El poder de la humanidad
XXXIV Conferencia Internacional
de la Cruz Roja y de la Media Luna Roja
28–31 de octubre de 2024, Ginebra

Prevención y minimización de las amenazas digitales contra las personas afectadas por conflictos armados

ELEMENTOS PRELIMINARES DE LA RESOLUCIÓN

Noviembre de 2023

ES

Original: inglés

Documento elaborado por el Comité Internacional de la Cruz Roja en consulta con la Federación Internacional de Sociedades de la Cruz Roja y de la Media Luna Roja

Público

ELEMENTOS PRELIMINARES DE LA RESOLUCIÓN

Prevención y minimización de las amenazas digitales contra las personas afectadas por conflictos armados

ANTECEDENTES

Los elementos preliminares de la resolución propuesta sobre prevención y minimización de las amenazas digitales contra las personas afectadas por conflictos armados exponen brevemente el posible contenido de los diferentes párrafos, sin ofrecer una formulación definitiva del texto. Luego de cada párrafo, se presentan los fundamentos que explican por qué sería útil incluirlo en la resolución.

Este documento se envía para consulta a los miembros del Consejo de Delegados del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja para recoger una primera ronda de comentarios, y tener una visión inicial acerca de si el enfoque propuesto sería aceptable y lograría consenso.

Para formular comentarios y observaciones sobre este documento, se ruega considerar las siguientes preguntas:

- ¿Está de acuerdo con los elementos propuestos para los párrafos del preámbulo y de la parte dispositiva de la resolución?
- ¿Considera que faltan elementos o que se debería agregar alguno?

No se espera recibir ahora comentarios detallados acerca de la redacción de los elementos preliminares. Más adelante, cuando esté disponible el anteproyecto de resolución, habrá oportunidad de comentar sobre aspectos específicos de la redacción.

INTRODUCCIÓN

La disponibilidad y la fiabilidad de la tecnología, la infraestructura (incluida la conectividad a internet) y los datos digitales son de suma importancia y pueden salvar vidas en situaciones de emergencia, especialmente en conflictos armados. Ayudan a la supervivencia de las personas afectadas porque, por ejemplo, les permiten saber dónde pueden conseguir alimentos, agua, mantas, un lugar seguro donde refugiarse, y también comunicarse o restablecer el contacto con familiares. Por otro lado, permiten que los gobiernos presten servicios básicos a la población y mantengan la gobernanza civil. La confidencialidad, la integridad y la disponibilidad de los datos y las tecnologías digitales también son esenciales para el funcionamiento de los servicios médicos -tanto militares como civiles- y forman parte integral de las actividades humanitarias, incluidas las del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (Movimiento).

La digitalización de los conflictos armados da lugar a nuevas amenazas para la vida, la seguridad y la dignidad de las personas civiles, el personal médico, el personal militar fuera

de combate y todos los que trabajan para prestarles protección y asistencia. Tanto los Estados como actores armados no estatales han utilizado métodos y medios de guerra digitales para superar a sus adversarios; y también se han usado métodos y medios de ese tipo para dejar infraestructura y servicios básicos fuera de funcionamiento, para incitar a la violencia contra la población civil, el personal médico y el personal militar fuera de combate, y para interrumpir las actividades médicas y humanitarias y socavar la confianza en estas. El uso malicioso de las tecnologías digitales alimenta los conflictos, erosiona la confianza y agrava las vulnerabilidades. El uso creciente de la inteligencia artificial en esas actividades puede agravar su escala e impacto.

El CICR, junto con sus socios del Movimiento, ha tenido un papel activo para evidenciar las amenazas que se plantean a la población civil, el personal médico y el personal militar fuera de combate a raíz de la digitalización de las operaciones militares. Además, se ha esforzado por entender y difundir el derecho internacional humanitario aplicable en los conflictos armados, incluidas las normas relativas a las operaciones cibernéticas y de información.

Además, el Movimiento ha promovido la comprensión de la protección de datos en las actividades humanitarias (v. "Manual sobre protección de datos en la acción humanitaria"), generado consenso internacional acerca de la importancia de proteger los datos en el contexto del restablecimiento del contacto entre familiares (v. XXXIII Conferencia Internacional, "Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos personales", y acordado medidas concretas con los miembros del Movimiento para la protección de los datos humanitarios (v. Consejo de Delegados de 2022, "Salvaguardar los datos humanitarios").

Los gobiernos han participado en foros de las Naciones Unidas sobre información y telecomunicaciones en el contexto de la seguridad internacional y la protección de los derechos humanos en el espacio digital.

El objetivo de la resolución propuesta para presentar en el foro humanitario único que ofrece la Conferencia Internacional de la Cruz Roja y de la Media Luna Roja es evidenciar el problema de las amenazas digitales contra la población civil, el personal médico y el personal militar fuera de combate, así como identificar medidas que los Estados y los miembros del Movimiento podrían adoptar para prevenirlas o minimizarlas.

Párrafos del preámbulo (PP)

PP 1
Este párrafo podría subrayar la importancia de la disponibilidad y la integridad de la tecnología, la infraestructura (incluida la conectividad a internet) y los datos digitales para la prestación de servicios esenciales (incluidos servicios médicos y humanitarios) a la población y a las personas civiles para que puedan buscar información sobre dónde hallar seguridad y bienes indispensables para la supervivencia y cómo mantener el contacto con familiares, en particular durante conflictos armados.

Fundamentos
Establecer una noción compartida acerca de la importancia de la tecnología, la infraestructura y los datos digitales para la vida, la seguridad y la dignidad de las personas afectadas por conflictos armados.

PP 2
Este párrafo podría recordar que los Estados están desarrollando capacidades digitales con fines militares, que esas capacidades se emplean en conflictos armados actuales y que su uso en futuros conflictos se está volviendo más probable. A la vez, podría expresar preocupación por el hecho de que esas tecnologías se utilizan para causar daño a la población y las personas civiles, el personal médico, el personal militar fuera de combate, los bienes de

carácter civil y otras personas y bienes protegidos, o causan esos daños incidentalmente, y por el riesgo de que esas capacidades causen daños superfluos y sufrimientos innecesarios.

Fundamentos
Reconocer los desarrollos militares en este ámbito y su potencial costo humano en situaciones de conflicto armado.

PP 3
Este párrafo podría expresar particular preocupación por el potencial costo humano causado por los efectos directos e indirectos de las ciberoperaciones que afectan la infraestructura civil, los servicios y los datos esenciales para la seguridad y la dignidad humanas y el funcionamiento de la sociedad.

Fundamentos
Reconocer el potencial costo humano de las ciberoperaciones.

PP 4
Este párrafo podría expresar particular preocupación por la escala, la velocidad y el alance de las operaciones de información digital y el daño que pueden causar al incitar a la violencia y al odio, generar tensiones y socavar la disponibilidad y la integridad de la información que las personas civiles necesitan para su seguridad y supervivencia en situaciones de conflicto armado.

Fundamentos
Reconocer el potencial costo humano de las operaciones de información.

PP 5
Este párrafo podría expresar preocupación por los civiles, en particular, los particulares, los grupos y las empresas que conducen ciberoperaciones u operaciones de información en relación con conflictos armados, y que esas operaciones exponen a los civiles a diversos daños y socavan el principio de distinción.

Fundamentos
Reconocer los riesgos que conlleva alentar o tolerar la participación de civiles en operaciones cibernéticas o de información en relación con conflictos amados.

PP 6
Este párrafo podría expresar preocupación por el hecho de que el uso militar de infraestructura digital civil, como los sistemas o las nubes de comunicación, podría convertirla en un objetivo militar, y por el impacto que los ataques contra esos objetivos tendrían en los civiles.

Fundamentos
Reconocer el riesgo que implica el uso de bienes de carácter civil con fines militares, ya que pueden convertirse así en objetivos militares y quedar expuestos a daños.

PP 7
Este párrafo podría expresar preocupación por el riesgo de que las ciberoperaciones, en particular las de carácter indiscriminado, conducidas en el contexto de un conflicto armado podrían afectar incidentalmente a las personas civiles fuera del territorio de las partes en conflicto debido a la interconexión mundial del ciberespacio.

Fundamentos
Reconocer el riesgo de que las ciberoperaciones se extiendan y dañen a personas civiles a través de las fronteras, sobre todo si los ataques son de carácter indiscriminado.

PP 8
Este párrafo podría recordar que las empresas tecnológicas ofrecen diversos productos, servicios e infraestructura de los que dependen las personas y los gobiernos, enfatizar su responsabilidad de respetar los derechos de las personas afectadas por conflictos armados y subrayar la importancia de incluir a las empresas tecnológicas en los debates sobre la protección de las personas civiles contra las amenazas digitales durante conflictos armados.

Fundamentos
Reconocer el papel particular que las empresas tecnológicas cumplen en la provisión de productos, servicios e infraestructura digitales, incluso durante conflictos armados.

PP 9
Este párrafo podría reconocer la importancia de la tecnología, la infraestructura (incluida la conectividad a internet) y los datos digitales para realizar actividades humanitarias eficientes y eficaces, y expresar profunda preocupación por el impacto que las ciberoperaciones, incluida la vulneración de datos, y las operaciones de información dirigidas contra organizaciones humanitarias podrían tener en las personas a las que prestan servicios estas organizaciones, las propias organizaciones y su personal.

Fundamentos
Reconocer la importancia de las tecnologías digitales, incluidos los datos, para las organizaciones humanitarias y los daños que causan los ataques contra ellas.

PP 10
Este párrafo preambular podría recordar el valor jurídico y protector de los emblemas y los símbolos distintivos, según corresponda, para identificar alas unidades y los medios de transporte sanitarios, al personal religioso y sanitario, así como a los miembros del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja que, por estar incluidos en los cuatro Convenios de Ginebra y la práctica continua a lo largo de 160 años, se han convertido en símbolos universalmente reconocidos de la ayuda imparcial y neutral y de la protección a las víctimas de conflictos armados y de otras emergencias. También podría destacar la investigación y las consultas realizadas por el CICR, en colaboración con instituciones académicas y con otros componentes del Movimiento, acerca de la factibilidad de un "emblema digital",[1] es decir, un medio digital para identificar la infraestructura y los datos digitales de las organizaciones y las entidades que están facultadas para exhibir los emblemas distintivos reconocidos por el derecho internacional humanitario.

Fundamentos
Recordar el papel de los emblemas distintivos conforme al derecho internacional humanitario y destacar la investigación y las consultas realizadas por el CICR acerca de un posible "emblema digital".

PP 11
Este párrafo podría recordar y reafirmar la resolución 4 "Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos personales", aprobada por la XXXIII Conferencia Internacional, y enfatizar que las cuestiones abordadas en esa resolución son importantes para la protección de otros datos humanitarios.

Fundamentos

[1] V. CICR, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions, 3 de noviembre de 2022.

Recordar y reafirmar el acuerdo alcanzado en la XXXIII Conferencia Internacional sobre la protección de los datos en la labor de restablecimiento del contacto entre familiares que realiza el Movimiento.

PP 12
Este párrafo podría tomar nota de la resolución 12, “Salvaguardar los datos humanitarios”, aprobada por el Consejo de Delegados celebrado en 2022, y acoger con satisfacción los compromisos contraídos por el Movimiento para proteger los datos humanitarios.

Fundamentos
Reconocer la labor iniciada en el Movimiento en materia de protección de los datos humanitarios.

PP 13
Este párrafo podría recordar la convicción de que ninguna disposición del derecho internacional humanitario, en particular las que se aplican a las operaciones cibernéticas o de información, pueden interpretarse de tal forma de legitimar o autorizar cualquier acto de agresión o cualquier otro uso de la fuerza incompatible con la Carta de las Naciones Unidas.

Fundamentos
Recordar la convicción compartida por los Estados tal como se la expresa en el preámbulo del Protocolo adicional I.

PP 14
Este párrafo podría enfatizar que las personas, así como las organizaciones médicas y humanitarias, también están expuestas a amenazas digitales en emergencias que no son conflictos armados, instar a los Estados a basarse en esta resolución para adoptar medidas eficaces para protegerlas de conformidad con los marcos jurídicos aplicables, y solicitar al Movimiento que adopte medidas apropiadas para favorecer la ciberseguridad y la protección de los datos en todo momento.

Fundamentos
Recordar la importancia de las amenazas digitales fuera de los conflictos armados y la necesidad de que los Estados y los componentes del Movimiento adopten medidas de protección fuera de los conflictos armados.

Párrafos dispositivos (PD)

PD 1
Este párrafo podría *enfatizar* el compromiso asumido por todos los miembros de la Conferencia Internacional para salvaguardar contra las amenazas digitales a las personas civiles y los bienes de carácter civil, así como a otras personas y bienes protegidos específicamente durante los conflictos armados.

Fundamentos
Expresar el objetivo humanitario compartido de proteger a las personas civiles y los bienes de carácter civil contra las amenazas digitales en situaciones de conflicto armado.

PD 2
Este párrafo podría reafirmar la importancia fundamental de las obligaciones que tienen todas las partes en conflicto en virtud del derecho internacional humanitario y de otros conjuntos de normas del derecho internacional, según sean aplicables, en particular, el derecho internacional de los derechos humanos, en relación con la protección contra las operaciones cibernéticas y de información de las personas civiles, los bienes de carácter civil y otras personas y bienes protegidos específicamente en situaciones de conflicto armado.

Fundamentos
Reafirmar el marco jurídico existente aplicable a las operaciones cibernéticas y de información en situaciones de conflicto armado.

PD 3
Este párrafo podría *instar* a todos los Estados y a todas las partes en conflictos armados a garantizar que el derecho internacional humanitario sea aplicado de forma tal que confiera protección adecuada a las personas civiles, el personal médico, el personal militar fuera de combate, la infraestructura civil y los datos, así como a otras personas y bienes específicamente protegidos en sociedades cada vez más digitalizadas; *exigir respeto* por las normas aplicables; y *urgir* a todos los Estados y a otros actores que desarrollan capacidades cibernéticas y de información a que adopten a nivel interno las necesarias medidas legislativas, administrativas y prácticas a fin de implementar sus obligaciones jurídicas.

Fundamentos
Instar a todos los Estados y a todas las partes en conflictos armados a conferir la adecuada protección contra las amenazas digitales e instar a que se implementen las normas jurídicas aplicables.

PD 4
Este párrafo podría *instar* a todos los Estados y partes en conflictos armado a respetar, en particular, el principio cardinal de distinción que establece el derecho internacional humanitario a fin de proteger a las personas civiles contra los peligros de las hostilidades, en especial cuando conducen operaciones cibernéticas y de información; enfatizar que están prohibidas las capacidades cibernéticas que reúnen las condiciones para ser consideradas como armas y que, por su naturaleza, tienen efectos indiscriminados; y subrayar la prohibición de los ataques directos contra las personas civiles y los bienes de carácter civil; de los actos o amenazas de violencia que tengan como objetivo principal sembrar el terror entre la población civil; de los ataques indiscriminados y desproporcionados; de atacar, destruir, eliminar o inutilizar los bienes indispensables para la supervivencia de la población; de la perfidia y de otros usos indebidos de los emblemas, símbolos, banderas, uniformes e insignias específicamente protegidos, incluso cuando se utilizan métodos y medios de guerra digitales; y *recordar* las obligaciones de preservar constantemente a la población civil y a los bienes de carácter civil y de adoptar todas las medidas de precaución posibles para evitar o, al menos, reducir lo más posible los daños causados incidentalmente a las personas civiles y proteger a la población civil y los bienes de carácter civil bajo su control contra los efectos de los ataques, incluso cuando emplean métodos y medios de guerra digitales.

Fundamentos
Reafirmar algunas de las normas básicas del derecho internacional humanitario que protegen a las personas civiles contra las amenazas digitales en situaciones de conflicto armado.

PD 5
Este párrafo también podría *instar* a los Estados y a las partes en conflictos armados a que cumplan la obligación que tienen en virtud del derecho internacional humanitario de respetar y proteger al personal, las unidades y los medios de transporte sanitarios en todas las circunstancias, incluso contra las operaciones cibernéticas y de información.

Fundamentos
Reafirmar la protección jurídica internacional específica del personal, las unidades y los medios de transporte sanitarios contra las amenazas digitales en situaciones de conflicto armado.

PD 6
Este párrafo podría *instar asimismo* a los Estados y a las partes en conflictos armados a respetar las obligaciones que tienen en virtud del derecho internacional humanitario de permitir y facilitar las actividades humanitarias imparciales en situaciones de conflicto armado, incluidas las que se realizan por medios digitales, así como a respetar y proteger al personal y las actividades humanitarias, incluso contra las operaciones cibernéticas y de información.

Fundamentos
Reafirmar la protección jurídica internacional específica de las organizaciones humanitarias imparciales contra las amenazas digitales durante los conflictos armados.

PD 7
Este párrafo podría *recordar* que, cuando las partes en un conflicto armado alientan la participación de civiles en las hostilidades, incluso empleando medios digitales, los civiles corren el riesgo de perder su protección jurídica contra los ataques o de que se perciba que la han perdido, e *instar* a las partes a tener esto presente y adoptar todas las medidas de precaución posibles para evitar exponer a los civiles a sufrir daños.

Fundamentos
Reconocer los riesgos que conlleva fomentar la participación de civiles en las hostilidades, e instar a adoptar todas las medidas de precaución posibles para proteger a los civiles.

PD 8
Este párrafo podría *enfatizar* que los actores no estatales, incluidos los civiles y los grupos armados no estatales, que conducen ciberoperaciones en relación con un conflicto armado deben cumplir el derecho internacional humanitario, cualquiera sea su estatuto; *reafirmar* el compromiso de los Estados de adoptar medidas para garantizar que los actores no estatales que operan bajo las instrucciones, la dirección o el control de un Estado, o desde su territorio, no conduzcan operaciones en violación del derecho internacional humanitario, y supriman las posibles violaciones de este derecho, y *alentar* al CICR y a las Sociedades Nacionales de la Cruz Roja y de la Media Luna Roja renueven sus esfuerzos para difundir el conocimiento del derecho internacional humanitario.

Fundamentos
Reafirmar el papel principal de los Estados para garantizar el respeto del derecho internacional humanitario por los actores no estatales, y reconocer el papel estatutario del Movimiento en lo que respecta a la difusión del derecho internacional humanitario.

PD 9
Este párrafo podría *recordar* que las empresas tecnológicas que operan en contextos afectados por conflictos armados o prestan servicios en relación con estos deben comprender y considerar las consecuencias de sus actividades en virtud del derecho internacional humanitario, tomar las medidas necesarias para que su personal cumpla las obligaciones pertinentes y adoptar las medidas adecuadas para proteger contra todo daño posible a su personal y a los civiles que empleen sus productos y servicios.

Fundamentos
Instar a las empresas tecnológicas a invertir en comprender las consecuencias de sus actividades en situaciones de conflicto armado y a adoptar las medidas necesarias para proteger a la población civil.

PD 10
Este párrafo podría alentar a los Estados a segmentar, es decir, separar física o técnicamente, en la medida posible, la infraestructura digital utilizada con fines militares de la infraestructura civil, reconociendo que el uso de la infraestructura civil con fines miliares puede convertirla en

un objetivo militar, lo que podría tener efectos perjudiciales para los civiles que también la utilicen.

Fundamentos
Alentar a los Estados a segmentar, en la medida posible, la infraestructura digital utilizada con fines militares de la infraestructura utilizada con fines civiles.

PD 11
Este párrafo podría *alentar* a todos los miembros del Movimiento, como parte de su labor, a considerar las amenazas digitales y los daños que pueden provocar, *urgir* a todos los miembros a mejorar su preparación y capacidad para responder a las amenazas digitales contra los civiles, por ejemplo, fortaleciendo la capacidad de detectar amenazas y de realizar actividades de protección de la población civil, e *invitar* a los Estados a apoyar al Movimiento en estos esfuerzos.

Fundamentos
Alentar al Movimiento a fortalecer su capacidad de responder a las amenazas digitales e invitar a los Estados a apoyar la inversión necesaria y el fortalecimiento de la capacidad en este aspecto.

PD 12
Este párrafo podría *destacar* el resultado de la investigación en curso sobre un emblema digital y su puesta a prueba, y *alentar* al CICR a que, en consulta con los Estados y los componentes del Movimiento, proponga una solución técnica, integral y duradera y presente opciones para que los Estados la incorporen en el derecho internacional humanitario.

Fundamentos
Invitar al CICR a continuar trabajando en torno a un emblema digital, en estrecha colaboración con los Estados y el Movimiento.

PD 13
Este párrafo podría *comprometer* a los componentes del Movimiento a adoptar las medidas necesarias, dentro de sus mandatos, capacidades y necesidades operacionales respectivos, a fortalecer su capacidad de garantizar el nivel adecuado de ciberseguridad y protección de los datos; a aplicar las mejores prácticas en materia de gestión de datos para todos los datos humanitarios; a implementar los criterios y las buenas prácticas pertinentes en el procesamiento de datos personales, tomando en consideración el Manual sobre protección de datos en la acción humanitaria; y a cumplir el derecho aplicable y los marcos de protección de datos personales pertinentes, y *expresar* el apoyo de los Estados a estas medidas.

Fundamentos
Comprometer al Movimiento a adoptar medidas adecuadas de ciberseguridad y protección de datos para proteger a la población a la que prestan servicios.

PD 14
Este párrafo podría *recordar* que el procesamiento de datos personales es necesario para que los componentes del Movimiento cumplan sus obligaciones, sobre todo en virtud del derecho internacional humanitario, de ser aplicable, y de los Estatutos del Movimiento, que ese procesamiento contribuye a y es necesario por importantes motivos de interés público y el interés vital de las personas, y podría *urgir* a los Estados y al Movimiento a que cooperen para garantizar que no se soliciten ni utilicen datos personales para fines incompatibles con el carácter humanitario de la labor del Movimiento y, de conformidad con el artículo 2, especialmente el párrafo 5, de los Estatutos del Movimiento, o de alguna forma que podría cercenar la confianza de las personas a las que presta servicios o la independencia, la imparcialidad y la neutralidad de las actividades del Movimiento.

Fundamentos
Destacar la importancia del procesamiento de datos en la labor humanitaria del Movimiento y la cooperación de los Estados para que los componentes del Movimiento puedan cumplir sus cometidos respectivos.

PD 15
Este párrafo podría *invitar* al CICR a continuar evaluando las amenazas digitales en situaciones de conflicto armado y la protección de los civiles contra estas, en particular conforme al derecho internacional humanitario, e informar al respecto en la XXXV Conferencia Internacional.

Fundamentos
Invitar al CICR a informar sobre el tema de esta resolución en la próxima Conferencia Internacional.