si basano sulle ICT, e a rispettare e proteggere il personale umanitario e i relativi beni in conformità con i loro obblighi giuridici internazionali, anche in relazione alle attività ICT;
8. *esorta* gli Stati e le parti in conflitto a proteggere le popolazioni civili e altre persone e beni protetti, inclusi i monumenti storici, le opere d'arte o i luoghi di culto che costituiscono il patrimonio culturale o spirituale dei popoli, in conformità con i loro obblighi giuridici internazionali, anche in relazione alle attività ICT;
9. *esorta* gli Stati, così come le componenti del Movimento ove opportuno e in conformità con i rispettivi mandati, a diffondere la conoscenza del DIU il più ampiamente possibile nei rispettivi Paesi, affinché i suoi principi possano essere conosciuti dall'intera popolazione, ed *esorta* gli Stati a prendere misure per prevenire e reprimere le violazioni del DIU, anche attraverso indagini e procedimenti giudiziari ove opportuno, in conformità con i loro obblighi giuridici internazionali, anche in relazione alle attività ICT;
10. *incoraggia* tutte le componenti del Movimento a considerare il rischio di danni che possono essere causati dalle attività ICT alla popolazione civile e ad altre persone e beni protetti, *esorta* tutte le componenti del Movimento a migliorare la loro preparazione e capacità di rispondere ai rischi derivanti da tali attività, incluso il modo in cui diversi gruppi di persone possono subire danni in modi differenti, ad esempio rafforzando le capacità per rilevare tali rischi e prevenire danni alle popolazioni civili, e *invita* gli Stati a sostenere il Movimento in questi sforzi;
11. *incoraggia* inoltre tutte le componenti del Movimento, ove appropriato e in conformità con i rispettivi mandati, a diffondere il DIU alle aziende tecnologiche private e a sensibilizzarle sul fatto che fornire servizi ICT a clienti che sono o potrebbero essere coinvolti in conflitti armati comporta determinati rischi, e a impegnarsi, ove opportuno, con queste aziende per incoraggiarle a considerare l'adozione di misure volte a proteggere le esigenze di tutte le persone colpite da conflitti armati, in conformità con il diritto internazionale e nazionale applicabile;
12. *incoraggia* il CICR a continuare a consultarsi e collaborare attivamente con gli Stati e le componenti del Movimento per: valutare ulteriormente e chiarire lo scopo specifico e la fattibilità tecnica di un emblema digitale; fornire, ove possibile, alle componenti del Movimento e agli Stati interessati attività di rafforzamento delle rispettive capacità per il suo potenziale utilizzo in relazione ai conflitti armati; e studiare possibili vie giuridiche e diplomatiche a questo riguardo;
13. *incoraggia* gli Stati e le componenti del Movimento a scambiare conoscenze e buone pratiche, a stabilire e rafforzare reti di contatto e comunicazione per promuovere la cooperazione internazionale, e a sviluppare capacità in materia di sicurezza ICT, protezione dei dati, diritto internazionale e protezione delle popolazioni civili e di altre persone e beni protetti dai rischi

derivanti da attività ICT dolose, tenendo conto dei diversi livelli di risorse a disposizione tra gli Stati e le componenti del Movimento.