CICR

Derecho internacional humanitario y ciberoperaciones durante conflictos armados

Documento de posición del CICR

Dirigido al Grupo de trabajo de composición abierta sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, y al Grupo de expertos gubernamentales sobre la Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional.

Noviembre de 2019

Índice

Resumen

- **Las ciberoperaciones se han vuelto una realidad de los conflictos armados contemporáneos.** Al Comité Internacional de la Cruz Roja (CICR) le preocupa el **posible costo humano** del aumento del recurso a las ciberoperaciones en esos contextos.
- **Desde la perspectiva del CICR, el derecho internacional humanitario (DIH) limita las ciberoperaciones durante los conflictos armados,** de la misma manera que limita, en ese marco, el empleo de todas las armas, medios o métodos de guerra, sean nuevos o tradicionales.
- Afirmar que el DIH es aplicable a la guerra cibernética no la legitima, de la misma manera que tampoco legitima ninguna otra forma de guerra. **Todo uso de la fuerza —de forma cibernética o cinética— por parte de los Estados se rige por la Carta de las Naciones Unidas y las normas correspondientes del derecho internacional consuetudinario**, en particular, la prohibición del uso de la fuerza. Los litigios internacionales deben resolverse por vías pacíficas, tanto para el ciberespacio como para todas las demás esferas.
- Se ha vuelto sumamente importante para la **comunidad internacional afirmar la aplicabilidad del DIH** al recurso a las ciberoperaciones durante conflictos armados**.** El CICR insta a que se mantengan **diálogos entre expertos gubernamentales y no gubernamentales sobre la manera en que se aplican las normas vigentes del DIH** y si el derecho que rige es adecuado y suficiente. En este sentido, **acogemos con beneplácito los debates intergubernamentales** que tienen lugar en este momento en el marco de dos procesos encomendados por la Asamblea General de las Naciones Unidas.
- En los últimos años, han ocurrido sucesos que ponen de relieve que las ciberoperaciones, dentro o fuera de los conflictos armados, pueden alterar el funcionamiento de infraestructuras civiles esenciales y obstaculizar la prestación de servicios fundamentales a la población. **En el contexto de los conflictos armados, la infraestructura civil está protegida de los ciberataques gracias a los principios y las normas vigentes del DIH**, en particular, los principios de distinción, proporcionalidad y precauciones en el ataque. Además, el DIH otorga protección especial, por ejemplo, a hospitales y bienes indispensables para la supervivencia de la población civil.
- **Durante los conflictos armados, está prohibido el empleo de herramientas cibernéticas que ocasionan y propagan daños de manera indiscriminada.** Desde una perspectiva tecnológica, es posible diseñar y utilizar algunas herramientas cibernéticas para atacar determinados bienes de manera específica y no para propagar ni ocasionar perjuicio indiscriminadamente. Sin embargo, dada la interconectividad que caracteriza al ciberespacio, todo lo que esté conectado a internet es susceptible de ser señalado como objetivo desde cualquier parte del mundo, y un ciberataque contra un sistema específico puede tener consecuencias para varios sistemas más. Por lo tanto, existe un riesgo real de que las herramientas cibernéticas no se diseñen de conformidad con el DIH, ya sea de manera deliberada o por error.

- **La interpretación que hacen los Estados de las normas vigentes del DIH determinará en qué medida esta rama del derecho protege de los efectos de las ciberoperaciones.** En particular, los Estados deben asumir posiciones claras respecto de su compromiso de interpretar el DIH de manera tal que se preserve la infraestructura civil de alteraciones considerables y queden protegidos los datos de carácter civil. La existencia de esas posiciones también ayudará a determinar si las normas vigentes son idóneas o si se necesitan nuevas. Si los Estados ven la necesidad de formular legislación nueva, deben **partir de la base del marco jurídico vigente —incluido el DIH— y fortalecerlo.**

I. Introducción

Las operaciones cibernéticas (o ciberoperaciones) durante los conflictos armados son una realidad[1]. Si bien solo algunos han reconocido públicamente que llevan adelante ese tipo de operaciones, un número creciente de Estados están desarrollando capacidades cibernéticas militares, cuyo uso es probable que aumente en el futuro.

Además, se han producido avances tecnológicos significativos en las capacidades cibernéticas ofensivas: en los últimos años, han tenido lugar sucesos que demuestran que las ciberoperaciones pueden afectar profundamente la infraestructura civil y resultar en daños a las personas.

En consonancia con su misión y su cometido, el Comité Internacional de la Cruz Roja (CICR) se preocupa, ante todo, por el recurso a las ciberoperaciones como medios y métodos de guerra durante conflictos armados, así como por la protección que otorga el DIH contra sus efectos.

Nuestra institución acoge con beneplácito los debates intergubernamentales que se mantienen actualmente en el marco de los dos procesos encomendados por la Asamblea General de las Naciones Unidas: el Grupo de trabajo de composición abierta sobre los Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional, y el Grupo de expertos gubernamentales sobre la Promoción del comportamiento responsable de los Estados en el ciberespacio en el contexto de la seguridad internacional. Ambos tienen el cometido de analizar "la forma en que el derecho internacional se aplica a la utilización de las tecnologías de la información y las comunicaciones por los Estados"[2]. El CICR presentará el presente documento de posición a ambos grupos en apoyo de las deliberaciones de los Estados al respecto.

Este documento se limita a cuestiones de índole jurídica y humanitaria que emanan del recurso a las ciberoperaciones durante conflictos armados. No aborda planteos relativos al marco jurídico aplicable a las ciberoperaciones que no estén relacionadas con conflictos armados.

II. El posible costo humano de las ciberoperaciones

Se ha recurrido a las operaciones cibernéticas en conflictos armados como apoyo o a la par de las operaciones cinéticas. Si bien el recurso a las ciberoperaciones puede presentar alternativas que otros medios o métodos de guerra no ofrecen, también entraña riesgos. Por un lado, estas operaciones podrían posibilitar que las partes en conflictos armados logren sus objetivos militares sin provocar daños civiles ni perjudicar físicamente la infraestructura civil. Por otro lado, algunas ciberoperaciones recientes —que tuvieron lugar, sobre todo, fuera del contexto de conflictos armados— han evidenciado que, actualmente, los actores más avanzados tienen la capacidad de interrumpir el suministro de servicios esenciales para la población civil.

Por medio de las ciberoperaciones, se abre la posibilidad para los beligerantes de infiltrarse en un sistema y recopilar, exfiltrar, modificar, encriptar o destruir datos. También es posible utilizar un sistema informático comprometido para activar, modificar o manipular de alguna otra manera procesos controlados por ese sistema. Existen diversos "objetivos" en el mundo real —como las industrias, la infraestructura, las telecomunicaciones, el transporte, los sistemas gubernamentales o financieros— que pueden alterarse, modificarse o dañarse. Como resultado de los debates que mantuvo con expertos de todo el mundo, así como de su propia investigación, el CICR ha pasado a

[1] En este documento, se utiliza el término "ciberoperaciones durante conflictos armados" para describir las operaciones ejecutadas contra una computadora, una red o un sistema informático, u otro dispositivo conectado, a través de un flujo de datos, cuando se recurre a ellas como métodos o medios de guerra en el contexto de un conflicto armado. Las ciberoperaciones dependen de las tecnologías de la información y de la comunicación.

[2] A/RES/73/27, párrafo dispositivo 5; A/RES/73/266, párrafo dispositivo 3.

preocuparse especialmente por el posible costo humano de las ciberoperaciones contra la infraestructura civil esencial, incluida la infraestructura de salud[3].

En los últimos años, los ciberataques han dejado expuesta la vulnerabilidad de los servicios esenciales. Aparentemente, estos ataques son cada vez más frecuentes, y su intensidad aumenta más rápido de lo que preveían los expertos. Además, existen aspectos sobre los que aún no se sabe mucho: cuáles son las herramientas y capacidades cibernéticas más sofisticadas que se han generado o están generándose, de qué manera podría evolucionar la tecnología y en qué medida el recurso a las ciberoperaciones durante conflictos armados puede llegar a diferir de las tendencias observadas hasta el momento.

Además, las características del ciberespacio despiertan preocupaciones específicas. Por ejemplo, las ciberoperaciones suponen un riesgo de escalada y de un consiguiente daño humano, por el simple hecho de que puede ser difícil para la parte atacada saber si el atacante se propone recopilar inteligencia o provocar efectos más perjudiciales. La parte atacada puede, entonces, reaccionar con más vehemencia de lo necesario, para anticiparse al panorama más negativo posible.

Las herramientas cibernéticas también tienen su manera particular de proliferar. Una vez utilizadas, pueden reutilizarse con otros fines y emplearse de manera generalizada por actores que no son quienes la formularon o utilizaron originalmente.

III. La aplicación del DIH a las ciberoperaciones durante los conflictos armados

Para el CICR, no caben dudas de que el DIH se aplica a las ciberoperaciones durante los conflictos armados. Por lo tanto, las limita, de la misma manera que limita, en ese marco, el empleo de otras armas, medios o métodos de guerra, ya sean nuevos o tradicionales[4]. Es indistinto si el ciberespacio se considera un ámbito de guerra similar al aéreo, terrestre, marítimo o exterior; si se lo considera diferente de esos ámbitos naturales, por haber sido creado por el hombre; o si no se lo considera como un ámbito de guerra.

Cuando los Estados aprueban tratados de DIH, lo hacen para regular conflictos presentes y futuros. Se han incorporado normas —en tratados de DIH— que prevén el desarrollo de nuevos medios y métodos de guerra, a partir de la presunción de que el DIH se aplicará a ellos. Por ejemplo, si el DIH no se aplicara a medios y métodos de guerra futuros, no sería necesario revisar la legalidad de estos a la luz las normas vigentes del DIH, tal como lo establece el artículo 36 del Protocolo adicional 1 del 8 de junio de 1977.

Esta conclusión recibe gran apoyo en la opinión consultiva emitida por la Corte Internacional de Justicia (CIJ) sobre la legalidad de la amenaza o del empleo de armas nucleares: la CIJ recordó que las normas y los principios establecidos del DIH aplicables en los conflictos armados rigen para "todas las formas de guerra y todos los tipos de armas", incluso "las del futuro"[5]. Para el CICR, esta afirmación se aplica al recurso a las ciberoperaciones durante los conflictos armados.

---

[3] V. CICR, *The Potential Human Cost of Cyber Operations*, 2019, disponible en línea en https://www.icrc.org/en/download/file/96008/the-potential-human-cost-of-cyber-operations.pdf.

[4] CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2011, 31IC/11/5.1.2, pp. 36-37: disponible en https://www.icrc.org/es/doc/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-es.pdf; "El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos", 2015, 32IC/15/11, p. 40: disponible en https://www.icrc.org/es/download/file/15128/32ic-report-on-ihl-and-the-challenges-of-armed-conflicts_es.pdf; ICRC, "El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos", 2019, 33IC/19/9.7, p. 18; disponible en https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_ES.pdf.

[5] Corte Internacional de Justicia (CIJ), "Legalidad de la amenaza o el empleo de armas nucleares", opinión consultiva, 8 de julio de 1996, párr. 86.

El CICR acoge con beneplácito la aseveración por parte de un número creciente de Estados y de organizaciones internacionales de que el DIH se aplica a las ciberoperaciones durante los conflictos armados y queda a la espera de los debates sobre la manera en que se aplica.

Los Estados también pueden decidir imponer límites adicionales a las ciberoperaciones que se sumen a los del derecho vigente, así como desarrollar normas complementarias, en particular, para reforzar la protección de las personas civiles y de la infraestructura civil contra los efectos de las ciberoperaciones. Para el CICR, toda nueva norma que se contemple debe partir del marco jurídico vigente, incluido el DIH, y reforzarlo.

En los casos no previstos por las normas vigentes del DIH, las personas civiles y los combatientes están protegidos por la llamada cláusula Martens, que establece que estos quedan bajo la protección y el imperio de los principios del derecho internacional derivados de la costumbre, de los principios de humanidad y de los dictados de la conciencia pública[6].

Es importante subrayar que la aseveración de que el DIH se aplica a las ciberoperaciones durante conflictos armados no legitima la guerra cibernética ni fomenta la militarización del ciberespacio. De hecho, el DIH impone algunos límites a esa militarización al prohibir el desarrollo de capacidades cibernéticas militares que violarían el DIH[7]. Además, todo uso de la fuerza —cibernética o cinética— por parte de los Estados se rige por la Carta de las Naciones Unidas y las normas correspondientes del derecho internacional consuetudinario, en particular, la prohibición del uso de la fuerza. Los litigios internacionales deben resolverse por vía pacífica, en el ciberespacio como en todas las demás esferas.

IV. La protección que otorga el DIH vigente

Los tratados de DIH y el derecho consuetudinario vigentes regulan los conflictos armados a través de numerosas disposiciones. En el ciberespacio, las normas que rigen la conducción de las hostilidades son particularmente pertinentes. Estas normas tienen como objetivo proteger a la población civil contra los efectos de las hostilidades. Se basan en el principio cardinal de distinción, que exige a los beligerantes diferenciar, en todo momento, entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares, así como dirigir sus operaciones únicamente contra estos últimos[8].

Más allá de la interconectividad que caracteriza el ciberespacio, si se analiza minuciosamente el funcionamiento de las herramientas cibernéticas, se llega a la conclusión de que no son necesariamente indiscriminadas. Muchos de los ciberataques recientes que se han denunciado públicamente parecerían, desde un punto de vista técnico, haber sido bastante discriminados: fueron diseñados y utilizados para atacar y dañar determinados bienes específicos, y no se han expandido ni ocasionado daños de manera indiscriminada. Sin embargo, procurar que se vean afectados únicamente los objetivos establecidos puede ser técnicamente complicado y requerir una planificación exhaustiva en cuanto al diseño y al uso de las ciberoperaciones. También cabe señalar que una ciberoperación que es técnicamente discriminada no necesariamente es legítima, ni durante un conflicto armado ni fuera de ese contexto.

Dicho esto, se han diseñado algunas herramientas cibernéticas para que se autopropaguen y afecten, de manera indiscriminada, sistemas informáticos de uso generalizado. Esta situación no es producto del azar: la posibilidad de autopropagación debe incluirse deliberadamente en el diseño de esas herramientas. La interconectividad que caracteriza el ciberespacio implica que todo lo que esté

[6] V. art. 1 (2) del Protocolo adicional I del 8 de junio de 1977 a los Convenios de Ginebra; párr. 9 del preámbulo de la Conferencia de la Haya de 1899 (II); y párr. 8 del preámbulo de la Conferencia de la Haya de 1907 (IV).

[7] V. Henckaerts y Doswald-Beck (eds.), *El derecho internacional humanitario consuetudinario*, Volumen *I: Normas*, CICR, Cambridge University Press, Cambridge, 2005 (en adelante, Estudio del CICR sobre DIH consuetudinario), normas 70 y 71; v. también art. 36, Protocolo adicional I.

[8] Art. 48, Protocolo adicional I; normas 1 y 7, Estudio del CICR sobre DIH consuetudinario; CIJ, *Legalidad de la amenaza o el empleo de armas nucleares*, opinión consultiva, 8 de julio de 1996, párr. 78.

conectado a internet puede ser señalado como objetivo desde cualquier parte del mundo. Además, un ataque a un sistema específico puede tener consecuencias para varios sistemas más y provocar efectos indiscriminados. Por lo tanto, existe un riesgo concreto de que las herramientas cibernéticas no hayan sido diseñadas ni se empleen de conformidad con el DIH, ya sea de manera deliberada o por error.

La aseveración de que el DIH —incluidos los principios de distinción, proporcionalidad y las precauciones— regula las ciberoperaciones durante los conflictos armados significa que, en virtud del derecho vigente, rigen las siguientes normas, entre muchas otras:

- se prohíben las capacidades cibernéticas que se consideran como armas y de tal índole que sus efectos sean indiscriminados[9];
- se prohíben los ataques contra las personas civiles y los bienes de carácter civil, incluso en casos en que se utilicen medios o métodos cibernéticos de guerra[10];
- quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil, incluso cuando se realizan por medios o métodos cibernéticos de guerra[11];
- se prohíben los ataques indiscriminados, es decir, los que están dirigidos contra objetivos militares y personas civiles o bienes de carácter civil sin distinción, incluso cuando se utilizan medios o métodos cibernéticos de guerra[12];
- se prohíben los ataques desproporcionados, incluidos los casos en que se utilicen medios o métodos cibernéticos de guerra. Los ataques se considerarán desproporcionados cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista[13];
- durante las operaciones militares, incluso cuando se utilizan medios y métodos de guerra cibernéticos, se debe tener cuidado constante de resguardar a las personas civiles y los bienes de carácter civil; se tomarán todas las precauciones factibles para evitar o reducir, en todo caso, a un mínimo los daños civiles que pudieran causar incidentalmente los ataques, incluso por medios y métodos cibernéticos de guerra[14];
- se prohíbe atacar, destruir, sustraer o inutilizar los bienes indispensables para la supervivencia de la población civil, incluso por medios y métodos cibernéticos de guerra[15]; y
- deben protegerse y respetarse los servicios médicos, incluso en la conducción de ciberoperaciones durante conflictos armados.[16]

Además, se tomarán todas las precauciones factibles para proteger a la población civil y los bienes de carácter civil de los efectos de los ataques realizados con medios y métodos cibernéticos de

[9] Norma 71, Estudio del CICR sobre DIH consuetudinario.
[10] Arts. 48, 51 y 52, Protocolo adicional I; normas 1 y 7, Estudio del CICR sobre DIH consuetudinario.
[11] Art. 51(2), Protocolo adicional I; norma 2, Estudio del CICR sobre DIH consuetudinario.
[12] Art. 51(4), Protocolo adicional I; normas 11 y 12, Estudio del CICR sobre DIH consuetudinario. Son ataques indiscriminados: (a) los que no están dirigidos contra un objetivo militar concreto; (b) los que emplean métodos o medios de guerra que no pueden dirigirse contra un objetivo militar concreto; o (c) los que emplean métodos o medios de guerra cuyos efectos no sea posible limitar conforme a lo exigido por el derecho internacional humanitario; y que, en consecuencia, en cualquiera de esos casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o bienes civiles sin distinción;
[13] Arts. 51 (5)(b) y 57, Protocolo adicional I; norma 14, Estudio del CICR sobre DIH consuetudinario.
[14] Art. 57, Protocolo adicional I; normas 15-21, Estudio del CICR sobre DIH consuetudinario.
[15] Art. 54, Protocolo adicional I; art. 14, Protocolo adicional II del 8 de junio de 1977 a los Convenios de Ginebra; norma 54 del Estudio del CICR sobre DIH consuetudinario.
[16] V., por ejemplo, art. 19, I Convenio para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña; art. 12, II Convenio para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar; art. 18, IV Convenio relativo a la protección debida a las personas civiles en tiempo de guerra; art. 12, Protocolo adicional I; art. 11, Protocolo adicional I; normas 25, 28 y 29 del Estudio del CICR sobre DIH consuetudinario.

guerra, una obligación que los Estados deben cumplir de por sí en tiempo de paz[17]. Podrían considerarse las siguientes medidas: separar la infraestructura y las redes cibernéticas militares de las civiles; separar de internet los sistemas informáticos de los cuales depende la infraestructura civil esencial; destinar esfuerzos a identificar la infraestructura y las redes cibernéticas que prestan servicio a instalaciones que gozan de especial protección, como los hospitales[18].

V. La necesidad de debatir cómo se aplica el DIH

La afirmación de que el DIH rige las ciberoperaciones en los conflictos armados es un primer paso fundamental para evitar o reducir al mínimo el sufrimiento humano que podrían llegar a provocar esas operaciones. Sin embargo, el CICR también incentiva a los Estados a tratar de llegar a un acuerdo respecto de cómo se aplican las normas y los principios del DIH a las ciberoperaciones. Ese acuerdo es necesario dada la interconectividad inherente al ciberespacio, y su carácter eminentemente digital plantea dificultades en cuanto a la interpretación de los principios y conceptos clave del DIH en relación con la conducción de las hostilidades.

En este documento de posición, el CICR hace hincapié sobre tres de los varios temas que abarca esta cuestión.

El uso militar del ciberespacio y los efectos sobre su carácter civil

Salvo por algunas redes militares específicas, el ciberespacio se utiliza predominantemente con fines civiles. Sin embargo, las redes civiles y militares pueden estar interconectadas, y estas últimas pueden depender de la infraestructura cibernética civil: cables de fibra óptica submarinos, satélites, enrutadores o nodos. A la inversa, los vehículos civiles, el transporte de carga y los controles de tráfico aéreo dependen cada vez más de sistemas de navegación satelital que también pueden ser utilizados por militares. Las cadenas de suministro logístico civiles y los servicios civiles esenciales utilizan las mismas redes web y de comunicación a través de las cuales circula parte de la información militar.

El uso de un bien de carácter civil con fines militares no convierte automáticamente a ese bien en un objetivo militar según el DIH[19]. Sin embargo, en caso de que sí se convierta en un objetivo militar, el bien deja de estar protegido en virtud de la prohibición de los ataques directos a los bienes de carácter civil. Resultaría por demás preocupante que el uso militar del ciberespacio llevara a la conclusión de que muchos bienes que forman parte de ese ámbito no gozan de la protección que les corresponde por tratarse de bienes de carácter civil. Si esto ocurriera, podría derivar en una gran alteración del uso civil del ciberespacio, un uso que adquiere cada vez más importancia.

Dicho esto, aunque determinadas partes de la infraestructura del ciberespacio dejaran de gozar de protección como bienes de carácter civil durante conflictos armados, todo ataque seguiría rigiéndose por la prohibición de los ataques indiscriminados y por las normas de proporcionalidad y las precauciones en el ataque. Precisamente como las redes civiles y militares están tan interconectadas, es fundamental evaluar el daño civil incidental previsto de cualquier ciberoperación a fin de que la población civil esté protegida de sus efectos[20].

---

[17] Art. 58, Protocolo adicional I; normas 22 a 24, Estudio del CICR sobre DIH consuetudinario.

[18] CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2015, p. 43.

[19] V. art. 52(2), Protocolo adicional I; norma 8, Estudio del CICR sobre DIH consuetudinario: "Por lo que respecta a los bienes, los objetivos militares se limitan a aquellos bienes que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar y cuya destrucción total o parcial, captura o neutralización ofrezca, en las circunstancias del caso, una ventaja militar definida." Para obtener información más detallada sobre los límites de la militarización de la infraestructura cibernética, v. CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2015, p. 42.

[20] V. CICR, *The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International*

La noción de "ataque" según el DIH y las ciberoperaciones

La infraestructura civil esencial que permite la prestación de servicios fundamentales depende, cada vez más, de sistemas digitalizados. La preservación de esa infraestructura y de esos servicios frente a ciberataques o daños incidentales es vital para proteger a la población civil.

El DIH otorga protección específica para determinadas infraestructuras, como los servicios médicos y los bienes indispensables para la supervivencia de la población, independientemente del tipo de operación del que se trate[21]. Sin embargo, la mayoría de las normas que parten de los principios de distinción, proporcionalidad y precauciones —que otorgan protección general a la población civil y los bienes de carácter civil— se aplican únicamente a las operaciones militares que se definen como "ataques" según el DIH[22]. En virtud del artículo 49 del Protocolo adicional I, "se entiende por 'ataques' los actos de violencia contra el adversario, sean ofensivos o defensivos"[23]. La cuestión de si la noción de "ataque" se interpreta de forma amplia o restringida con respecto a las ciberoperaciones es, por lo tanto, esencial para la aplicabilidad de estas normas y la protección que confieren a las personas civiles y a la infraestructura civil.

Está ampliamente aceptado que las ciberoperaciones que se podría prever que causen muertes, heridas o daños físicos constituyen ataques según el DIH. El CICR considera dentro de esa categoría las ciberoperaciones que ocasionan perjuicio por medio de sus efectos directos e indirectos previsibles: por ejemplo, cuando los pacientes de la unidad de cuidados intensivos de un hospital fallecen debido a que una ciberoperación dirigida a una red eléctrica provocó la interrupción del suministro de energía de ese hospital.

Más allá de eso, los ataques que alteran de manera significativa los servicios esenciales sin necesariamente ocasionar daños físicos representan uno de los riesgos más graves para las personas civiles. Sin embargo, aún hay diferencias de opinión acerca de si las ciberoperaciones que resultan en una pérdida de funcionalidad sin causar daños físicos deben considerarse ataques según el DIH. Para el CICR, durante un conflicto armado, una operación diseñada para desactivar una computadora o una red informática constituye un ataque según el DIH, ya sea por medios cinéticos o cibernéticos[24]. Si se interpreta que la noción de ataque hace referencia únicamente a las operaciones que provocan muertes, heridas o daño físico, entonces una ciberoperación que tiene como objetivo interrumpir el funcionamiento de una red civil (como una red eléctrica, bancaria o de comunicación) o que se prevé que provocará ese efecto de manera incidental puede no estar contemplada por las normas esenciales del DIH que protegen a la población civil y a los bienes de carácter civil. Sería difícil conciliar una interpretación tan excesivamente restrictiva del concepto de ataque con el objeto y fin de las normas del DIH sobre la conducción de las hostilidades. Para lograr la protección adecuada de la población civil contra los efectos de las ciberoperaciones, es esencial que los Estados coincidan en su definición de ataque.

Humanitarian Law, 2018: disponible en https://www.icrc.org/en/download/file/79184/4358_002_expert_meeting_report_web_1.pdf, pp. 37-40.

[21] V. texto relacionado con las notas al pie 16 y 15 de este documento. Se prohíbe atacar, destruir, sustraer o inutilizar los "bienes indispensables para la supervivencia".

[22] La noción de "ataque" según el DIH, definida en el art. 49 del Protocolo adicional 1 difiere de la noción de "ataque armado" que figura en el art. 51 de la Carta de las Naciones Unidas, que se inscribe dentro del ámbito del *jus ad bellum*. Afirmar que una ciberoperación determinada o un tipo de ciberoperación constituye un ataque según el DIH no necesariamente implica que constituiría un ataque armado según la Carta de las Naciones Unidas.

[23] Para obtener información sobre las normas que se aplican específicamente a los ataques, v. el texto el relación con las notas al pie 10 a 14 de este documento.

[24] V. CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2011, p. 37; CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2015, pp. 41–42.

Datos civiles y el concepto de bienes de carácter civil

Los datos civiles esenciales —datos médicos, biométricos, de seguridad social, registros impositivos, cuentas bancarias, expedientes de clientes de empresas o listas y registros de elecciones— son un elemento muy importante de las sociedades digitalizadas. Esos datos son imprescindibles para el funcionamiento de la mayoría de los aspectos de la vida civil, a nivel individual o social. Protegerlos se ha vuelto una cuestión cada vez más preocupante.

Parte de la protección específica que otorga el DIH abarca los datos esenciales, como los que pertenecen a unidades médicas, contemplados dentro de la obligación de respetar y proteger esas unidades[25].

En líneas más generales, los principios y normas esenciales del DIH que rigen la conducción de las hostilidades protegen a las personas civiles y a los bienes de carácter civil[26]. Por lo tanto, sería importante que los Estados acordaran que los datos civiles están protegidos en virtud de esas normas.

La eliminación o alteración de los datos civiles esenciales puede paralizar rápidamente los servicios gubernamentales y la actividad de empresas privadas. Para la población civil, estas operaciones pueden provocar más daño que la destrucción de los bienes físicos. La posibilidad de considerar los datos civiles como bienes de carácter civil y en qué medida es una cuestión aún sin resolver. Para el CICR, afirmar que la eliminación o la adulteración de esos datos esenciales de carácter civil no estarían prohibidas por el DIH en un mundo tan dependiente de los datos parece difícil de conciliar con el objeto y fin de esta rama del derecho. El reemplazo de archivos y documentos en papel por datos digitales no debe disminuir la protección que les confiere el DIH[27]. Excluir los datos civiles esenciales de la protección otorgada a los bienes de carácter civil dejaría un vacío considerable en materia de protección.

VI. Atribución del comportamiento en el ciberespacio a los efectos de la responsabilización de los Estados

El ciberespacio ofrece una amplia variedad de posibilidades técnicas para que los actores oculten o falsifiquen su identidad, lo que vuelve más compleja la cuestión de la atribución y genera dificultades considerables. Por ejemplo, incluso durante conflictos armados, el DIH se aplica únicamente a las operaciones relacionadas con el conflicto. Si no es posible identificar al autor de una ciberoperación, y, por ende, tampoco es posible identificar el vínculo que guarda con un conflicto determinado, resulta extremadamente difícil establecer si el DIH es aplicable a esa operación. La atribución de las ciberoperaciones también es importante para poder responsabilizar a los actores que infringen el derecho internacional, incluido el DIH. La percepción de que es más fácil negar la responsabilidad por los ciberataques también podría disminuir los reparos para recurrir a ellos y hacer que muchos actores tuvieran menos escrúpulos en emplearlos sin respetar el derecho internacional.

Dicho esto, la atribución no es un problema para los actores que conducen, dirigen o controlan las ciberoperaciones: todos tienen la información disponible para determinar dentro de qué marco legal internacional operan y qué obligaciones deben respetar.

Según el derecho internacional, un Estado es responsable de los comportamientos atribuibles a él, incluidas las posibles violaciones del DIH. Por ejemplo:

- comportamientos de órganos estatales, incluidas sus fuerzas armadas o servicios de inteligencia;

[25] V. nota al pie de página 16.

[26] V. texto relacionado con las notas al pie 10 y 15 de este documento.

[27] CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2015, p. 43; CICR, "El derecho internacional humanitario y los retos de los conflictos armados contemporáneos", 2019, p. 21.

- comportamientos de personas físicas o jurídicas, como empresas privadas facultadas por el Estado para ejercer elementos de la autoridad gubernamental;
- comportamientos de personas o grupos, como milicias o grupos de piratas informáticos, que procedan según instrucciones del Estado o bien bajo su dirección o control; y
- comportamientos de personas o grupos privados que el Estado reconoce y acepta como propios[28].

Estos principios se aplican independientemente de si el comportamiento se ejerce por medios cibernéticos o de otra índole.

VII. Conclusión

El recurso a las ciberoperaciones como medios y métodos de guerra en conflictos armados plantea un riesgo real para las personas civiles. A fin de proteger a la población y las infraestructuras civiles, es fundamental reconocer que esas operaciones no ocurren en un vacío legal. El CICR insta a todos los Estados a aseverar que el DIH se aplica a las ciberoperaciones durante los conflictos armados, partiendo de la comprensión de que esa afirmación no incentiva la militarización del ciberespacio ni legitima la guerra cibernética.

Al mismo tiempo, el CICR considera que es necesario seguir debatiendo, sobre todo entre los Estados, de qué manera debe interpretarse y aplicarse el DIH en el ciberespacio. Existe una necesidad urgente de que se entable ese diálogo, ya que los Estados que decidan desarrollar o adquirir las capacidades cibernéticas que se consideran armas, medios y métodos de guerra, ya sea con fines ofensivos o defensivos, deben procurar que esas capacidades puedan utilizarse conforme a las obligaciones que les competen en virtud del DIH[29]. Este diálogo debe estar fundado en una comprensión profunda del desarrollo de las capacidades cibernéticas militares, su posible costo humano y la protección que confiere el derecho vigente. Los Estados deben determinar si las normas actuales son adecuadas y suficientes en relación con los desafíos que plantea el carácter interconectado y ampliamente digital del ciberespacio o si deben adaptarse en función las particularidades de este último. En caso de que se formulen nuevas normas para proteger a la población civil de los efectos de las ciberoperaciones o por otros motivos, deberían basarse en el marco jurídico actual, incluido el DIH, y fortalecerlo.

El CICR recibe con agrado los debates intergubernamentales que tienen lugar en este momento en el marco de los dos procesos encomendados por la Asamblea General de las Naciones Unidas y agradece la oportunidad de expresar su punto de vista ante los Estados participantes. La institución manifiesta, asimismo, la voluntad de poner a disposición sus conocimientos especializados para ese diálogo, en la medida en que los Estados lo consideren apropiado.

[28] Norma 149, Estudio del CICR sobre DIH consuetudinario. V. también Comisión de Derecho Internacional, "Responsibility of States for Internationally Wrongful Acts", 2001, en particular, arts. 4 a 11.

[29] V. CICR, "El derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos", 2019, págs. 28-29; CICR, *Guía para el examen jurídico de las armas, los medios y los métodos de guerra nuevos: medidas para implementar el artículo 36 del Protocolo adicional I de 1977*, 2006, p. 4; art. 36, Protocolo adicional I.