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

SEGUNDA 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 funcionarios 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 24 DE NOVIEMBRE DE 2025
9:00–18:00 (UTC+1)
FORMATO: PRESENCIAL (EN EL HUMANITARIUM DEL CICR 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 sobre TIC se apoya en los debates internacionales sobre el uso de las TIC y los avances logrados hasta hoy, en particular la resolución 2 de la XXXIV Conferencia Internacional de la Cruz Roja y de la Media Luna Roja "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". Esta línea de trabajo se inscribe en un esfuerzo continuo por desarrollar un entendimiento común acerca de cómo el DIH impone límites 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.

La primera consulta sobre esta línea de trabajo se llevó a cabo el 15 de mayo de 2025 y se abocó a identificar las cuestiones e inquietudes jurídicas y humanitarias que plantean las características singulares de las actividades relacionadas con las TIC en conflictos armados, y a analizar cómo atenderlas con miras a defender la protección que confiere el DIH a la población civil y los bienes de carácter civil, así como a otras personas y bienes protegidos en conflictos armados. La segunda consulta, durante la que se profundizará ese análisis, se realizará en formato híbrido el 24 de noviembre de 2025 en Ginebra.

Para más detalles sobre las cuestiones que se tratarán en esta línea de trabajo, se invita a los participantes a consultar el **documento de antecedentes** adjunto a esta nota conceptual.

Objetivos

La segunda consulta retomará los debates que se desarrollaron durante la primera consulta y las conclusiones a las que se arribó en esa oportunidad. Se centrará en profundizar el análisis de las cuestiones jurídicas y humanitarias que surgen del uso de las TIC en conflictos armados. Durante el encuentro, se buscará ampliar el entendimiento común e identificar posibles recomendaciones jurídicas y prácticas para mejorar la protección de las personas civiles y los bienes de carácter civil en contextos de guerra digital.

Esta consulta tendrá los siguientes objetivos:

- **Proporcionar una actualización sobre la línea de trabajo y sus progresos**
    - informar a los participantes sobre las conclusiones de la primera consulta reflejadas en el informe sobre los progresos alcanzados, así como sobre las ideas surgidas en eventos complementarios subsiguientes;
    - delinear los próximos pasos hacia la determinación de las recomendaciones finales de la línea de trabajo.
- **Profundizar el debate sobre las cuestiones jurídicas y humanitarias identificadas para ampliar el entendimiento común surgido de él**

- facilitar intercambios pormenorizados sobre las cuestiones identificadas durante la primera consulta para seguir estudiándolas, entre ellas:
    - implicaciones para el DIH de las operaciones de TIC que tienen efectos no físicos, como la pérdida de funcionalidad del sistema atacado;
    - protección que confiere el DIH a los datos civiles y de otras índoles, por ejemplo, contra manipulación, daños o eliminación, extracción y publicación;
    - protección específica en el marco del DIH de personas, bienes y actividades, así como de la infraestructura digital y los datos relacionados, contra los efectos de las operaciones de TIC;
    - límites que impone el DIH a la divulgación de información por medio de actividades relacionadas con TIC;
    - implicaciones para el DIH del uso militar de infraestructura de TIC de carácter civil y de la participación de personas civiles en actividades de TIC en contextos de conflicto armado, y medidas basadas en el DIH para mitigar los riesgos asociados de daño para la población civil y los servicios civiles esenciales;
- fortalecer las medidas prácticas a fin de mejorar el cumplimiento del DIH y mitigar el riesgo para la población civil.

Siguientes etapas

A principios de 2026 se llevará a cabo una tercera consulta con los Estados para seguir profundizando los debates de los encuentros anteriores y los consensos a los que se haya arribado a partir de ellos. Estas consultas sentarán las bases para las recomendaciones que se formulen en la línea de trabajo. En el segundo trimestre de 2026, se invitará a todos los Estados interesados a hacer comentarios sobre las recomendaciones, que seguirán analizándose en consultas sucesivas con los Estados.

Las consultas con los Estados se complementarán con debates regionales y otros eventos complementarios, que se anunciarán en el sitio web Humanity in War.

Participantes

- La consulta se llevará a cabo principalmente de forma presencial en Ginebra, aunque también se podrá participar en línea.
- La consulta es **abierta para todos los Estados interesados**. Se recomienda principalmente la participación de funcionarios 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.
- También se invitará a participar a otros representantes con conocimientos específicos en la materia (por ejemplo, miembros de organizaciones internacionales, la sociedad civil y el ámbito académico).
- Se aceptan inscripciones hasta el 15 de noviembre de 2025 en https://forms.office.com/e/LuDKik93vY.

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 **preguntas orientativas** incluidas en el programa. Algunas preguntas orientativas se acompañan de **situaciones ilustrativas** que deben leerse junto con ellas. Para enmarcar y facilitar el debate, se adjunta un **documento de antecedentes** a esta nota conceptual.
- 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 21 de noviembre de 2025 a ihlinitiative@icrc.org, con el asunto "ICT workstream second 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 la confidencialidad, estas declaraciones se publicarán en el sitio web del CICR.**
- 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)
Segunda ronda de consultas

9:00–18:00, 24 de noviembre de 2025
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	08:30 –9:00
Apertura y presentación	09:00 –9:30
Panel de debate: Cuestiones jurídicas y humanitarias centrales que surgen del uso de las TIC en conflictos armados	09:30 –10:30
Sesión 1: Medidas prácticas para promover el cumplimiento del DIH y proteger a la población civil del uso de TIC en conflictos armados	10:30 –11:30
Preguntas orientativas 1. ¿Qué medidas jurídicas y operacionales ha adoptado o considerado adoptar su Estado para fomentar el cumplimiento del DIH y prevenir o mitigar el daño civil cuando se llevan adelante actividades relacionadas con TIC en contextos de conflicto armado? ¿En qué se diferencian esas medidas de las que se aplican a las operaciones cinéticas, por las características específicas de las operaciones de TIC, y cómo pueden abordarse esas especificidades? 2. ¿Qué medidas ha adoptado o considerado adoptar su Estado para prevenir y hacer cesar las violaciones del DIH relacionadas con actividades de TIC o cometidas por medio de ellas? 3. ¿Qué formas de fortalecimiento de la capacidad o cooperación internacional serían las más adecuadas para ayudar a los Estados a mejorar el cumplimiento y a compartir medidas prácticas en este ámbito?	
Pausa	11:30 –12:00
Sesión 2: Protección de las poblaciones civiles y otras personas y objetos protegidos ante los peligros derivados de las actividades relacionadas con las TIC durante conflictos armados	12:00 –13:00
Preguntas orientativas	

1. ¿Cuáles son los costos humanos y las repercusiones para el DIH de las operaciones de TIC que tienen efectos no físicos, como impedir el funcionamiento del sistema atacado? Considere una operación de TIC que se lleva a cabo en el contexto de un conflicto armado contra un bien de carácter civil, como el servidor de un prestador de servicios de transporte, un proveedor de internet o un banco. En el momento de la operación, el servidor no se está usando de manera que permita calificarlo de objetivo militar. Como consecuencia de la operación, el bien atacado ya no brinda el servicio habitual, a pesar de no haber sufrido daños físicos. ¿Cómo evalúa su Estado la legalidad de la operación de TIC? ¿Cambiaría esa evaluación si se produjeran daños físicos como resultado de los efectos previsibles, directos o indirectos, de la operación? 2. ¿Cómo aborda su Estado la protección que confiere el DIH a los datos civiles y de otras índoles contra la manipulación, el daño, la eliminación, la extracción o la publicación no autorizada, por ejemplo? ¿Su Estado distingue entre diferentes categorías de datos (biométricos, financieros, de salud, etc.) para determinar de qué protección gozan en virtud del DIH? Considere una operación de TIC que se lleva a cabo en el contexto de un conflicto armado para eliminar datos civiles (por ejemplo, datos de salud, de seguridad social, de cuentas bancarias, datos impositivos o de los clientes de empresas civiles). ¿Cómo evalúa su Estado la legalidad de esa operación? ¿Qué normas del DIH limitan la posibilidad de manipular, dañar o destruir datos civiles u otros datos protegidos en tiempo de conflicto armado? ¿Qué protección confiere el DIH contra la copia no autorizada, la captura y la posible publicación de datos civiles u otros datos protegidos? 3. ¿Qué normas del DIH preservan a las personas civiles y los bienes de carácter civil contra las operaciones de TIC que no se califican como "ataques" de conformidad con el DIH? Por ejemplo, ¿qué medidas prácticas se deben adoptar al realizar actividades relacionadas con TIC para cumplir con la obligación de tener cuidado constante de resguardar a las personas civiles y los bienes de carácter civil en la conducción de operaciones militares?	
Almuerzo (no incluido)	13:00 –14:00
Sesión 3: Implementación de protecciones específicas para las personas, los bienes y las actividades contra los efectos del uso de TIC durante un conflicto armado	14:00 –15:00
Preguntas orientativas 1. ¿Qué medidas prácticas adopta o considera adoptar su Estado para que las actividades relacionadas con TIC en contextos de conflicto armado no causen daños ni trastornos en el funcionamiento de los servicios de salud, las actividades humanitarias u otros bienes indispensables para la supervivencia de la población civil, entre ellos sus sistemas de TIC y sus datos? ¿Qué precauciones toma o considera tomar su Estado para preservar esos bienes específicamente protegidos de daños, en particular de los daños causados por actividades relacionadas con TIC? 2. Con respecto a la protección específica de las instalaciones y el personal de salud, considere una operación de TIC, en el contexto de un conflicto armado,	

que lleva adelante una parte para obtener acceso a los servidores de una instalación de salud en territorio del adversario. La parte en cuestión recopila los datos de salud de los miembros de las fuerzas armadas tratados allí y cifra los expedientes de los pacientes, lo que impide que el personal médico pueda acceder a ellos. ¿En qué medida la protección específica de las instalaciones de salud abarca la confidencialidad, la integridad y la disponibilidad de los datos a los que accede su personal y que se recopilan, procesan y almacenan para su funcionamiento? Del mismo modo, ¿cómo se aplica esa protección a los datos a los que accede y que recopila, procesa y almacena el personal humanitario, y los bienes que se utilizan en operaciones humanitarias? 3. ¿Qué riesgos específicos emanan de las actividades relacionadas con TIC con respecto a la prohibición de la violencia sexual y/o el reclutamiento o uso ilícito de niños en las hostilidades? ¿Qué medidas prácticas adopta o considera adoptar su Estado para prevenir y abordar esos actos ilícitos?	
Sesión 4: Protección de las personas civiles y otras personas protegidas en virtud del DIH ante la propagación de información que entrañe una violación del DIH durante los conflictos armados	15:00 –16:00
Preguntas orientativas 1. ¿Qué límites impone el DIH a la propagación de información por medio de actividades relacionadas con TIC en conflictos armados? Considere, por ejemplo, una campaña de información de una de las partes en el conflicto en cuyo marco: • se publican en internet imágenes de prisioneros de guerra y el trato que reciben; • se redactan y difunden por redes sociales mensajes engañosos que exacerban la tensión entre las comunidades locales, lo que acrecienta el riesgo de violencia. ¿Qué salvaguardias o mecanismos de supervisión ha establecido o considera establecer su Estado para evitar que las personas privadas de libertad se vean expuestas a la curiosidad del público a raíz de actividades relacionadas con TIC? ¿Cómo determina su Estado si las operaciones de información en las que se utilizan TIC constituyen un acto prohibido de promoción o incitación de actos violatorios del DIH, o de propagación del terror entre la población civil? 2. ¿Cómo aborda su Estado el riesgo de que la difusión de que la desinformación promovida con ayuda de las TIC obstruya los servicios de salud o las actividades humanitarias en contextos de conflicto armado? Considere una campaña en internet que hace circular imágenes y publicaciones falsas para afirmar engañosamente que un hospital se está utilizando con fines militares. La desinformación provoca desconfianza entre la población local y genera trastornos en el acceso del personal de salud; por otra parte, el personal que ingresa en las instalaciones sufre cada vez más provocaciones o intimidación. ¿Qué normas del DIH protegen a los servicios médicos y las actividades humanitarias contra la desinformación en la esfera digital? ¿Qué medidas	

jurídicas u operacionales adopta o considera adoptar su Estado para atender estos riesgos? 3. ¿Qué otras medidas toma o considera tomar su Estado a fin de prevenir el uso de las TIC, en particular en redes sociales, para difundir información violatoria del DIH?	
Pausa	16:00 –16:30

Sesión 5: Responder a los riesgos de daño ocasionado por el uso militar de la infraestructura civil de TIC y la participación de personas civiles en actividades relacionadas con TIC en conflictos armados	16:30 –17:30
Preguntas orientativas 1. ¿Cuál es el costo humano y las repercusiones para el DIH del uso militar de infraestructura civil, y qué medidas fundadas en el DIH se deben adoptar con el objeto de mitigar los riesgos asociados para la población civil y los servicios civiles esenciales? Considere un centro de datos comercial que se encuentra en el territorio de un Estado parte en un conflicto armado, y que contiene tanto datos y aplicaciones militares como datos de la población civil y aplicaciones que se usan para la prestación de servicios civiles esenciales. • ¿Cómo aplica su Estado las normas y los principios del DIH, como la distinción, la proporcionalidad y la precaución, al evaluar una operación de TIC contra una infraestructura de TIC con esas características? Si una parte determinada de la infraestructura de TIC, como un servidor, pasa a ser un objetivo militar, ¿cómo deben analizarse los efectos en sus usos civiles al planificar y llevar a cabo una operación de TIC en su contra? • ¿Qué precauciones puede y debe tomar el Estado que lleva adelante la operación de TIC para proteger a la población civil y los servicios civiles esenciales que dependen de la infraestructura de TIC atacada? • ¿Qué precauciones puede y debe tomar el Estado que alberga el centro de datos para proteger a la población y los bienes de carácter civil bajo su control de los efectos de las operaciones de TIC en contra del centro de datos? • ¿Qué precauciones puede y debe tomar la empresa propietaria y encargada del funcionamiento del centro de datos para evitar que los datos civiles se vean afectados por operaciones de TIC dirigidas contra las aplicaciones y datos militares alojados en el mismo centro?	

2. ¿Qué peligros podría entrañar para las personas civiles su participación en actividades relacionadas con TIC en contextos de conflicto armado, y qué medidas fundadas en el DIH se deben adoptar para mitigarlos? Considere las operaciones de TIC que realizan hackers civiles en territorio de una de las partes beligerantes en el contexto de un conflicto armado, diseñadas para desestabilizar las comunicaciones militares o dañar la infraestructura de TIC de empresas privadas, a fin de debilitar la economía del Estado enemigo o causar desazón en la población. • ¿Qué obligaciones jurídicas tienen los hackers civiles en virtud del DIH al realizar cualquier operación de este tipo? • ¿Qué medidas puede adoptar el Estado afectado en contra de estas operaciones de TIC? 3. ¿Qué medidas prácticas toma o considera tomar su Estado para que la población civil de su jurisdicción o que está bajo su control —como los hackers civiles, grupos de hackers o empleados de empresas tecnológicas que realicen actividades en el ámbito de las TIC en relación con un conflicto armado— conozcan y respeten el DIH, y para que conozcan los riesgos asociados con sus actos y estén lo más protegidos posible contra ellos?	
Observaciones finales	17:30 –18:00