Humanity
In War

En el marco de la Iniciativa mundial para impulsar el compromiso político con el derecho internacional humanitario (Iniciativa Mundial sobre DIH), **Ghana, Luxemburgo, México, Suiza y el Comité Internacional de la Cruz Roja (CICR)** tienen el agrado de hacer la siguiente presentación:

LÍNEA DE TRABAJO 6

TERCERA CONSULTA CON LOS ESTADOS SOBRE CÓMO PROCURAR QUE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES SE UTILICEN DE CONFORMIDAD CON EL DERECHO INTERNACIONAL HUMANITARIO DURANTE LOS CONFLICTOS ARMADOS

Para representantes gubernamentales especializados en DIH, ciberseguridad o ciberoperaciones militares que se desempeñen en la capital de su país, así como representantes de las misiones permanentes en Ginebra

LUNES 16 DE FEBRERO DE 2026

10:00–14:00 (UTC+1)

FORMATO: PRESENCIAL (EN GINEBRA) Y EN LÍNEA (POR ZOOM)

Antecedentes

El uso creciente de las tecnologías de la información y las comunicaciones (TIC) durante los conflictos armados plantea importantes cuestiones humanitarias y jurídicas. Si bien es un hecho ampliamente reconocido que el DIH impone límites al uso de las TIC en conflictos armados, las características específicas del entorno de estas tecnologías dan lugar a interrogantes complejas acerca de cómo se aplica el DIH en la práctica. Muchos Estados han señalado la necesidad de seguir debatiendo esta cuestión.

La línea de trabajo relativa a las TIC de la Iniciativa Mundial sobre DIH retoma los debates internacionales acerca del uso de las TIC y los avances realizados hasta hoy, como los informes del Grupo de Trabajo de Composición Abierta de las Naciones Unidas sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso y del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, las posturas nacionales y comunes sobre las ciberoperaciones y el derecho internacional, y la resolución 2 de la XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, titulada "Protección de la población civil y de otras personas y bienes protegidos ante el posible costo humano de las actividades relacionadas con las tecnologías de la información y las comunicaciones durante conflictos armados". Complementa los debates multilaterales en curso, entre ellos el mecanismo mundial de próximo lanzamiento sobre los avances en el ámbito de las TIC en el contexto de la seguridad internacional y la promoción de comportamientos responsables de los Estados en el uso de las TIC. Esta línea de trabajo se inscribe en un esfuerzo continuo por desarrollar un entendimiento común de los límites que impone el DIH a las actividades relacionadas con las TIC durante los conflictos armados, con el fin de proteger a las personas civiles contra los daños causados por esas operaciones.

Durante las dos primeras consultas con los Estados de la línea de trabajo sobre las TIC, que tuvieron lugar el 15 de mayo y el 24 de noviembre de 2025 respectivamente, se reconocieron las considerables consecuencias humanas que puede tener el uso de TIC en conflictos armados, y se puso de relieve el imperativo de proteger a las personas y preservar la dignidad humana. También se reafirmó que el DIH sigue siendo el marco jurídico principal para proteger a la población civil y otras personas y bienes protegidos contra los peligros que emanan del uso de TIC en conflictos armados internacionales y no internacionales.

En ambas consultas, los participantes analizaron los implicaciones humanitarias y jurídicas del uso de las TIC en conflictos armados, y consideraron medidas prácticas para favorecer el cumplimiento del DIH y fortalecer la protección de la población civil en este contexto.

En la tercera consulta se desarrollarán estos debates y las observaciones surgidas de ellos, con miras a seguir alimentando un entendimiento común sobre cómo respetar el DIH en el uso de TIC en contextos de conflicto armado para preservar de daños a la población civil.

Objetivos

Esta consulta se propone los siguientes objetivos:

- **Consolidar los consensos emergentes** en torno a la protección que brindan las normas y principios del DIH a la población civil y otras personas y bienes protegidos contra los peligros que surgen de las actividades relacionadas con las TIC en contextos de conflicto armado. Si bien los Estados han reafirmado ampliamente la necesidad de respetar y fortalecer esas

protecciones, hay que seguir conversando sobre ciertas cuestiones para promover un entendimiento común. Las observaciones centrales preparadas por los colíderes y el CICR de conformidad con el objetivo de la línea de trabajo de preservar a la población civil de daños en la era digital están pensadas como una base que oriente el debate, invite a hacer nuevos aportes y ayude a evaluar caminos concretos para generar un consenso sobre los límites que establece el DIH al uso de TIC en conflictos armados.

- **Recopilar perspectivas y prácticas nacionales** en torno a medidas jurídicas, operacionales y políticas adoptadas o consideradas para garantizar el cumplimiento del DIH en lo relativo al uso de TIC en conflictos armados: por ejemplo, legislación, prácticas militares, difusión del DIH, diálogo con el sector tecnológico y medidas para prevenir y hacer cesar las violaciones del DIH.
- **Identificar aspectos sobre los que hay que seguir reflexionando y dialogando**, como paso previo a la preparación de recomendaciones preliminares que se han de someter a la consideración de los Estados y que, en última instancia, se incorporarán en los frutos de la Iniciativa Mundial sobre DIH.

Siguientes etapas

Luego de las tres rondas de consultas, los Estados colíderes y el CICR plantearán recomendaciones concretas, que se presentarán a todos los Estados para que las debatan:

- El **1 de abril de 2026**, la primera versión de las recomendaciones correspondientes a cada línea de trabajo se enviará a todas las misiones permanentes en Ginebra y se publicará en el sitio web Humanity in War.
- La **cuarta ronda de consultas** se llevará a cabo entre **el 4 y el 6 de mayo de 2026** en **formato híbrido**. En ese período, se invitará a todos los Estados a compartir sus comentarios sobre la primera versión de las recomendaciones correspondientes a cada línea de trabajo, que se debatirán de manera consecutiva.
- El **1 de junio de 2026**, se enviará a todos los Estados y se publicará en el sitio web Humanity in War la segunda versión de las recomendaciones correspondientes a cada línea de trabajo.
- La **quinta ronda de consultas** se celebrará entre **el 22 y el 26 de junio de 2026** en **formato híbrido**. Se invitará a todos los Estados a poner en común sus comentarios finales sobre las recomendaciones. Luego de esta ronda de consultas, los Estados colíderes y el CICR harán las recomendaciones definitivas correspondientes a cada línea de trabajo, que se presentarán a todos los Estados en la segunda mitad de 2026.

Participantes

- El formato de la consulta será híbrido, es decir que se podrá participar tanto en persona como en línea.
- La consulta estará abierta a todos los Estados interesados. Se recomienda principalmente la participación de representantes gubernamentales especializados en DIH, ciberseguridad o ciberoperaciones militares que se desempeñen en la capital de su país, así como de representantes de las misiones permanentes en Ginebra.

- También se invitará a participar a otros representantes con conocimientos específicos en la materia (por ejemplo, miembros de organizaciones internacionales, la sociedad civil, el ámbito académico y el sector tecnológico).
- Se aceptan inscripciones hasta el viernes 13 de febrero de 2026, por medio de este formulario.

Procedimiento

- Los idiomas de trabajo serán **árabe, chino, español, francés, inglés y ruso**, con interpretación simultánea.
- Les solicitamos que limiten sus intervenciones a **cuatro minutos** a fin de que todos los participantes tengan tiempo suficiente para tomar la palabra. Al final de cada sesión y una vez que hayan hecho sus aportes todos los organismos participantes que así lo deseen, los Estados y otros participantes tendrán la oportunidad de debatir las ideas planteadas por los demás.
- Se solicita a los participantes que, al preparar su intervención, tengan en cuenta las **observaciones principales de los colíderes de la línea de trabajo y el CICR en lo relativo al respeto del DIH en el uso de las TIC en conflictos armados,** además de las **preguntas orientativas** incluidas en el programa. También se puede consultar el documento de antecedentes de la línea de trabajo como referencia para enmarcar el debate.
- En vista de las dificultades técnicas que plantean los encuentros híbridos, recomendamos que las delegaciones presentes en Ginebra hagan sus intervenciones en persona y que, en todos los casos, ofrezcan toda su atención a las delegaciones que participan de forma virtual.
- A lo largo de toda la consulta, el debate tendrá un carácter **inclusivo, constructivo, no politizado y orientado a soluciones**. Si bien se invita a los participantes a hacer referencia a las prácticas nacionales en su respectivo país, solicitamos que se abstengan de hacer comentarios sobre contextos específicos o sobre la práctica de otros Estados.
- Para facilitar la interpretación, invitamos a los participantes a enviar por correo electrónico una copia de sus intervenciones antes del viernes 13 de febrero de 2026 a ihlinitiative@icrc.org, con el asunto "ICT workstream thid consultation". También alentamos a los participantes a enviar una transcripción completa de sus intervenciones por correo electrónico luego de la reunión. **A menos que se solicite expresamente un tratamiento confidencial, las intervenciones se publicarán en el sitio web Humanity in War.**
- La reunión de la consulta quedará grabada, pero la grabación no estará disponible públicamente.

Programa

Procurar que las tecnologías de la información y las comunicaciones se utilicen de conformidad con el derecho internacional humanitario durante los conflictos armados
(Línea de trabajo sobre las TIC)
Tercera ronda de consultas

10:00–14:00, 16 de febrero de 2026
Humanitarium del CICR, 17 avenue de la Paix, 1202 Ginebra

** Todos los horarios pueden variar en función del número de intervenciones.*

Registro y desayuno / Inicio de sesión y conexión	9:30–10:00
Apertura y presentación	10:00–10:10
Sesión 1: Observaciones principales de los colíderes de la línea de trabajo y el CICR en lo relativo al respeto del DIH en el uso de las TIC en conflictos armados	10:10–12:00
Observaciones principales En vista del costo humano de las actividades relacionadas con las TIC en contextos de conflicto armado, así como los daños y trastornos que estas pueden ocasionar en la sociedad, y subrayando el imperativo de proteger a la población civil y preservar la dignidad humana, es esencial fortalecer el respeto del DIH en el uso de las TIC en conflictos armados. Los Estados y las partes en conflictos armados adoptarán medidas prácticas, individuales y colectivas, para mitigar los riesgos a los que pueda quedar expuesta la población civil, así como para que las actividades relacionadas con TIC que se realicen en el contexto de un conflicto armado sean respetuosas de las disposiciones que establece el DIH. **Protección de la población civil, las personas civiles y los bienes de carácter civil ante los peligros derivados de las actividades relacionadas con las TIC durante conflictos armados** En la conducción de actividades relacionadas con las TIC asociadas con un conflicto armado, se debe cumplir en todo momento con lo que dispone el DIH, en particular con los principios de humanidad, necesidad militar, distinción, proporcionalidad y precaución. Las operaciones de TIC de las que cabe prever que dejen un saldo de personas fallecidas o heridas, o que provoquen daños o destrucción de bienes, por ejemplo, de manera tal que dichos bienes queden impedidos de funcionar, constituyen ataques en virtud del DIH, y deben llevarse adelante de conformidad con todas las normas y principios del DIH sobre conducción de las hostilidades, en particular la prohibición de cometer ataques directos contra personas civiles y bienes de carácter civil, ataques indiscriminados y ataques desproporcionados, así como la obligación de tomar todas las precauciones factibles a fin de evitar o, al menos, minimizar el daño incidental a la población civil. El principio de que una parte en un conflicto armado solo puede recurrir a los métodos y medios de guerra que sean necesarios para debilitar a las fuerzas militares del enemigo, la obligación de tomar precauciones constantemente para resguardar a la población civil, las personas civiles y los bienes de carácter civil en la conducción de operaciones militares, y las normas que salvaguardan la propiedad contra su confiscación o destrucción confieren protecciones adicionales contra los peligros que surgen de las actividades relacionadas con las TIC.	

Protección de datos

Los datos son un elemento central en el proceso de digitalización que atraviesa el mundo y para el funcionamiento de los servicios civiles esenciales. La forma en que se manejen los datos durante los conflictos armados puede afectar la vida y la dignidad de las personas. Los datos gozan de protección en virtud de los siguientes elementos del DIH:

- los principios y normas que rigen la conducción de las hostilidades, en particular la distinción —que exige que las operaciones militares se dirijan únicamente a datos que constituyan objetivos militares y prohíbe los ataques que afecten indistintamente a datos civiles y militares—, la proporcionalidad y la precaución;
- el principio de que una parte en un conflicto armado solo puede recurrir a los métodos y medios de guerra que sean necesarios para debilitar a las fuerzas militares del enemigo;
- la obligación de tomar precauciones constantemente para preservar a la población civil, las personas civiles y los bienes de carácter civil en la conducción de las operaciones militares;
- las normas que protegen la propiedad contra el pillaje, la confiscación y la destrucción.

Las actividades de recopilación de información en sí mismas no están prohibidas por el DIH, ni siquiera cuando implican acceder a datos.

Uso de infraestructura civil de TIC con fines militares

Los Estados y las partes en conflictos armados deben conocer y minimizar el riesgo de que se produzcan daños a la población civil a raíz del uso militar de infraestructura civil de TIC en un conflicto armado.

Cuando ese tipo de uso convierte a la infraestructura civil de TIC, o partes de ella, en objetivo militar, todo ataque contra dicho objetivo está sujeto a la prohibición de cometer ataques indiscriminados o desproporcionados, así como a la obligación de tomar todas las precauciones factibles.

Al evaluar la legalidad de esas operaciones, hay que tomar en cuenta todos los efectos incidentales directos e indirectos que quepa prever, incluidos los usos civiles de la infraestructura de TIC. Se deben tomar todas las precauciones factibles para preservar a la población civil y los servicios civiles esenciales que dependen de esa infraestructura. También se deben tomar todas las precauciones factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible el número de víctimas y de heridos que pudieran causar incidentalmente entre la población civil, así como los daños a los bienes de carácter civil. En ese sentido, se debe procurar que solo se vean afectados los componentes o funciones de la infraestructura de TIC utilizados con fines militares, y no los que están al servicio de la población civil.

Los Estados y las partes en conflictos armados deben tomar todas las precauciones posibles para proteger contra los peligros que representan las operaciones militares a la población civil y los bienes de carácter civil que estén bajo su control. Eso implica, siempre que sea física y técnicamente posible, separar los componentes de la infraestructura de TIC utilizados con fines militares de aquellos que desempeñan funciones civiles.

Participación civil en actividades relacionadas con TIC durante un conflicto armado

Las personas civiles, incluidos los hackers y los empleados de empresas de tecnología, deben respetar el DIH cuando actúan en un contexto de un conflicto armado o relacionado con él.

Los Estados deben garantizar el respeto del DIH por parte de las personas civiles cuyas actividades relacionadas con TIC durante un conflicto armado se puedan atribuir al Estado en cuestión, dar a conocer el DIH entre las personas civiles sobre las que ejercen autoridad, en particular hackers y empleados de empresas de tecnología, y tomar las medidas necesarias para informarlas de los riesgos jurídicos y prácticos que implica llevar adelante ese tipo de actividades en el contexto de un conflicto armado. También deben poner en práctica la diligencia debida para prevenir que las personas civiles cometan violaciones del DIH a través o con ayuda de actividades relacionadas con TIC, y hacer cesar dichas violaciones en el caso de que se produzcan. No deben alentar, ayudar ni asistir a las personas civiles para que violen el DIH, en particular por medio de actividades relacionadas con TIC. Los Estados y las partes en un conflicto armado deben evitar, en la medida de lo posible, la actuación de personas civiles en operaciones de TIC que constituyan una participación directa en las hostilidades, a fin de protegerlas contra los peligros que emanan de las operaciones militares. En el caso de que ocurra dicha participación, en la medida de lo posible, las personas civiles en cuestión se deben incorporar en las fuerzas armadas. Los niños no deben participar en las hostilidades. **Productos y servicios de las empresas de tecnología en conflictos armados** Las empresas de tecnología ofrecen diversos productos y servicios civiles relacionados con las TIC de los que depende la población civil, los gobiernos y las organizaciones humanitarias, también en contextos de conflicto armado, y esos bienes de carácter civil, así como los empleados civiles que prestan servicios relacionados con las TIC, gozan de protección en virtud del DIH. Estas empresas no deben perder de vista que brindar productos y servicios relacionados con las TIC a partes en conflictos armados acarrea riesgos de orden jurídico y práctico. Deben conocer, evaluar y minimizar los riesgos de daño a los que se exponen las personas civiles y los bienes de carácter civil, ya sea porque se trata de su personal o de su propiedad, o a causa de una proximidad física, de una conexión digital o de una dependencia de la infraestructura o los servicios en cuestión. Eso implica separar física o técnicamente, en la medida de lo posible, los productos y servicios que se utilizan para operaciones militares de los que se utilizan con fines civiles. Se espera de las empresas de tecnología que hagan lo necesario para evitar que su personal sea partícipe o cómplice de violaciones del DIH, en particular por medio de la prestación de productos o servicios relacionados con las TIC a partes en un conflicto armado, y que, si eso ocurre, tomen medidas adecuadas. ***Preguntas orientativas*** 1. ¿Tiene algún comentario sobre las observaciones principales planteadas más arriba? ¿Hay alguna cuestión que daba seguir debatiéndose? 2. ¿Existen otros elementos o salvaguardas que deban considerarse con miras a fortalecer la protección de la población civil y otras personas y bienes protegidos contra los peligros que surgen de las actividades relacionadas con TIC en contextos de conflicto armado?	
Receso	12:00–12:30
Sesión 2: Observaciones principales de los colíderes de la línea de trabajo y el CICR en lo relativo al respeto del DIH en el uso de las TIC en conflictos armados (continuación)	12:30–13:55

Observaciones principales

Protección de los servicios médicos, las actividades humanitarias y otras personas, bienes y actividades que gozan de protección específica

El personal, las unidades y los transportes sanitarios, así como el personal y los bienes humanitarios, se deben respetar y proteger en todo momento, de conformidad con el DIH, en particular contra los efectos de las actividades relacionadas con las TIC. Cuando estas actividades se desarrollan en contextos de conflicto armado, se debe evitar que generen trastornos indebidos en el funcionamiento de los servicios médicos y las actividades humanitarias, lo que incluye sus datos, las TIC que utilizan y sus sistemas de comunicación. La confidencialidad de los datos médicos y humanitarios se debe respetar de conformidad con el DIH. Esa protección es crucial para preservar la confianza en los servicios de salud y en la labor de las organizaciones humanitarias imparciales. Además, los Estados y las partes en un conflicto armado deben hacer todo lo posible para evitar que los servicios médicos y las actividades humanitarias sufran daños, también a raíz de actividades relacionadas con las TIC que sean obra de terceros como ciberdelincuentes y otros actores no estatales, y que no puedan atribuirse a una de las partes en el conflicto.

Tanto en el entorno digital como en el mundo real, es importante que la protección específica que otorga el DIH a los servicios médicos y las actividades humanitarias sea clara y esté a la vista, para propiciar que se la respete. Una forma de indicar esta protección es el "emblema digital", actualmente en desarrollo. Se alienta a los Estados y otros actores pertinentes a seguir trabajando con el CICR a fin de analizar vías jurídicas, técnicas y diplomáticas para su implementación.

Se debe respetar la protección específica de la que gozan los bienes indispensables para la supervivencia de la población civil, las obras e instalaciones que contienen fuerzas peligrosas, la propiedad cultural y la defensa civil, en particular al llevar adelante operaciones de TIC en contextos de conflicto armado. Eso incluye tanto sus datos como la infraestructura de TIC indispensable para su funcionamiento.

El DIH también prohíbe la violencia sexual, así como el reclutamiento y uso de niñas, niños y adolescentes en hostilidades cuando dichos actos se comenten con el apoyo o a través de actividades relacionadas con las TIC.

Propagación de información que viola el DIH

Los Estados deben abstenerse de utilizar las TIC para propagar información que entrañe una violación del DIH, y hacer todo lo posible para evitar que otros actores lo hagan. Eso incluye difundir información que incite o aliente a violar el DIH, que exponga a personas privadas de libertad a insultos o a la curiosidad del público, o cuyo propósito principal sea sembrar el terror entre la población civil. Los Estados y las partes en conflictos armados no deben propagar información que deshumanice al adversario o que difunda el odio hacia una población civil, en particular por medio de TIC.

Los servicios médicos y la acción humanitaria deben estar protegidos contra las operaciones de desinformación realizadas con ayuda de TIC que buscan obstruir su labor en contextos de conflicto armado, puesto que esos actos interfieren indebidamente y son incompatibles con la obligación de respetar y proteger al personal humanitario y de salud, así como sus actividades.

Medidas para fortalecer el cumplimiento del DIH

Los Estados deben adoptar medidas de alcance nacional para garantizar el cumplimiento del DIH en el uso de TIC durante los conflictos armados. Para ello, hay que difundir el DIH entre las fuerzas armadas y la población en general, sobre todo entre aquellos que puedan participar en actividades relacionadas con las TIC, e incorporar los principios y normas del

DIH, así como su aplicación a las actividades relacionadas con TIC, en la legislación nacional, la doctrina militar, los procedimientos operacionales, las reglas de enfrentamiento y la formación, según corresponda. Siempre que sea necesario, las unidades militares y los mandos responsables de las actividades relacionadas con TIC deben poder disponer de asesoramiento jurídico específico. De conformidad con las obligaciones que impone a los Estados el derecho internacional, al estudiar, desarrollar, adquirir o adoptar capacidades de TIC que funcionan como nuevas armas, métodos o medios de guerra, se debe determinar si su empleo estaría prohibido por el derecho internacional, en ciertas condiciones o en todas las circunstancias. Incorporar enfoques con sensibilidad etaria y de género en los marcos nacionales contribuye a cumplir las obligaciones que impone el DIH también en lo que respecta a atender los riesgos relacionados con las TIC. A fin de preservar a la población civil y a otras personas protegidas de la propagación de información que viole el DIH, el diálogo con los actores pertinentes, entre ellos el sector tecnológico, puede ayudar a propiciar el cumplimiento de la legislación vigente. Ese diálogo puede consistir en alentar a las empresas de tecnología a adoptar salvaguardas y prácticas que reduzcan el riesgo de que las plataformas en línea u otros servicios relacionados con las TIC se utilicen para incitar, propiciar o facilitar violaciones del DIH, o para ocasionar daños a la población civil y los bienes de carácter civil por cualquier otra vía. Es esencial que cada Estado adopte todas las medidas necesarias de orden legislativo, normativo y demás —incluso, cuando corresponda, sanciones penales— a fin de prevenir y hacer cesar las violaciones del DIH cometidas a través o con ayuda de actividades relacionadas con las TIC por personas o en territorios que se encuentran bajo su jurisdicción o control. El desarrollo y la difusión pública de las perspectivas y posiciones nacionales sobre cómo se aplica el derecho internacional, en particular el DIH, al uso de las TIC, así como el intercambio de aprendizajes y buenas prácticas para minimizar el riesgo de que las actividades relacionadas con las TIC ocasionen daños a la población civil, pueden fortalecer la transparencia, la confianza y los consensos. Cuando sea posible, se harán esfuerzos para contribuir al fortalecimiento de las capacidades en el ámbito bilateral, regional y mundial, a fin de que los Estados estén mejor equipados para implementar y aplicar cabalmente el DIH en las actividades relacionadas con las TIC. ***Preguntas orientativas*** **1.** ¿Tiene algún comentario sobre las observaciones principales planteadas más arriba? ¿Hay alguna cuestión que daba seguir debatiéndose? **2.** ¿Existen otros elementos o salvaguardas que deban considerarse con miras a fortalecer la protección de la población civil y otras personas y bienes protegidos contra los peligros que surgen de las actividades relacionadas con TIC en contextos de conflicto armado?	
Observaciones finales	13:55–14:00