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

Protección de la población civil y de otras personas y bienes protegidos ante operaciones cibernéticas y de información durante los conflictos armados

DOCUMENTO DE ANTECEDENTES

Abril de 2024

ES
CD/24/XX
Original: inglés
Para información

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

DOCUMENTO DE ANTECEDENTES

Protección de la población civil y de otras personas y bienes protegidos ante operaciones cibernéticas y de información durante los conflictos armados

RESUMEN

La presente resolución procura abordar algunos de los peligros que enfrentan la población civil y otras personas y bienes protegidos ante las operaciones cibernéticas y de información en situaciones de conflicto armado. Pretende generar conocimientos compartidos sobre las oportunidades que ofrece la existencia y la fiabilidad de las tecnología de la información y la comunicación (TIC) durante los conflictos armados, y sobre los peligros que entraña el uso de las TIC en operaciones cibernéticas y de información, e identificar medidas específicas para hacer frente a algunos de esos peligros. La resolución insta a los Estados y a los componentes del Movimiento Internacional de la Cruz Roja y de la Media Luna Roja (Movimiento) a adoptar medidas destinadas a alcanzar esos fines.

La existencia y la fiabilidad de las TIC ofrecen oportunidades en los ámbitos social, económico, de desarrollo y de la información y la comunicación. En tiempo de conflicto armado, las TIC pueden mejorar y salvar vidas. Por ejemplo, las TIC permiten que las personas sobrevivan buscando dónde pueden obtener alimentos, agua y mantas o encontrar un lugar seguro, y les permite contactar y localizar a familiares de los que no han tenido noticias. Al mismo tiempo, el uso de las TIC con finalidad militar durante un conflicto armado puede dar lugar a nuevos peligros para la vida, la seguridad y la dignidad de la población civil y de otras personas y bienes protegidos. De especial interés son las operaciones cibernéticas y de información que se dirigen contra poblaciones civiles y otras personas y bienes protegidos, en particular, las que se dirigen a los establecimientos sanitarios y las operaciones humanitarias que entrañan peligros específicos.

A fin de abordar algunos de esos peligros, la resolución recuerda el consenso entre los Estados respecto de que el derecho internacional humanitario es aplicable solo en situaciones de conflicto armado, a la vez que reconoce la necesidad de continuar analizando cómo y cuándo se aplica el DIH al uso de las TIC, por ejemplo, en el caso de las operaciones cibernéticas y de información. A continuación, la resolución recuerda algunas de las normas y principios esenciales del DIH sobre la protección de la población civil, exige su implementación efectiva e insta a los Estados a cumplir sus obligaciones de respetar y proteger al personal, las unidades y los transportes (es decir, los vehículos) sanitarios en todas las circunstancias y permitir y facilitar, así como respetar y proteger, las actividades de socorro humanitario. En este contexto, la resolución propone invitar a los Estados y a los componentes del Movimiento a hacer suya la investigación encabezada por el Comité Internacional de la Cruz Roja (CICR) –en consulta con expertos externos y los otros componentes del Movimiento– sobre la factibilidad de un "emblema digital", y alienta a continuar trabajando en torno a este tema.

La resolución también recuerda la responsabilidad de los componentes del Movimiento de adoptar las medidas necesarias, dentro del alcance de sus respectivos cometidos, capacidades y necesidades operacionales, para mejorar su capacidad de mantener los niveles adecuados de ciberseguridad y protección de datos.

1) INTRODUCCIÓN

La existencia y la fiabilidad de las tecnologías de la información y la comunicación (TIC) ofrecen oportunidades en los ámbitos social, económico, de desarrollo y de la información y la comunicación, y pueden salvar y mejorar vidas. Por ejemplo, durante un conflicto armado, las TIC permiten que las personas sobrevivan buscando dónde pueden obtener alimentos, agua y mantas o un lugar seguro, y les permite contactar y localizar a familiares de los que no han tenido noticias. Las TIC también tienen el potencial de permitir que las organizaciones humanitarias envíen socorros humanitarios con mayor eficacia, y pueden permitir que los beligerantes, por ejemplo, den avisos por medios eficaces y mejoren los medios de reconocimiento para la protección de las personas civiles. Asimismo, el uso de las TIC con finalidad militar durante un conflicto armado puede dar lugar a nuevos peligros para la vida, la seguridad y la dignidad de la población civil y de otras personas y bienes protegidos.

El CICR, junto con los socios del Movimiento, ha sido pionero en la investigación y en la consulta con expertos sobre los posibles costos humanos de las operaciones cibernéticas y de información durante los conflictos armados. Reconociendo esos riesgos, y en consonancia con nuestro mandato, el CICR trabaja para que se entienda y se difunda el conocimiento del DIH, entre otros aspectos, en relación con los nuevos medios y métodos de guerra. Los Estados han debatido el tema de las TIC en foros de las Naciones Unidas en el contexto de la seguridad internacional y la protección de los derechos humanos. Desde 2019, el Movimiento presta cada vez más atención a los riesgos relacionados con la protección de datos, en particular, la vulneración de datos, en las operaciones humanitarias.

La resolución propuesta, que se presentará ante un foro humanitario único como la Conferencia Internacional de la Cruz Roja y de la Media Luna Roja (Conferencia Internacional), tiene por finalidad llamar la atención sobre la necesidad de proteger a las poblaciones civiles y a otras personas y bienes protegidos ante operaciones cibernéticas y de información, e identificar las medidas que los Estados y los miembros del Movimiento pueden adoptar a fin de prevenir o minimizar los daños.

2) CONTEXTO

La resolución propuesta será la primera en que la Conferencia Internacional trate el uso de las capacidades de las TIC durante los conflictos armados, en particular, las operaciones cibernéticas y de información. Se basará en resoluciones de la Conferencia Internacional y el Consejo de Delegados sobre protección de datos, así como en informes realizados por el CICR, con la colaboración de expertos de todas partes del mundo, sobre la protección de las personas civiles contra las amenazas digitales.

En lo que respecta a la protección de los datos humanitarios, la resolución propuesta aspira a tomar como base la resolución "Restablecimiento del contacto entre familiares en un marco de respeto de la privacidad, incluso en materia de protección de los datos personales", aprobada en la XXXIII Conferencia Internacional, celebrada en 2019, así como las medidas acordadas por los componentes del Movimiento en la resolución "Salvaguardar los datos humanitarios", aprobada en el Consejo de Delegados reunido en 2022. El *Manual sobre protección de datos en la acción humanitaria* también puede ser de interés.

Con respecto al posible costo humano de las operaciones cibernéticas y de información, y las medidas prácticas que deberían tener en cuenta los Estados y las organizaciones humanitarias, el CICR desearía que las delegaciones prestaran atención, en particular, al informe publicado en 2023 por su consejo consultivo mundial acerca de las amenazas digitales durante conflictos armados (en inglés). El consejo consultivo reunió a un grupo mundial de referentes jurídicos, militares y tecnológicos, así como del ámbito de las políticas. El informe contiene cuatro principios rectores y 25 recomendaciones específicas para los beligerantes, los Estados, las empresas tecnológicas y las organizaciones humanitarias,

destinadas a prevenir o mitigar las amenazas digitales para la población civil[1]. Como en la resolución propuesta también se trata el tema de un posible "emblema digital", el informe *Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks and Possible Solutions* puede ser de particular interés.

3) ANÁLISIS/PROGRESOS

En lugares afectados por conflictos armados y otras situaciones de emergencia, las personas suelen depender de la existencia y la fiabilidad de las TIC para acceder a bienes y servicios que son fundamentales para su supervivencia y bienestar. Las TIC permiten a los Gobiernos prestar servicios esenciales a la población y mantener la gobernanza ciudadana. La confidencialidad, la integridad y la disponibilidad de TIC, y de los datos de los que dependen, también son fundamentales para el funcionamiento de los servicios de salud –tanto militares como civiles– y son elementos cada vez más importantes de las operaciones humanitarias, incluso las que emprende el Movimiento. Además, las TIC se usan actualmente como medio o método de guerra, en particular, en forma de operaciones cibernéticas y de información. Esta realidad trae aparejados interrogantes y desafíos para la protección de poblaciones afectadas por conflictos y para la acción humanitaria basada en principios.

A) Peligros para la población civil causados por operaciones cibernéticas y de información

Las observaciones realizadas en conflictos armados contemporáneos y la investigación y las consultas antes mencionadas han permitido identificar cuatro tipos de peligros que son especialmente relevantes, debido a su probabilidad y a su potencial impacto negativo en las personas civiles.

Operaciones cibernéticas
Cuanto más depende nuestra vida cotidiana de las TIC, mayor es el riesgo de que el uso de operaciones cibernéticas durante un conflicto armado cause daños a la población civil. Las operaciones cibernéticas tienen el potencial de inhabilitar o dañar físicamente establecimientos industriales, redes de comunicación y otros componentes de la infraestructura crítica de un Estado en formas que podrían causar daños directa o indirectamente, y provocar lesiones o la muerte de personas civiles, incluso por impedir el funcionamiento adecuado de los servicios esenciales. Las operaciones cibernéticas ideadas para manipular información podrían tener consecuencias similares, incluso mediante el robo, la filtración, la manipulación o la eliminación de datos. Debido a la interconectividad que caracteriza al ciberespacio, existe un riesgo real de que las operaciones cibernéticas –cuando se las diseña intencionalmente o cuando no se las somete a pruebas o controles adecuados– afecten indiscriminadamente sistemas informáticos de uso generalizado e infraestructura civil lejos del escenario del conflicto, causen directa o indirectamente daños, lesiones o la muerte a personas civiles, y provoquen una escalada del conflicto.

Operaciones de información
Las operaciones de información no son ninguna novedad en los conflictos armados. Están permitidas en determinadas circunstancias, por ejemplo, para alertar a las personas civiles sobre ataques militares o para engañar al adversario respetando el derecho internacional. Hoy en día, la digitalización ha incrementado la magnitud, la velocidad y el alcance de esas operaciones. En superposición con la desinformación, y a veces como desinformación propiamente dicha (entendida comúnmente como información falsa o manipulada con la intención de causar daño), las operaciones de información se difunden por múltiples ecosistemas y plataformas: distorsionan hechos, ejercen influencia en las creencias y comportamientos de las personas, aumentan las tensiones y el riesgo de que se causen daños

[1] Otras publicaciones del CICR que pueden ser de interés son *The Potential Human Cost of Cyber Operations*, de 2019; *Avoiding Civilian Harm from Military Cyber Operations During Armed Conflicts*, de 2021; y *Harmful Information:Misinformation, Disinformation and Hate Speech in Armed Conflict and Other Situations of Violence*, de 2021.

a las personas civiles promoviendo la desconfianza y fomentando el odio. En particular, estas operaciones pueden afectar, en particular, a las mujeres, los niños, las niñas y las minorías que están en situación de vulnerabilidad. Asimismo, la información dañina puede afectar negativamente la disponibilidad, la integridad y la fiabilidad de información fundamental necesaria para la seguridad y la supervivencia de las personas civiles en tiempo de conflicto armado. Comparadas con los medios tradicionales, las plataformas digitales no suelen contar con la supervisión editorial necesaria ni con la capacidad de moderar contenidos, por lo que la información dañina se difunde con mayor facilidad. Las personas civiles también pueden difundir contenido dañino sin tener conciencia de ello, con lo que se amplifica su potencial alcance e impacto.

Personas civiles involucradas en operaciones cibernéticas y de información
Desde hace tiempo, las personas civiles –como individuos, en grupos o como parte de empresas– desempeñan funciones militares durante los conflictos armados y participan en las iniciativas de guerra. Con la digitalización de la sociedad, están aumentando los tipos de operaciones que pueden realizar y la cantidad de actores civiles que participan en los conflictos armados. Estos cambios traen aparejados riesgos para la población civil a los que no siempre se les presta atención: cuanto mayor sea la participación de personas civiles en las hostilidades, mayor será el riesgo de daños al que se expongan. A mayor cantidad de infraestructura o servicios digitales compartidos entre la población civil y las fuerzas armadas, mayor riesgo de que sea atacada la infraestructura civil.

Operaciones cibernéticas y de información dirigidas contra establecimientos sanitarios y organizaciones humanitarias
Desde hace varios años, el CICR tiene la preocupación de que, a medida que aumenta la digitalización, los establecimientos sanitarios se vuelven más vulnerables a las operaciones cibernéticas y a los daños incidentales causados por las operaciones de ese tipo dirigidas a otros objetivos. También están surgiendo nuevos peligros debido a la desinformación que se difunde por medios digitales cuyo objetivo es socavar la labor vital de los servicios médicos y que pone en riesgo al personal sanitario. El potencial costo humano de las operaciones cibernéticas y de información es mayor durante los conflictos armados y otras situaciones de emergencia, cuando la necesidad de contar con servicios médicos es más apremiante.

En una época caracterizada por una gran cantidad de personas afectadas y una capacidad de respuesta insuficiente, las operaciones cibernéticas y de información contra las organizaciones humanitarias pueden tener consecuencias devastadoras para las poblaciones que necesitan su protección y asistencia para sobrevivir. En los últimos años, los componentes del Movimiento se han convertido en víctimas de esas operaciones. Las operaciones cibernéticas y de información pueden adoptar diferentes formas, desde operaciones cibernéticas que destruyen o interrumpen el funcionamiento de la infraestructura digital de las organizaciones humanitarias y operaciones que se infiltran en sus sistemas para acceder a sus datos, hasta operaciones de desinformación que debilitan su reputación y ponen en peligro su capacidad de trabajo.

Tanto para los actores sanitarios como para los humanitarios, la vulneración de datos no solo pone en riesgo la vida y los medios de supervivencia, sino que además debilita la confianza que la población civil y las partes en conflictos armados depositan en ellos, lo que afecta su acceso a las personas y puede poner en riesgo la seguridad de su personal.

B) Respuesta colectiva del Movimiento y los Estados Partes en los Convenios de Ginebra

Para dar respuesta a los peligros mencionados, la resolución propuesta persigue dos objetivos principales.

En primer lugar, en los párrafos del preámbulo, pretende crear un conocimiento común de algunos de los riesgos de que las operaciones cibernéticas y de información causen daños a la población civil y a otras personas y bienes protegidos durante los conflictos armados. La resolución pone de relieve el riesgo de operaciones cibernéticas que interrumpen el funcionamiento de las TIC que forman parte de la infraestructura civil crítica y los servicios esenciales o que son usadas por éstos; de operaciones de información que incitan a la violencia y el odio en violación del DIH; los peligros específicos que las operaciones cibernéticas y de información causan a los servicios sanitarios y las operaciones humanitarias, incluidos sus datos; y los desafíos y los riesgos que surgen cuando se alienta a los civiles a conducir –o se tolera que conduzcan– operaciones cibernéticas y de información durante conflictos armados.

En segundo lugar, en los párrafos dispositivos, la resolución recuerda el consenso entre los Estados respecto de que el DIH solo es aplicable en situaciones de conflicto armado, y el reconocimiento de la necesidad de continuar analizando cómo y cuándo se aplica el DIH al uso de las TIC, por ejemplo, en las operaciones cibernéticas y de información. A continuación, la resolución recuerda algunas de las normas y principios esenciales del DIH sobre la protección de la población civil, exige su implementación efectiva e insta a los Estados a cumplir sus obligaciones de respetar y proteger al personal, las unidades y los transportes (es decir, los vehículos) sanitarios, en todas las circunstancias, y de permitir y facilitar, así como de respetar y proteger, las actividades y el personal de socorro humanitario. Asimismo, la resolución alienta a todos los componentes del Movimiento a integrar la protección de la población civil y de otras personas y bienes protegidos durante los conflictos armados en su trabajo operacional, jurídico y de políticas, y a adoptar las medidas necesarias, dentro del alcance de sus respectivos cometidos, capacidades y necesidades operacionales, para mejorar su capacidad de mantener los niveles adecuados de ciberseguridad y protección de datos en todas sus áreas de actividad. En este sentido, la resolución invita a colaborar con los Estados y a lograr su apoyo.

Una forma de mejorar la protección de las actividades humanitarias y de asistencia de salud ante los peligros que entrañan las operaciones cibernéticas y de información puede consistir en que el CICR conduzca investigaciones sobre un posible “emblema digital”; esto es, un medio digital de identificación de la infraestructura y los datos de las organizaciones y las entidades que tienen derecho a desplegar los emblemas distintivos reconocidos en el derecho internacional humanitario. En este sentido, la resolución acoge con satisfacción el trabajo realizado hasta ahora por el Movimiento y en consulta con Estados y otros expertos, y alienta a continuar trabajando en torno a este tema.

4) RECURSOS NECESARIOS

Al aprobar la resolución, los Estados y los componentes del Movimiento se comprometen a adoptar las medidas necesarias, dentro del alcance de sus respectivos cometidos, capacidades y operaciones, para mejorar la protección de la población civil y de otras personas y bienes protegidos durante los conflictos armados. La resolución también exige que los componentes del Movimiento adopten las medidas necesarias para mejorar su capacidad de garantizar los niveles adecuados de ciberseguridad y protección de datos. Además, alienta al CICR a continuar con sus investigaciones y pruebas, en consulta con los Estados y los componentes del Movimiento, a fin de conocer la factibilidad técnica de un emblema digital.

Para implementar esos compromisos, puede ser necesario que los Estados o los componentes del Movimiento empleen determinados recursos, de acuerdo con sus legislaciones, políticas, programas y actividades actuales.

5) IMPLEMENTACIÓN Y SEGUIMIENTO

El éxito de esta resolución depende de que los Estados y los componentes del Movimiento incorporen las medidas acordadas en su propia legislación, políticas, programas y actividades. De los Estados se espera que se ocupen de esta cuestión como parte de su implementación del DIH y de las políticas de protección de la población civil. De los componentes del Movimiento se espera que implementen las partes pertinentes de la resolución en lo que respecta a la seguridad de los datos y la protección de los datos personales, dentro de lo viable y apropiado, así como a la difusión del conocimiento del DIH.

Todos los miembros de la Conferencia Internacional están invitados a informar a la próxima Conferencia Internacional sobre los avances logrados en la implementación de esta resolución.

6) CONCLUSIONES Y RECOMENDACIONES

En el año del 75.º aniversario de la aprobación de los cuatro Convenios de Ginebra, la presente resolución pretende abordar las realidades cambiantes de los conflictos armados. Aspira a crear un conocimiento común e identificar medidas específicas para abordar algunas de las amenazas que plantean las operaciones cibernéticas y de información para la población civil y otras personas y bienes protegidos durante los conflictos armados. Insta a los Estados y a los componentes del Movimiento a adoptar medidas a tal efecto, dentro del alcance de sus respectivas responsabilidades.

La aprobación de esta resolución constituirá un hito en las iniciativas internacionales actuales destinadas a garantizar que el uso de las TIC contribuya al bienestar de las personas. Pondrá el foco específicamente en las necesidades de protección de las personas afectadas por los conflictos armados. Al ser aprobada en un foro excepcional como el de la Conferencia Internacional y al centrarse en el interés humanitario específico de proteger a las personas civiles y a los actores sanitarios y humanitarios en situaciones de conflicto armado, la resolución se destacará entre los esfuerzos intergubernamentales de los foros multilaterales a la vez que los complementará.