JULIO, 2021 | CESIUB VOL.4

EL DERECHO INTERNACIONAL HUMANITARIO Y LAS NUEVAS TECNOLOGÍAS

Producción Académica del Grupo de Trabajo de Derecho Internacional

Imagen de portada. Créditos de la foto: Getty Images en portal de noticias BBC.

Índice

CESIUB
Centro de Estudios Internacionales de la Universidad de Belgrano

GRUPO DE TRABAJO DE DERECHO INTERNACIONAL

Imagen que retrata el trabajo de la ciberdefensa militar estadounidense.
Créditos de la foto: J.M. Eddins Jr., US Air Force

"Las operaciones cibernéticas y el futuro de los conflictos armados."

POR GUILLERMINA VALLEJO Y RAMSÉS SOLANO

Las tragedias y horrores humanitarios de la guerra, impulsaron a las naciones a reflexionar acerca de las reglas políticas y sociales que nos conllevarían a un futuro en el que se mantuviese la paz. El Derecho Internacional Humanitario (en adelante DIH) comprende un conjunto de normas del Derecho Internacional que busca restringir los métodos y medios de guerra que pueden emplear las partes beligerantes en una situación de conflicto armado, así como garantizar la protección de la población y los bienes de carácter civil (Melzer, N., 2019). Si bien reconoce que desde una perspectiva militar puede ser necesario para las partes llevar a cabo ciertas hostilidades, afirma al mismo tiempo, que las acciones bélicas tienen límites con el fin de minimizar el sufrimiento humano causado por los conflictos armados.

Durante el último siglo, el avance de la tecnología se ha exponenciado en todo el globo, ya sea por la necesidad de conectarnos a distancia o por la simple ambición de facilitarnos el trabajo. Sin embargo, pocas veces evaluamos la amenaza que puede llegar a representar para nuestra sociedad. Los datos de millones de civiles están a pocas teclas de búsqueda y que ese sistema no sea impenetrable para agentes externos nos hace dudar si realmente estamos seguros. Los Estados hacen todo lo posible para adaptarse a las nuevas amenazas en un mundo que corre a gran velocidad y, aun así, ¿todos los Estados tienen los recursos para defenderse?

Estos crecientes y cada vez más frecuentes avances tecnológicos nos obligan, entonces, a tomar conciencia de las nuevas amenazas a las que se enfrentan los actores del sistema internacional en consecuencia y a reflexionar sobre la interpretación del DIH para que su aplicabilidad a los conflictos contemporáneos se mantenga fiel a su propósito. Hoy en día, uno de los aspectos que complejizan la conducción de las hostilidades es la expansión de las operaciones militares al ámbito del ciberespacio, producto del accionar de actores estatales y no estatales. No es un dato menor que cada vez más Estados destinen enormes recursos a programas de aplicación militar de nuevas tecnologías, sobre todo, de desarrollo de ciberoperaciones con fines militares. Ahora bien, no sólo es complejo definir la nueva terminología sino que, además, es sumamente difícil arribar a un determinado grado de acuerdo acerca de si el DIH vigente es suficiente, o si se requiere de nuevas normas para poder regular adecuadamente los conflictos armados contemporáneos. A su vez, nunca debemos dejar de preguntarnos cómo el uso de operaciones

cibernéticas, y en particular, el empleo de ataques cibernéticos, afecta a la población y bienes de carácter civil.

A pesar de todo esto, existe un consenso generalizado de que las operaciones cibernéticas vinculadas a un conflicto armado se encuentran reguladas por el DIH. En este sentido, es significativa la posición del Comité Internacional de la Cruz Roja (en adelante CICR) en el documento presentado al Grupo de Trabajo de Composición Abierta sobre los Avances en el campo de la información y las telecomunicaciones en el Contexto de la Seguridad Internacional y al Grupo de Expertos Gubernamentales sobre el Avance del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional de 2019 (en adelante Documento de Posición del CICR). En este documento, se sostiene que "el DIH limita las ciberoperaciones durante los conflictos armados, de la misma manera que limita, el empleo de todas las armas, medios y métodos de guerra en ese marco" dado que "cuando los Estados aprueban tratados de DIH, lo hacen para regular conflictos presentes y futuros" (CICR, 2019, p. 5).

La posición del CICR encuentra sustento en el artículo 36 del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977 (en adelante Protocolo adicional I) que dispone que, al momento de estudiar, desarrollar, adquirir o adoptar una nueva arma, o nuevos medios o métodos de guerra, los Estados contratantes tienen la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el derecho internacional aplicable (Conferencia Diplomática sobre la Reafirmación y el Desarrollo Internacional Humanitario Aplicable en los Conflictos Armados, 1977, Protocolo Adicional a los Convenios de Ginebra de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I)). En este sentido, en su opinión sobre la legalidad de la amenaza o el empleo de armas nucleares de 1996, la Corte Internacional de Justicia (CIJ) señaló que los principios y normas del DIH que regulan los conflictos armados se deberían aplicar a las armas nucleares aunque éstas hayan sido desarrolladas con posterioridad a la entrada en vigencia de los Convenios de Ginebra de 1949 y los Protocolos adicionales de 1977, ya que no hacerlo sería "incompatible con el carácter intrínsecamente humanitario de los principios jurídicos de que se trata, que impregna todo el derecho de los conflictos armados y se aplica a todas las formas de guerra y a todas las clases de armas, las del pasado, las del presente y las del futuro" (CIJ, 1996, párrafos 74-87). Estas son cuestiones significativas ya que considerar que la militarización del ciberespacio también tiene sus límites, impacta directamente en el alcance de la protección que el DIH pretende asegurarle a la población civil y a los bienes del mismo carácter.

El verdadero debate se encuentra en la manera en la cual el DIH se aplica para operaciones cibernéticas vinculadas a un conflicto armado. En el Documento de Posición del CICR, el Comité brinda un detalle respecto de cómo deben interpretarse, desde su perspectiva, los principios y normas establecidos por el DIH en lo referente a operaciones cibernéticas utilizadas en conflictos armados. A modo de ejemplo, se especificó que la prohibición de desarrollar nuevas armas, o nuevos medios o métodos de guerra incompatibles con el DIH, implica

Estados Unidos y Australia firman el primer acuerdo en la historia para desarrollar un campo de entrenamiento cibernético virtual, el Acuerdo de Proyecto de Capacidades de Entrenamiento Cibernético, el 3 de noviembre del 2020.
Créditos de la foto: SGT Sebastian Beurich para US CYBER COMMAND

la prohibición de desarrollar capacidades cibernéticas que puedan emplearse como armas cuyos efectos sean indiscriminados y desproporcionados (Comité Internacional de la Cruz Roja, 2019). Aun con estas precisiones, es lógico que surjan preguntas respecto de la manera en la que estas interpretaciones deben ser puestas en operación. Lo fundamental en este aspecto es que, cualquiera sea el caso, es erróneo suponer que la conducción de operaciones cibernéticas en el marco de un conflicto armado sucede en un vacío legal.

Una de las complejidades que caracteriza la expansión de las actividades militares al ciberespacio es la dificultad para identificar al autor que lleva adelante determinadas operaciones cibernéticas, algo por demás relevante si tenemos en cuenta que para poder determinar la aplicabilidad del DIH a una situación, primero necesitamos identificar que esa situación guarde un vínculo con un conflicto armado. Es más, la atribución de las responsabilidades en caso de que se cometa una violación al DIH necesita de la identificación de los actores correspondientes. No obstante, el documento del CICR recuerda que “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” (CICR, 2019, p.10).

Por otro lado, el CICR considera con especial preocupación la frecuencia de operaciones cibernéticas no vinculadas a conflictos armados que han tendido a alterar, modificar y dañar los sistemas informáticos de los cuales depende cada vez más la infraestructura civil (Comité Internacional de la Cruz Roja, 2019). Existen múltiples casos de operaciones cibernéticas que ponen en peligro el funcionamiento adecuado de redes eléctricas (Rodenhäuser, T., Mačák, K., 2021). Pero, sobre todo, el CICR señala el inmenso costo humano que pueden tener los ataques cibernéticos cuyos objetivos son la infraestructura civil que soporta el suministro de servicios esenciales, particularmente, los de atención médica y sanitaria, si fueran a tener lugar en situaciones bélicas cuando la vulnerabilidad de la población civil se encuentra exacerbada y en la necesidad de ser protegida (Comité Internacional de la Cruz Roja, 2019).

Asimismo, existen otras complejidades; desde la perspectiva de Kubo Mačák (Caltagirone, S., 2019), asesor legal del CICR, los sistemas informáticos de control industrial (ICS por sus siglas en inglés) que sustentan el funcionamiento de infraestructura relacionada con el suministro de servicios esenciales, califican como bienes de carácter civil cuyo ataque se encuentra prohibido. De hecho, cuando estos bienes son considerados, además de civiles, objetos indispensables para la supervivencia de la población como sucede con la infraestructura médica y sanitaria o de suministro de agua potable, el DIH establece una protección aún más amplia. Sin embargo, el DIH reconoce la legalidad de un ataque cibernético dirigido a un bien de carácter civil siempre y cuando este constituya un objetivo militar, algo que no implica únicamente que este bien sea utilizado con fines militares, sino que requiere cumplir con otros criterios como, por ejemplo, que el éxito del ataque implique además una ventaja militar definitiva sobre el enemigo. Aun así, nada de esto elimina la obligación de tomar todas las precauciones posibles para evitar o, al menos, minimizar el daño colateral a la población y a bienes de carácter civil y de no proceder con el ataque si dicho daño resultara excesivo.

Ahora bien, hay que tener en cuenta que en el ciberespacio hay una gran cantidad de redes militares que están interconectadas con redes civiles. Según el CICR, por un lado, hay redes militares que dependen de infraestructura cibernética civil (cables de fibra óptica submarinos, satélites, enrutadores o nodos). Por el otro, hay redes civiles que dependen de infraestructura cibernética militar (por ejemplo, los controles de

tráfico aéreo que dependen de sistemas de navegación satelital). Por ende, existe el riesgo de considerar que muchos de los bienes de carácter civil que forman parte del ciberespacio constituyen objetivos militares. Debido a estos peligros, el CICR recomienda a los actores del ciberespacio diferenciar la infraestructura y las redes y sistemas informáticos civiles de aquellos militares, sobre todo cuando estas se relacionan con servicios e instalaciones que gozan de especial protección, como los hospitales (Comité Internacional de la Cruz Roja, 2019).

En especial, existen dos grandes temas que aún no se han resuelto. Uno de ellos concierne a la definición de ataque en el contexto de las ciberoperaciones, aspecto por demás importante dado que una gran parte de las normas y principios del DIH se aplican exclusivamente a las operaciones que califican como ataques. El Protocolo adicional I establece en su artículo 49 que "se entiende por 'ataques' los actos de violencia contra el adversario, sean ofensivos o defensivos" (Conferencia Diplomática sobre la Reafirmación y el Desarrollo Internacional Humanitario Aplicable en los Conflictos Armados, 1977, Protocolo Adicional a los Convenios de Ginebra de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I)). De esto se deriva, que exista un consenso generalizado en caracterizar como 'ataque' a las operaciones cibernéticas que pueden causar "muertes, heridas o daños físicos". Sin embargo, luego existen diferentes opiniones. Por ejemplo, el CICR incluye dentro de la definición de 'ataque' cibernético a las "ciberoperaciones que ocasionan perjuicio por medio de sus efectos directos e indirectos previsibles" como es el caso de una ciberoperación que, al interrumpir la red de suministro eléctrico de un hospital, ocasiona indirectamente la muerte de alguno de sus pacientes. Por su parte, los expertos que fueron convocados para la elaboración del Manual de Tallin 2.0, una iniciativa del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN, acordaron calificar como 'ataque' cibernético a toda "operación cibernética, ofensiva o defensiva, que se espera de forma razonable cause lesiones o la muerte a personas o daños o destrucción a objetos" (Schmitt, 2019, p.338), aun cuando estos sean consecuencia de un daño colateral.

El debate se produce con respecto a la inclusión de ciberoperaciones que alteran significativamente los servicios esenciales de la población civil sin ocasionar daños físicos y que son el tipo de operaciones cibernéticas más utilizadas. Desde la perspectiva del 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" (CICR, 2019, p.9). En cuanto a los expertos del Manual de Tallin 2.0, una mayoría consideró que la pérdida de funcionalidad solo da lugar a un 'ataque' cuando requiere el reemplazo de componentes físicos (Schmitt, M. N., 2019). Pero esto de ninguna manera zanja la discusión ya que, dentro de esta mayoría, hay quienes definieron esa pérdida de funcionalidad como situaciones en las que los componentes físicos de la infraestructura cibernética deben repararse o reemplazarse, mientras que otros incluyeron las situaciones en las que basta reinstalar el sistema operativo o los datos personalizados de los que el sistema depende para recuperar la funcionalidad (Schmitt, M. N., 2019). Sin embargo, perdura un problema, y es que existen muchas operaciones cibernéticas capaces de ocasionar pérdida de funcionalidad de sistemas informáticos al punto tal de perturbar de forma significativa el desarrollo normal de la vida civil sin causar daños físicos sobre los componentes y sobre las cuales, por consiguiente, no aplicarían los límites del DIH. Michael Schmitt, editor general del Manual de Tallin, opina que esto sería difícil de conciliar con un DIH cuya finalidad es proteger a la población civil del sufrimiento causado por las operaciones que se llevan a cabo durante los conflictos armados (Schmitt, M. N., 2019).

El segundo gran tema de discusión se refiere a la protección de los datos civiles digitalizados. Para el CICR, se entiende que existen datos indispensables para la supervivencia de la población civil, como los datos médicos, que deberían tener una protección específica como sucede durante los conflictos armados con la infraestructura del sector de la salud (Comité Internacional de la Cruz Roja, 2019). Por su parte, la mayoría de los expertos de Tallin 2.0, concluyeron que los datos civiles no son compatibles con la definición del término "objeto" o "bien" que figura en los comentarios de los Protocolos adicionales de 1977 y, por ende, no pueden ser caracterizados como bienes de carácter civil ni contar con la protección reservada para los mismos. En contraste, hubo una minoría de expertos para los cuales la no protección de estos datos sería contraria al objeto del DIH. Para esta minoría, lo que hace que un bien sea caracterizado como un bien de carácter civil protegido por el DIH en situaciones de conflicto armado es "la gravedad de las consecuencias de la operación, no la naturaleza del daño" (Schmitt, 2019, p.341). En este sentido, también el CICR opinó que no prohibir la eliminación o la adulteración de datos esenciales de carácter civil sería algo difícil de conciliar con la finalidad del DIH ya que hoy en día vivimos en un mundo profundamente digitalizado.

En vistas a las dificultades mencionadas y a la actualidad de estos debates, hay quienes rescatan que los Estados pueden en el mientras tanto adoptar por su propia cuenta compromisos destinados a limitar el sufrimiento humano causado por operaciones cibernéticas durante un conflicto armado, aun cuando nada los obliga a hacerlo (Rustici, R. M., 2011). En esta misma línea, Michael Schmitt señala que los Estados pueden abstenerse, en primer lugar, de realizar operaciones cibernéticas contra infraestructura o datos civiles que interfieran con funciones o servicios civiles esenciales. En segundo lugar, pueden privarse de operaciones cibernéticas de las que se prevén efectos negativos sobre la población civil que resultaran excesivos en relación con el beneficio concreto a obtener (Schmitt, 2019).

A modo de conclusión, es fundamental rescatar la trascendencia de aseverar que el DIH regula las operaciones cibernéticas que se emplean como parte de la conducción de las hostilidades en conflictos armados. En todos los ámbitos de la vida los acontecimientos tecnológicos han impactado en la realidad material de las personas. De la misma forma, la tecnología seguirá evolucionando y modificando la manera en la que se desarrollan los conflictos armados en el futuro. Es por esto mismo, que 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" (CICR, 2019, p.2). Para visualizar la importancia de llegar a un consenso, siempre es un buen ejercicio reflexionar acerca de cómo se verían los conflictos armados en el futuro sin una interpretación o evolución del DIH que permita imponer límites al sufrimiento humano.

Reunión del Consejo de Dirección de la Universidad de Defensa Nacional (UNDEF) donde se concretó la creación del Instituto de Ciberdefensa de las Fuerzas Armadas de Argentina, presidida en parte por el entonces Ministro de Defensa, Agustín Rossi.
Crédito de la foto: Estado Mayor Conjunto de las Fuerzas Armadas

"Los Sistemas de Armas Autónomas en su dimensión ética y legal."

POR: MILAGROS DELORENZI Y ANDREA ROMERO SALAZAR

La cuarta revolución industrial nos permitió adentrarnos en un mundo que no hace tantos años, sólo podíamos concebir en historias de ciencia ficción. Hoy, las máquinas han adquirido un nivel de automatización e independencia tal que la tecnología ha logrado posicionarse como un elemento preponderante en muchos aspectos, incluyendo una revolución en el ámbito militar.

En este contexto, el Derecho Internacional Humanitario (DIH) se enfrenta a nuevos desafíos derivados del empleo de Sistemas de Armas Autónomas (AWS) y Sistemas de Armas Autónomas Letales (LAWS), que son el reflejo de la convergencia de tecnologías digitales y físicas. De esta forma, la posibilidad de su implementación en los conflictos armados pone en duda el cumplimiento efectivo de la normativa plasmada en los Convenios de Ginebra de 1949 (CICR, 2014) y sus Protocolos Adicionales.

A pesar de que no existe una definición internacionalmente acordada, el Comité Internacional de la Cruz Roja (CICR) -institución promotora del derecho humanitario **(**DIH**)**- define a los Sistemas de Armas Autónomas como aquellas que "pueden identificar y atacar blancos, es decir, que poseen autonomía en las 'funciones críticas' de adquirir, rastrear, seleccionar y atacar objetivos" (CICR, 2014). La aparición de métodos más rápidos y fuertes que los humanos para la realización de ciertas tareas, tales como los robots, han traído consigo una redefinición del concepto tradicional de los conflictos armados, difuminando las barreras entre lo civil y militar.

Asimismo, la revolución en el campo de la inteligencia artificial y el "machine learning" dio lugar a máquinas aptas para el desarrollo de tareas más específicas. Aunque al día de hoy las armas autónomas continúan requiriendo el control por parte de los humanos, algunos Estados como Rusia o Estados Unidos ya han demostrado sus intenciones de lograr una completa automatización de las operaciones militares (Scharre, 2018; pág 8-9).

El inminente cambio en el desarrollo de los conflictos armados, nos permite diferenciar entre dos espacios claros: por un lado, el área donde se lleva a cabo el combate como tal, y por otro, el lugar desde donde el usuario controla las armas remotas, lejos de la zona real de peligro. Dado que no existe una regulación específica aplicable a estas nuevas armas, las mismas se encuentran enmarcadas únicamente por las limitaciones que impone el DIH vigente, las cuales fueron elaboradas en otro contexto histórico. (CICR, 2020)

El CICR ha demostrado su preocupación en torno a las armas autónomas y cómo estas son utilizadas. La organización identifica dos usos para las mismas: el empleo en la conducción de hostilidades, por un lado, y la utilización durante la acción humanitaria, por otro. Si bien el CICR no se posiciona en contra de las armas autónomas *per sé*, toma en cuenta para qué y de qué forma son utilizadas. En base a ello, asegura que "toda nueva tecnología de guerra debe ser usada en complicidad con las reglas del Derecho Internacional Humanitario" (CICR, 2019; pág. 2).

Teniendo en cuenta que aún no existe una regulación específica aplicable a este campo del DIH, cabe destacar el artículo 36 del Protocolo I de los Convenios de Ginebra de 1949 (CICR, 1977) que señala que "cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante."

La pregunta gira en torno a si las máquinas deberían poder tomar decisiones acerca de la vida o la muerte durante la guerra. Por ello, cuando hablamos de conflictos armados es preciso tener en cuenta tanto la dimensión legal como ética, ya que ambos campos están estrechamente vinculados. Las consideraciones éticas han impulsado en muchas ocasiones la limitación de métodos y medios de la guerra, siendo la Cláusula Martens un buen ejemplo de ello. La misma, considerada como parte del DIH, fue incluida en los Convenios de La Haya de 1899 y 1907 y posteriormente incorporada en los Protocolos adicionales de 1977 a los Convenios de Ginebra de 1949.

Esta cláusula subraya que "en los casos no comprendidos en las disposiciones reglamentarias adoptadas por ellas, las poblaciones y los beligerantes permanecen bajo la garantía y el régimen de los principios del Derecho de Gentes preconizados por los usos establecidos entre las naciones civilizadas, por las leyes de la humanidad y por las exigencias de la conciencia pública" (Ticehurst, 1997). Las armas completamente autónomas, con capacidad de seleccionar y atacar blancos sin necesidad de la intervención humana, ponen en duda el cumplimiento de esta cláusula básica y de los principios de humanidad, tales como el respeto por la vida y la dignidad humana, generando preocupación tanto a nivel legal como moral.

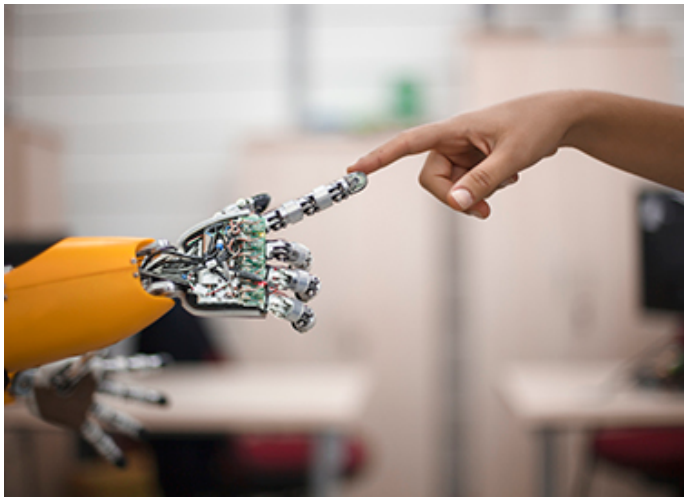
Asimismo, existen una serie de principios en el DIH que se encargan de regular los métodos y los medios de la guerra, los cuales "se aplican a todas las armas nuevas y los desarrollos tecnológicos bélicos, incluidas las armas autónomas" (CICR, 2013). A este respecto, cabe destacar el principio de distinción, plasmado en el artículo 48 del Protocolo Adicional I (CICR: IHL Database, 1977), que establece la necesidad de diferenciar entre civiles y combatientes. Según el mismo, los ataques únicamente podrán estar direccionados hacia objetivos militares y no hacia los bienes civiles. Este es uno de los puntos más controversiales en torno al uso de las armas autónomas, ya que se discute si a través de los sensores que posee un robot se podría distinguir el objetivo al cual ataca.

Un civil enfrentando un tanque de guerra representa la parte ética y moral que se pone en juego en un posible conflicto con armas autónomas. Créditos de la foto: Jonah M. Kessel para The New York Times.

Esto se complementa con la prohibición de ataques indiscriminados y la regla de proporcionalidad. Estos principios aseguran que los ataques estén orientados hacia un objetivo militar específico, previniendo los posibles daños a objetivos civiles de forma indistinta; y buscan evitar ataques que puedan llegar a causar pérdidas incidentales de vidas o bienes civiles considerados excesivos en relación a los hechos concretos y directos, más allá de que estuvieran dirigidos contra un objetivo militar en primer lugar.

El DIH exige la protección de la población civil y bienes civiles, por lo que las partes beligerantes se ven obligadas a tomar precauciones en cuanto a qué objetivos se ataca, los medios y métodos utilizados, la proporción de los ataques y la suspensión de los mismos en caso de no estar dirigidos a un objetivo militar.

Los retos que el desarrollo de los sistemas de armas autónomas presenta para el DIH han sido el centro del debate intergubernamental sobre las tecnologías emergentes y su capacidad letal en el marco de la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados (CCW) de las Naciones Unidas (CIRC, 1981). Actualmente existe un consenso en cuanto al papel que tienen los humanos en el control de estas armas y la importancia de regularlas; pero las posturas aún difieren en lo que respecta a cómo los humanos deberían ejercer la responsabilidad y el control de las mismas.



Una mano humana y otra robótica interactuando ejemplifica la interacción entre humanos y robots si se llegaran a emplear las armas autónomas. Fuente: Association for Advancing Automation

Ahora bien, existen dos grandes posturas en torno a qué tipo y qué grado de control humano es necesario para el cumplimiento de las normas de DIH. Un primer enfoque señala que llegará un punto en el que la tecnología y la programación será tan sofisticada que se le podrán asignar una mayor cantidad de tareas sin necesidad de un alto grado de control humano. De hecho, alegan que estas son ventajosas pues podrán diferenciar a los civiles de los militares de manera más eficiente que un combatiente; destacando la falta de emocionalidad como una ventaja, ya que es algo que puede alterar el juicio de un humano durante el conflicto armado. Asimismo, traen a la mesa el hecho de que los presupuestos militares y las bajas no deseadas se reducirían significativamente. Así, las máquinas inteligentes podrían salvar vidas y hacer de las guerras algo más “humano”. Una segunda visión establece que la autonomía de las armas no es contradictoria con el control humano, sino que debe haber una coexistencia entre ambas. Para esta postura, las normas actuales del DIH requieren que la toma de decisiones se haga en base a las condiciones del contexto y el juicio de una persona capaz de actuar en base a valores éticos y morales. (Boulanin, Davison, Goussac y Peldán Carlsson, 2020; pág. 3-13)

Las preocupaciones en torno a estas nuevas tecnologías reflejan la necesidad de ser reguladas mediante la negociación entre Estados antes de que las mismas sean empleadas en el campo de batalla de manera efectiva (Reniec, 2019). Nos enfrentamos entonces al dilema de Collingridge, que propone dos formas de pararnos frente al desarrollo de la tecnología: llevar a cabo la prohibición o regulación preventiva con el fin de evitar consecuencias indeseables, o bien dejar que se desarrollen para poder observar sus consecuencias, pero en detrimento del poder de regulación.

Esta cuestión es algo que se encuentra presente en las reuniones del Grupo de Expertos Gubernamentales (GGE). Este grupo se estableció en el año 2016 en el seno de Naciones Unidas a partir de la Convención sobre Ciertas Armas Convencionales (CCW) anteriormente mencionada. Su función gira en torno al intercambio de opiniones y ahondamiento en las diversas dimensiones que tiene el campo de los sistemas de armas autónomos en correlación con los objetivos de la Convención (UNDOCS, 2017). Los expertos que lo conforman se posicionan a favor de una regulación preventiva antes de que las grandes potencias se aboquen al desarrollo pleno de las mismas, invirtiendo tiempo y recursos financieros. Sin embargo, la falta de consenso se refleja en la definición del grado de autonomía necesario que estas armas deben alcanzar para que se conviertan en un problema.

No caben dudas de que las armas autónomas llegarán para quedarse y posiblemente emprenderán "la tercera revolución en la guerra después de la pólvora y las armas nucleares¨ (Knight, 2017).

Muchas veces la realidad supera la ficción y los avances en el campo de la inteligencia artificial y “machine learning” son un fiel reflejo de ello. Si bien cada postura respecto a la incorporación de Sistemas de Armas Autónomas a los conflictos armados es respetada y tiene sus puntos válidos, es cierto que, según las normas vigentes del DIH y el estado actual de los avances tecnológicos, es difícil asegurar el cumplimiento de los principios de distinción, proporcionalidad y precaución que promueve el CICR. Esto ha dado pie a una serie de preguntas y debates en el plano ético y legal acerca de la responsabilidad en cuanto a la utilización de estas máquinas. Ante tal situación, y frente a los inminentes cambios en los conflictos armados contemporáneos, los expertos deberán trabajar en conjunto con los Estados para encontrar una “ventana de viabilidad” que permita arribar a un consenso.

Armas semiautónomas y su injerencia en el espacio aéreo.
Créditos de la foto: Shutterstock para UNSW Sydney

De Actualidad

POR: JULIETA RODRÍGUEZ LEUMANN, CAMILA AVENDAÑO CAVALLO Y MARTINA BLANCO

Corte Internacional de Justicia

El 31 de mayo de 2021 la Corte de Justicia Internacional anunció el fallecimiento del Juez Richard Crawford. De nacionalidad australiana, dedicó su vida a las leyes obteniendo a lo largo de su carrera importantes títulos de las Universidades de Adelaida y Oxford, así como posgrados en varias universidades de Europa. Su trayectoria en el campo del Derecho Internacional fue sobresaliente. Su impecable trabajo jurídico queda plasmado en libros, informes oficiales y artículos académicos de su autoría, material de consulta para los profesionales y estudiantes del derecho. Sin dudas será recordado como un importante baluarte de las ciencias jurídicas.

Para más información visitar: https://www.icj-cij.org/public/files/press-releases/0/000-20210531-PRE-01-00-EN.pdf

Corte Penal Internacional

El 16 de junio de 2021, el Sr. Karim Asad Ahmad Khan, quien había sido electo el 12 de febrero del corriente año, asumió el cargo de Fiscal de la Corte Penal Internacional. Conforme al artículo 45 del tratado fundacional de la CPI, el Estatuto de Roma, la ceremonia fue celebrada en audiencia pública y presidida por el juez Piotr Hofmański. El presidente expresó el rol esencial que cumple el Fiscal. Asimismo, el Sr. Khan prestó juramento y emitió sus primeras declaraciones como Fiscal agradeciendo la oportunidad y afirmando que hará su mayor esfuerzo para cumplir con sus nuevas responsabilidades.

Para más información visitar: https://www.icc-cpi.int/Pages/item.aspx?name=pr1598

Mecanismo Residual Internacional de los Tribunales Penales

El 8 de junio de 2021 se confirmó la sentencia definitiva del excomandante militar serbobosnio Ratko Mladic, mediante el Mecanismo Residual Internacional de los Tribunales Penales (IRMCT) de la ONU. Aquel fue condenado a cadena perpetua por cometer crímenes de lesa humanidad y genocidio durante la Guerra de los Balcanes, por el asedio a Sarajevo en 1992 y la matanza de Srebrenica en 1995. Mladic, asistido por Serbia, logró fugarse durante 15 años, aunque luego fue arrestado en 2011 en Lazarevo siendo finalmente recluido en la unidad de detención de la ONU en La Haya. A pesar de que los abogados de Mladic negaban su responsabilidad acerca de algunos actos puntuales, la IRMCT dictaminó en contra de dichas alegaciones.

Para más información visitar: https://www.irmct.org/sites/default/files/case_documents/210608-appeal-judgement-JUD285R0000638396-mladic-13-56-en.pdf

FUENTES

“Las operaciones cibernéticas y el futuro de los conflictos armados.”

- Caltagirone, S., (3 de diciembre de 2019), Industrial cyber attacks: a humanitarian crisis in the making, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2019/12/03/industrial-cyber-attacks-crisis/
- Comité Internacional de la Cruz Roja, (2019), Documento de Posición del CICR, Derecho internacional humanitario y ciberoperaciones durante conflictos armados.
- Conferencia Diplomática sobre la Reafirmación y el Desarrollo Internacional Humanitario Aplicable en los Conflictos Armados (1977), Protocolo Adicional a los Convenios de Ginebra de agosto de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales (Protocolo I).
- Corte Internacional de Justicia, (1996), Opinión consultiva del 8 de julio de 1996 sobre la legalidad de la amenaza o el empleo de armas nucleares.
- Durham, H., (26 de marzo de 2020), Cyber operations during armed conflict: 7 essential law and policy questions, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/
- Gisel, L., Rodenhäuser, T., Dörmann, K., Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts, International Review of the Red Cross (2020), 109 (913), 287-334, Digital technologies and war, disponible en https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf
- Gisel, L., Rodenhäuser, T., (28 de noviembre de 2019), Cyber operations and international humanitarian law: five key points, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/
- Informe del Comité Internacional de la Cruz Roja, (octubre de 2018), The Humanitarian Metadata Problem: “Doing no harm” in the digital era.
- Los Convenios de Ginebra del 12 de agosto de 1949, (2012), Ginebra, Suiza, Comité Internacional de la Cruz Roja, disponible en https://www.icrc.org/es/doc/assets/files/publications/convenios-gva-esp-2012.pdf
- Mačák, K., Jančárková, T., Minárik, T., (6 de octubre de 2020), The right tool for the job: how does international law apply to cyber operations?, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/
- Mačák, K., Rodenhäuser, T., Gisel, L., (2 de abril de 2020), Cyber attacks against hospitals and COVID-19 pandemic: How strong are international law protections, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2020/04/02/cyber-attacks-hospitals-covid-19/
- Marelli, M., Perrig, A., (7 de mayo de 2020), Hacking humanitarians: mapping the cyber environment and threat landscape, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2020/05/07/hacking-humanitarians-mapping-cyber-environment/
- Melzer, N., (2019), Derecho Internacional Humanitario Una Introducción Integral, Ginebra, Suiza, Comité Internacional de la Cruz Roja.
- OEA, Comité Jurídico Interamericano (noviembre de 2020), Derecho Internacional y Operaciones Cibernéticas del Estado, disponible en http://www.oas.org/es/sla/cji/docs/Derecho_Internacional_y_Operaciones_Cibern%C3%A9ticas_del_Estado_publicacion.pdf
- Protocolos Adicionales a los Convenios de Ginebra de 1949 del 12 de agosto de 1949, (2012), Ginebra, Suiza, Comité Internacional de la Cruz Roja, disponible en icrc-003-0321.pdf
- Rodenhäuser, T., Mačák, K., (9 de marzo de 2021), Even ‘cyber wars’ have limits. But what if they didn’t?, ICRC Humanitarian Law and Policy blog, disponible en https://blogs.icrc.org/law-and-policy/2021/03/09/even-cyber-wars-have-limits/
- Rustici, R. M., (2011), Armas Cibernéticas: La igualdad de condiciones a nivel internacional, originalmente publicado en inglés en la revista Parameters, disponible en https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20120831_art006SPA.pdf
- Schmitt, M. N., (abril de 2019), Wired warfare 3.0: Protecting the civilian population during cyber operations, International Review of the Red Cross No. 910, disponible en https://international-review.icrc.org/sites/default/files/reviews-pdf/2019-12/irrc_101_910_17.pdf
- Stoll, P., (7 de diciembre de 2018), Los rastros digitales podrían poner en peligro a las personas que reciben asistencia humanitaria: informe del CICR y Privacy International, disponible en https://www.icrc.org/es/document/los-rastros-digitales-podrian-poner-en-peligro-las-personas-que-reciben-asistencia
- 32ª Conferencia Internacional de la Cruz Roja y de la Media Luna Roja, (diciembre de 2015), Cuarto informe sobre el derecho internacional humanitario y los desafíos de los conflictos armados contemporáneos preparado por el CICR, Ginebra, Suiza.

"Los Sistemas de Armas Autónomas en su dimensión ética y legal"

- CICR: Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados, abierta a la firma el 10 de abril de 1981, entró en vigor el 2 de diciembre de 1983. Recuperado de: https://www.icrc.org/es/doc/resources/documents/misc/5tdl6d.htm
- Comité Internacional de la Cruz Roja: Armas autónomas: los Estados deben abordar importantes retos humanitarios y éticos. 02-09-2013. Recuperado de: https://www.icrc.org/es/doc/resources/documents/faq/q-and-a-autonomous-weapons.htm
- Comité Internacional de la Cruz Roja: Artificial intelligence and machine learning in armed conflict: A human-centred approach. Geneva, 6 June 2019. Recuperado de: https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach
- Comité Internacional de la Cruz Roja: Empleo De Armas Y Equipamiento En Las Operaciones Para Hacer Cumplir La Ley. Mayo 2020. Recuperado de: Https://Www.Icrc.Org/Es/Document/El-empleo-de-armas-y-equipamiento-en-las-operaciones-para-hacer-cumplir-la-ley
- Comité Internacional de la Cruz Roja: Expert meeting. Autonomous weapons systems technical, military, legal and humanitarian aspects. Geneva, Switzerland 26 to 28 March 2014. Recuperado de: https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014
- Convenios de Ginebra de 1949 y sus Protocolos adicionales. Aprobado el 12 de agosto de 1949 por la Conferencia Diplomática para Elaborar Convenios Internacionales destinados a proteger a las víctimas de la guerra, celebrada en Ginebra del 12 de abril al 12 de agosto de 1949. Entrada en vigor: 21 de octubre de 1950. Recuperado de: https://www.icrc.org/es/document/los-convenios-de-ginebra-de-1949-y-sus-protocolos-adicionales
- Neil C. Reniec: Autonomous Weapons Systems: When is the right time to regulate? 26 de septiembre de 2019. Recuperado de: https://blogs.icrc.org/law-and-policy/2019/09/26/autonomous-weapons-systems-right-time-regulation/
- Paul Scharre: Army of None: Autonomous Weapons and the Future of War. 2018. Pág. 8-9
- Protocolo Adicional I de 1977 a los Convenios de Ginebra, artículo 48. CICR: IHL Database. Practice Relating to Rule 1. The Principle of Distinction between Civilians and Combatants. Recuperado de: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_cou_ch_rule1
- Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales. Sección 1: Métodos y medios de la guerra, artículo 36 sobre armas nuevas. 8 de junio de 1977. Recuperado de: https://www.icrc.org/es/document/protocolo-i-adicional-convenios-ginebra-1949-proteccion-victimas-conflictos-armados-internacionales-1977#GUERRA
- Rupert Ticehurst: La cláusula de Martens y el derecho de los conflictos armados. Revista Internacional de la Cruz Roja. 31-03-1997. Recuperado de: https://www.icrc.org/es/doc/resources/documents/misc/5tdlcy.htm
- UNDOCS: Grupo de Expertos Gubernamentales de las Altas Partes Contratantes en la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados. 22 de diciembre de 2017. Recuperado de: https://undocs.org/pdf?symbol=es/CCW/GGE.1/2017/3
- Vincent Boulanin, Neil Davison, Netta Goussac y Moa Peldán Carlsson: Limits on Autonomy in Weapons Systems. Identifying Practical Elements of Human Control. Stockholm International Peace Research Institute, International Committee of the Red Cross. 2020. Pág. 3-13
- Will Knight: ¿Pueden los robots militares tomar el control? MIT Technology Review (2017, 17 agosto). Recuperado de: https://www.technologyreview.es//s/5068/pueden-los-robots-militares-tomar-el-control

Actualizaciones Jurisprudenciales:

- https://www.irmct.org/sites/default/files/case_documents/210608-appeal-judgement-JUD285R0000638396-mladic-13-56-en.pdf
- https://www.icc-cpi.int/Pages/item.aspx?name=pr1598
- https://www.icj-cij.org/public/files/press-releases/0/000-20210531-PRE-01-00-EN.pdf

DATOS DEL GRUPO DE TRABAJO

Director del CESIUB: Patricio DeGiorgis

Coordinación Académica: Eduardo Diez y Dalma Varela

Tutora a cargo: Natalia L. Loscocco

Tutora adjunta: Valeria M. Allo

Coordinadora: Agustina Eugenia Castro

Miembros: Andrea Romero Salazar, Camila Avendaño Cavallo, Guillermina Vallejo, Julieta Rodriguez Leumann, Milagros Delorenzi, Valentina Pellaquim Radice, Ramsés Solano Bastidas y Martina Blanco.

Contacto: derechointernacionalcesiub@gmail.com