FACULTAD DE DERECHO Y

CIENCIAS SOCIALES DE LA

UNIVERSIDAD DE BELGRANO

LICENCIATURA EN RELACIONES INTERNACIONALES

Director: Lic. Pablo Dons

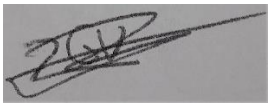
Trabajo final de carrera: Evolución y estado actual de los debates del Derecho Internacional Humanitario en el ciberespacio.

Alumna: GUILLERMINA VALLEJO

Matrícula: 10228475

Profesora tutora: NATALIA L. LOSCOCCO

Año: 2023



Índice

Agradecimientos

A la Universidad de Belgrano, por formarme en su Casa de estudios y por darme la oportunidad de contar con una carrera universitaria en una disciplina que llena mis ansías de vocación en esta vida.

A todos los profesores de la Universidad, por transmitir su pasión en cada una de las asignaturas de la carrera y por estimular la curiosidad y el interés de quienes pasamos por sus aulas.

A mi tutora, la profesora Natalia L. Loscocco, por ser uno de esos profesores que te regalan su conocimiento y experiencia de la forma más desinteresada y generosa posible, por su paciencia al momento de acompañarme en el proceso que fue la realización de este trabajo final de carrera y por el cariño y la dedicación con la que me impartió algunas de las enseñanzas más valiosas que llevo conmigo para afrontar el resto de mi vida profesional.

A mis amigos y mis compañeros, por enfrentar junto a mí lado los desafíos y oportunidades que conllevan ser un estudiante universitario y por enriquecerme con sus opiniones y perspectivas.

A mis padres, Eduardo y Susana, por brindarme la oportunidad de estudiar, por tenderme la mano en los momentos de preocupaciones, por alentarme en cada una de las pequeñas victorias, por inculcarme los valores, la confianza, el orgullo y la empatía necesarios para poder terminar una carrera universitaria y seguir creciendo como profesional.

A mis hermanos, Emiliano y Gerónimo, por escuchar mis inquietudes, por compartir sus propias experiencias y por ofrecerme consejo.

Capítulo I: Análisis de la propuesta de investigación y metodología de estudio

Introducción

Hoy en día, las ciberoperaciones durante conflictos armados, entendidas éstas como "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 método o medio de guerra en el contexto de un conflicto armado" (CICR, 2019a, p. 4, nota al pie 4), ocupan un lugar muy alto en la agenda internacional. Esto se debe a que, aunque pocos Estados reconocen haber recurrido a ciberataques en apoyo de sus operaciones militares, el Comité Internacional de la Cruz Roja (en adelante CICR) calcula que más de cien Estados han desarrollado o están desarrollando capacidades militares informáticas (CICR, 2019a).

Todo apunta a que las ciberoperaciones se han vuelto un medio cada vez más prevalente en los conflictos armados contemporáneos y, como con cada nuevo método o medio de guerra emergente, ha crecido la preocupación dentro de los círculos de expertos en el Derecho Internacional Humanitario (en adelante DIH) y en las Relaciones Internacionales respecto de las consecuencias que tiene esta nueva forma de llevar a cabo las hostilidades para la población y los bienes de carácter civil afectados por un conflicto armado. Los avances tecnológicos en materia militar resultan alarmantes, fundamentalmente a la luz de sucesos que, en los últimos años, dejaron en evidencia que la infraestructura civil y los servicios vitales, determinantes para el funcionamiento normal de los Estados, resultan particularmente vulnerables al ataque de ciberoperaciones durante conflictos armados.

La infraestructura civil y de servicios esenciales está actualmente digitalizada y conectada: redes de suministro de electricidad, sistemas de abastecimiento de agua, hospitales, industrias, telecomunicaciones, transporte, sistemas gubernamentales y sistemas financieros dependen cada vez más de las nuevas tecnologías. Lo mismo sucede con los datos civiles esenciales: datos médicos, biométricos, de registros impositivos, de cuentas bancarias y de registros de elecciones. Sin embargo, ninguna de las infraestructuras y redes de datos mencionados suelen estar adecuadamente protegidos frente a la posibilidad de un ciberataque que, intencional o accidentalmente, es capaz de paralizar toda actividad pública y privada, así como interrumpir la provisión de servicios esenciales para la supervivencia y protección de una población civil afectada por el desenlace de un conflicto armado[1]. Incluso los programas de ayuda humanitaria

[1] Ejemplos de ello se encuentran en v. "Stuxnet (2010)" en Kubo Mačák, Tomáš Minárik y Taťána Jančárková (eds.), Cyber Law Toolkit, disponible en https://cyberlaw.ccdcoe.org/; "Steel mill in Germany (2014)" en Kubo Mačák, Tomáš Minárik y Taťána Jančárková (eds.), Cyber Law Toolkit, disponible en https://cyberlaw.ccdcoe.org/; "Power grid cyberattack in Ukraine (2015) en Kubo Mačák, Tomáš Minárik y Taťána Jančárková (eds.), Cyber Law Toolkit, disponible

pueden verse interrumpidos e incapacitados por un ciberataque ya que la asistencia depende cada vez más de la recolección de información digital que permita a las organizaciones comunicarse con el personal humanitario desplegado en zonas o situaciones de conflicto, por un lado, y con las poblaciones civiles afectadas, por el otro.

Ahora bien, existe un amplio consenso entre expertos y Estados respecto a que las ciberoperaciones durante los conflictos armados no se desenvuelven en un vacío legal, sino que se rigen por el Derecho Internacional Humanitario. Esto se debe a que los Estados, al aprobar tratados de DIH, lo hacen para regular tanto conflictos presentes como futuros, de forma tal que los mismos tratados prevén en sus normas el desarrollo de nuevos medios y métodos de guerra sobre los cuales aplicarán. Un ejemplo de ello es el artículo 36 del Protocolo adicional I a los Convenios de Ginebra del 8 de junio de 1977 que establece la necesidad de revisar la legalidad de los nuevos medios y métodos de guerra desarrollados a futuro a la luz del Derecho Internacional Humanitario. Asimismo, la opinión consultiva emitida por la Corte Internacional de Justicia (en adelante CIJ) sobre la legalidad de la amenaza o del empleo de armas nucleares, recuerda que las normas y los principios del DIH aplicables en los conflictos armados rigen para todas las formas de guerra y todos los tipos de armas, incluso las del futuro. Esta misma posición es apoyada, a su vez, por el CICR.

No obstante, considerando que para la comunidad internacional no es sólo importante afirmar la aplicabilidad del DIH a las ciberoperaciones durante los conflictos armados, sino también arribar a un consenso universal sobre la manera en que se aplican las normas vigentes y si el derecho que rige es adecuado y suficiente, este trabajo pretende explorar aquellas preocupaciones relativas a la naturaleza de las hostilidades en el ciberespacio que suscitan debate entre Estados y expertos.

Tema de investigación

El tema de investigación que se pretende llevar a cabo para este trabajo final de carrera versa sobre las normas que establece el Derecho Internacional Humanitario con el fin de regular los métodos y medios de guerra que pueden emplear las partes beligerantes en una situación de conflicto armado, así como para garantizar la protección de la población y los bienes de carácter civil, en particular, la adecuación de estas normas a los conflictos armados contemporáneos caracterizados por el empleo de operaciones cibernéticas.

Pregunta y problema de investigación

En cuanto al problema de investigación, el trabajo pretende demostrar que las normas vigentes del Derecho Internacional Humanitario resultan inadecuadas para la nueva naturaleza de las guerras. Dicha problematización del tema de investigación derivó de la siguiente pregunta: ¿Bajo

---

en https://cyberlaw.ccdcoe.org/; e "Industroyer – Crash Override (2016)" en Kubo Mačák, Tomáš Minárik y Taťána Jančárková (eds.), Cyber Law Toolkit, disponible en https://cyberlaw.ccdcoe.org/.

qué circunstancias puede una operación cibernética por sí sola desencadenar la aplicación del Derecho Internacional de los Conflictos Armados (en adelante DICA)?

Justificaciones

Considero que la investigación desarrollada es de gran relevancia para las Relaciones Internacionales debido a que el uso de operaciones cibernéticas como medio y método en los conflictos armados y la cuestión de cómo se aplica del DIH a dichas operaciones ha evolucionado considerablemente en los últimos veinte años. Desde el punto de vista operativo, la utilización de operaciones cibernéticas se ha vuelto una característica distintiva de los conflictos armados contemporáneos. Habiendo tomado consciencia de este nuevo cambio en la naturaleza de los enfrentamientos, un número cada vez mayor de Estados, incluidos los cinco miembros permanentes del Consejo de Seguridad de la Organización de las Naciones Unidas (en adelante ONU), han desarrollado capacidades militares cibernéticas (UNIDIR, 2013; Craig, 2018).

Este fenómeno tiene importantes implicancias jurídicas y políticas porque, aunque los Estados han llegado a algunos acuerdos sobre determinados aspectos del régimen normativo que rige las operaciones cibernéticas, la cuestión de la aplicación del DIH a las mismas sigue siendo objeto de intensos debates. Hay cuestiones fundamentales que siguen siendo controvertidas sobre las cuales o bien no hay acuerdo entre los Estados o bien es necesario profundizar en el análisis. Por ello, si bien mi intención con este trabajo es profundizar en la temática, el mismo no está orientado a analizar todas las cuestiones controvertidas que emergen de la evolución del uso de ciberoperaciones ni todos los debates pertinentes por expertos gubernamentales y no gubernamentales, objetivos muy ambiciosos a los fines de la presente tesina. En cambio, este trabajo se limita a investigar la temática de las operaciones cibernéticas como desencadenantes de un conflicto armado y, por ende, de la aplicabilidad del DIH sobre la cuestión.

Objetivo general y objetivos específicos

El objetivo general de la presente investigación consiste en analizar el alcance y la aplicabilidad del DIH frente a la progresiva militarización del espacio cibernético durante conflictos armados. En particular, este trabajo pretende determinar bajo qué circunstancias puede, de ser pasible, el empleo de operaciones cibernéticas por actores estatales y no estatales atravesar los umbrales de intensidad y organización requeridos en las hostilidades para dar lugar al inicio de un conflicto armado, independientemente de su carácter internacional o no internacional.

Los objetivos específicos que se persiguen con este trabajo consisten en:

1. Comparar la naturaleza de las partes que participan en las hostilidades, la intensidad de la violencia que desencadena la aplicabilidad del DIH y las normas de éste aplicables a los dos tipos de conflicto armado identificados por la normativa internacional.
2. Evaluar la aplicabilidad del DIH a las operaciones cibernéticas.

3. Determinar bajo qué circunstancias específicas pueden las operaciones cibernéticas desencadenar conflictos armados internacionales y no internacionales, en virtud de los requisitos establecidos por los Artículos 2 y 3 comunes a los cuatro Convenios de Ginebra de 1949
4. Analizar los desafíos de aplicar las disposiciones del DIH a los conflictos armados contemporáneos caracterizados por el cada vez más prevalente uso de operaciones cibernéticas.

Hipótesis

Considerando lo ya descrito, planteo la siguiente hipótesis: Las operaciones cibernéticas, que acompañan operaciones cinéticas o se emplean en ausencia de ellas, pueden desencadenar conflictos armados internacionales y no internacionales.

Diseño metodológico

Como se mencionó anteriormente, el objetivo general de este trabajo consiste en evaluar bajo qué circunstancias puede el empleo de operaciones cibernéticas por actores estatales y no estatales atravesar los umbrales de intensidad y organización requeridos en las hostilidades para dar lugar al inicio de un conflicto armado internacional y no internacional; esto a la luz de los artículos 2 y 3 comunes a los cuatro Convenios de Ginebra de 1949. Para ello, se utilizará una metodología de análisis cualitativa, descriptiva y explicativa. No obstante, esto no quita que durante la realización de este trabajo se utilicen datos secundarios de carácter cuantitativo, tales como estadísticas que complementen la comprensión del avance de este fenómeno. Asimismo, se van a citar casos para ilustrar los aspectos más relevantes y problemáticos de aplicar en la práctica el DIH a operaciones cibernéticas.

Capítulo II: Antecedentes y consideraciones teórico-conceptuales

Estado del arte

Al encarar este trabajo, encontré una amplia y diversa cantidad de bibliografía correspondiente a la temática planteada. Gracias a las delimitaciones del problema de investigación y del marco conceptual a utilizar, pude adecuar los aportes de la bibliografía y fuentes consultadas a mis objetivos de investigación. Esto me permitió enriquecer y definir mi abordaje al trabajo final de carrera de grado, trabajo en el cual pretendo, desde mi humilde lugar de estudiante, contribuir a una mirada internacionalista sobre la naturaleza cibernética de los conflictos armados contemporáneos predominantes en la escena internacional y, en paralelo, la tendencia de éstos a tensionar el entendimiento de los tomadores de decisiones y expertos en la temática acerca de la manera en qué las normas del DIH deben regular la conducta de las partes beligerantes.

De acuerdo con la bibliografía general y clásica sobre nuestra disciplina, acudí a varias obras y trabajos de ciertos autores que deben destacarse. *¿Un mundo unipolar, multipolar o apolar? La naturaleza y la distribución del poder en la sociedad internacional contemporánea* de José Antonio Sanahuja Perales fue utilizado para sumar al análisis de la temática planteada a partir de expertos del Derecho Internacional, un análisis sobre la estructura básica del sistema internacional, terreno en el cual se producen los conflictos armados. En igual sentido, los libros *Handbook of International Relations* de Walter Carlsnaes, Thomas Rise y Beth A. Simmons y *Global Politics* de Andrew Heywood me fueron sumamente útiles para tener un panorama básico pero completo de la disciplina de las Relaciones Internacionales y sus diferentes teorías. Asimismo, *World Order* de Henry Kissinger me permitió revisar tanto las dinámicas principales de las relaciones entre Estados a lo largo de los años, como las características propias del contexto internacional actual, por uno de los personajes más trascendentales en la disciplina.

A su vez, los conceptos clave de “sensibilidad” y “vulnerabilidad” fueron tomados de la teoría de la interdependencia compleja, desarrollada en *Power and Interdependence* de Robert Keohane y Joseph Nye. Los mismos me sirvieron al momento de estructurar los efectos que tiene el despliegue cada vez más omnipresente de las operaciones cibernéticas en el contexto de los conflictos armados sobre los Estados y la población civil. Otro concepto importante de estos autores para el abordaje de ese trabajo fue la analogía de la distribución de poder en el sistema internacional como un “tablero de ajedrez tridimensional”, así como la ampliación de la visión estatocéntrica del poder.

Además, *The Tragedy of Great Power Politics* de John J. Mearsheimer y *Realism and the Present Great Power System: Growth and Positional Conflict Over Scarce Resources* de Randall Schweller fueron utilizados para comprender los principios fundamentales del realismo ofensivo

y defensivo, corrientes dentro de la teoría neorrealista clásica que me resultaron clave para comprender el desenlace del conflicto en la política internacional. También recurrí a *Politics Among Nations: The Struggle for Power and Peace* de Morgenthau para entender las bases de la corriente realista y hacer uso de su concepto del poder.

Por otra parte, como fuentes fundamentales del Derecho Internacional Humanitario, utilicé como base para esta investigación la lectura de las cuatro Convenciones de Ginebra de 1949[2], de los cuales son parte casi todos los Estados del sistema internacional, y sus tres Protocolos adicionales[3]. Al mismo tiempo, incorporé otros tratados que desempeñan una función importante en la codificación del Derecho Internacional Humanitario y su aplicabilidad. Algunos de estos documentos prohíben el uso de ciertas armas y tácticas militares, mientras que otros protegen a ciertas categorías de personas o de bienes. Estos fueron: la Convención de la Haya de 1954 para la protección de los bienes culturales en caso de conflicto armado y sus dos Protocolos adicionales; la Convención de 1972 sobre Armas Bacteriológicas; la Convención de 1976 sobre Técnicas de Modificación Ambiental con Fines Militares u otros Fines Hostiles; la Convención de 1980 sobre Ciertas Armas Convencionales y sus cinco Protocolos; la Convención de 1993 sobre Armas Químicas; la Convención de 1997 sobre las Minas Antipersonal; el Estatuto de Roma de 1998; el Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la participación de niños en los conflictos armados; y la Convención de 2008 sobre Municiones en Racimo.

De forma complementaria, utilicé el manual de *Derecho Internacional Humanitario: una introducción integral* del Comité Internacional de la Cruz Roja (compilación a cargo de Nils Melzer). Este libro ofrece una introducción sumamente completa a los fundamentos del DIH, su lugar en el Derecho Internacional contemporáneo y su interrelación con otras ramas de este último, sus características básicas y su ámbito de aplicación personal, geográfico y temporal.

Otra bibliografía central para la base de mi análisis en ese trabajo fueron *Weapons and the Law of Armed Conflict (Second Edition)* de William Boothby, *Cyber Operations and International Law* de François Delerue y *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* del Centro de Excelencia de Defensa Cibernética Cooperativa de la Organización del Tratado del Atlántico Norte (en adelante OTAN). El libro de Boothby me resultó útil y de fácil lectura ya que

[2] Los cuatro Convenios de Ginebra de 1949 comprenden los siguientes tratados: I Convenio de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña; II Convenio de Ginebra para aliviar la suerte que corren los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar; II Convenio de Ginebra relativo al trato debido a los prisioneros de guerra; y IV Convenio de Ginebra relativo a la protección debida a las personas civiles en tiempo de guerra.

[3] Los Protocolos adicionales a los cuatro Convenios de Ginebra se componen de: El Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977; el Protocolo II adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional de 1977; y el Protocolo III adicional a los Convenios de Ginebra de 1949 relativo a la aprobación de un signo distintivo adicional de 2005.

reúne en un solo volumen gran parte del DIH, tanto convencional como consuetudinario, que regula los medios de guerra e interpreta la evolución de las normas a futuro. A su vez, incluye los conceptos centrales y estrategias definidas en los manuales internacionales sobre el derecho aplicable a la 'guerra cibernética'.

Por su parte, el libro *Cyber Operations and International Law de* Delerue ofrece un análisis exhaustivo del Derecho Internacional aplicable a las operaciones cibernéticas patrocinadas por Estados según se trate de ciberoperaciones por debajo del umbral de un conflicto armado (es decir, operaciones cibernéticas en tiempos de paz), ciberoperaciones producidas luego de iniciado un conflicto armado que vienen a complementar las actividades militares cinéticas previas, y ciberoperaciones que desencadenan el inicio de un conflicto armado cuyas operaciones militares se desarrollan pura y exclusivamente en el terreno del ciberespacio. En cambio, el *Manual de Tallin* no analiza las operaciones cibernéticas por debajo del umbral del empleo de la fuerza de un conflicto armado. El manual, que no es vinculante y no representa necesariamente la postura de la OTAN ni la de ninguna otra organización o Estado, refleja en noventa y cinco normas que reafirman la aplicabilidad del DIH a los conflictos cibernéticos, las opiniones de los expertos que participaron a título personal del proyecto, acerca de la manera en que las normas y los principios existentes del Derecho Internacional pueden aplicarse a las operaciones cibernéticas durante un conflicto armado. Asimismo, incorpora argumentos a favor y en contra de las distintas posturas relativas al alcance y aplicación de cada una de las normas elaboradas durante la iniciativa.

Entre algunas de las resoluciones de las Naciones Unidas tenidas en cuenta, destaco aquí las resoluciones de la Asamblea General N° 68/243 del 27 de diciembre de 2013 y N° 0/237 del 23 de diciembre de 2015, que establecen Grupos de Expertos Gubernamentales para que sigan estudiando las amenazas existentes y potenciales en el contexto de seguridad internacional vinculadas a la esfera de la información y las telecomunicaciones. También las normas y medidas de cooperación y construcción de confianza que permitan guiar un comportamiento responsable de los Estados. Asimismo, destaco la Resolución de la Asamblea General N° 76/19 del 8 de diciembre, que reconoce la aprobación por consenso del informe final del 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 del informe final del Grupo de las Naciones Unidas de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Contexto de la Seguridad Internacional.

En lo que hace a artículos académicos, cabe anticipar que todos los mencionados, así como otros que fueron citados a lo largo del trabajo o que son debidamente acreditados en la bibliografía de esta tesis de grado, resultaron de suma importancia para poder nutrir mi

conocimiento en la temática de investigación planteada. Todos ellos habilitaron la realización de este trabajo final de carrera y, en consecuencia, la ampliación de mi formación como profesional.

En primer lugar, hago alusión especial al artículo *Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts* del CICR que describe la evolución durante las últimas dos décadas del uso de las operaciones cibernéticas durante los conflictos armados y de los debates acerca de cómo se aplica el Derecho Internacional Humanitario a dichas operaciones. En segundo lugar, destaco *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law* de Kubo Mačák. Este trabajo presenta los argumentos a favor de una interpretación progresiva de la noción de "objetivo militar" en el DIH, incluyendo los datos informáticos dentro del concepto. En tercer lugar, cabe destacar el artículo *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians* de Cordula Droege, el cual versa sobre las principales problemáticas que se plantean al aplicar el DIH a las nuevas tecnologías.

Por otra parte, hago mención la Guía Interpretativa sobre la Participación Directa en Hostilidades del Comité Internacional de la Cruz Roja. Igualmente, incluyo *The Use of Cyber Force and International Law* de Michael N. Schmit que continúa el trabajo del Manual de Tallin. Por otro lado, incorporo *Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare* de Jeffrey T. Biller y Michael N. Schmitt, artículo que examina los conceptos de 'armas', 'medios' y 'métodos de guerra' aplicados a las operaciones cibernéticas.

Por último, señalo *Decoding Article 8 of the International Law Commision;s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors* de Kubo Mačák, *Cyber Operacions and jus in bello* de Nilz Melzer, *The Notion of Combatancy in Cyber Warfare* de Sean Watts, *Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis* de David Wallace, *Easier Said Than Done: Legal Reviews of Cyber Weapons* de Gary Brown y Andrew Metcalf, *Sovereignty in the Age of Cyber* de Gary P. Corn y Robert Taylor, y *How Cyber Changes the Laws of War* de Jack Goldsmith. Cada uno de estos artículos y publicaciones trata problemáticas específicas que hacen a la evolución del debate de la aplicabilidad del DIH a las ciberoperaciones durante situaciones de conflicto armado y fueron centrales al momento de la realización de esta investigación.

Finalmente destaco la importancia del trabajo de *The Cyber Law Toolkit*, recurso que puso a mi disposición todo un conjunto de herramientas de análisis de un total de 25 escenarios hipotéticos de incidentes cibernéticos, basados en ejemplos reales del contexto internacional actual, con sus respectivos análisis jurídicos a partir de distintas ramas del Derecho Internacional, que sirvieron de referencia para mi propia investigación al momento de estructurar mi análisis.

Marco teórico y marco conceptual

Para la realización de este trabajo resultaron clave varios conceptos y supuestos de distintas teorías de las Relaciones Internacionales, así como definiciones centrales del Derecho Internacional Humanitario y del contexto de la ciberseguridad. A continuación, intentaré realizar un breve repaso de ellos.

Para empezar, el estudio del poder es una parte significativa de las Relaciones Internacionales, si no la más importante. Para José Antonio Sanahua Perales, el **poder** puede definirse como la capacidad de influir o de controlar el resultado de los acontecimientos. Por ende, el poder tiene dos dimensiones características: autonomía, es decir, la capacidad de estar libre de influencias y coacciones externas; e influencia o coacción, es decir, la capacidad de inducir o inhibir determinados comportamientos (Perales, 2008). Sobre la base de esto, podemos decir que un actor tiene poder si se presentan tres escenarios: cuando es capaz de obtener los resultados que espera en caso de un conflicto de intereses con un tercero, cuando es capaz de definir la agenda internacional y cuando es capaz de moldear las ideas, los significados intersubjetivos y los valores que guían las preferencias de los actores en los procesos de toma de decisiones del ámbito internacional.

Precisamente, uno de los máximos exponentes de la **teoría realista clásica**, Hans J. Morgenthau, sostiene la noción de la política internacional como, esencialmente, una **lucha por el poder**. Para este autor, no importa cuáles sean los objetos últimos de una política de un Estado, el objetivo inmediato siempre será el poder ya que es éste el que le permite controlar las mentes y las acciones de otros hombres para, eventualmente, lograr sus objetivos primarios (Morgenthau, 1985). Dentro de la teoría realista, el **neorrealismo ofensivo** de John J. Mearsheimer supone que, aunque la intensidad en la competencia de los Estados puede variar, es imposible erradicar la **potencialidad del conflicto** en las Relaciones Internacionales. La razón de esto es que los Estados, cuyo objetivo principal es garantizar su supervivencia, coexisten en un sistema internacional anárquico en el que no existe una autoridad central que se sitúe por encima de las unidades, capaz de ofrecer protección. Sin embargo, las unidades que componen dicho sistema poseen todas cierta capacidad militar (tengamos en cuenta que los Estados disponen, como mínimo, de un ejército nacional, sea este poderoso o fallido). Esto implica que cada Estado posee la capacidad de infligir daño a otro. Por ende, los Estados, actores racionales que basan su accionar en cálculos de costo-beneficio, optarán por comportarse siempre suponiendo que otros Estados representan potenciales amenazas a su seguridad. Ante la eventual posibilidad de que estalle un conflicto, preferirán desconfiar de sus pares y estar siempre preparados para ir a la guerra. Esto implica concentrar la mayor cantidad de poder en sí mismos que sea posible a través de una serie de medios económicos, diplomáticos y militares que les permitan incrementar su cuota de poder relativo en el sistema. Esto se debe a que

mientras más poder tengo como Estado, mayor es la probabilidad que tengo de disuadir a otro Estado de no agredirme o, en su defecto, mayor es la probabilidad que tengo de ganar en caso de verme involucrado en un conflicto. En otras palabras, la búsqueda de poder de los Estados se debe a que el poder es el medio que les permite lograr cierta seguridad por lo que ningún poder es suficiente (Mearsheimer, 2001).

Por otra parte, la **teoría de la interdependencia compleja** de Keohane y Nye, amplía la visión estatocéntrica de las Relaciones Internacionales, característica de los postulados realistas, y ofrece algunos conceptos centrales para el análisis de este trabajo. Por un lado, Nye destaca que la **distribución de poder** en el sistema internacional debe ser analizada como un "tablero de ajedrez tridimensional": existe un "tablero superior" en el que el poder se entiende como poder militar, pero también existe un "tablero intermedio" en el cual el poder se define en términos económicos y un "tablero inferior" en el que el poder se torna difuso y se escurre cada vez más en manos de actores no estatales que irrumpen en las Relaciones Internacionales (Keohane & Nye, 1998). En otras palabras, hay un tablero militar, otro económico y un tablero transnacional. En este último, la agenda se amplía en torno a amenazas que trascienden la lógica estatal tradicional ya que emergen temas como el crimen organizado, el terrorismo, los ciberataques, el cambio climático y las pandemias, dinámicas sobre las cuales los Estados tienen poco o casi nulo control.

A su vez, Keohane y Nye basan su teoría de la interdependencia en la creciente interconexión entre países y demás actores del sistema internacional que observan como resultado de la mayor cantidad de transacciones internacionales. Empero, la **interdependencia** no se trata únicamente de interconexión; los mayores flujos de dinero, bienes, personas y mensajes que tienen lugar a través de las fronteras nacionales generan situaciones en las que dos o más países, o dos o más actores no estatales, ejercen efectos el uno sobre el otro que implican costos recíprocos, por lo general asimétricos. Dentro del concepto de interdependencia, situación que restringe la autonomía de las partes (aunque no necesariamente en términos iguales) se pueden diferenciar dos efectos: la sensibilidad y la vulnerabilidad. La **sensibilidad** hace referencia a cuán afectado se ve un actor por un acontecimiento externo. En cambio, la **vulnerabilidad** mide la capacidad de respuesta que tiene un actor frente a un hecho externo y en qué medida su capacidad de respuesta le permite superar o sobrellevar el impacto. Entonces, si un actor cuenta con una capacidad de respuesta limitada frente a un acontecimiento externo que lo lleva a seguir experimentando costos aún luego de haber modificado sus políticas, es tanto sensible como vulnerable. En cambio, un actor que se ve afectado por un acontecimiento externo, pero que logra, luego de modificar sus políticas, reducir o eliminar los costos experimentados, es sensible más no vulnerable.

Asimismo, existen diversos autores que han teorizado recientemente sobre el **estado actual de las relaciones internacionales**. Entre estos autores se encuentran Esteban Actis y Nicolás Creus, quienes observan que, aunque no existe relación bilateral más trascendental para la política internacional que la que se da entre los Estados Unidos y China, esta relación no tiene lugar en el contexto de una "nueva Guerra Fría", como algunos expertos sostienen. La relación se da en el contexto de un sistema internacional cuya distribución del poder es bipolar, pero la disputa entre Estados Unidos y China es una disputa intracapitalista ya que compiten dos modelos que, a pesar de presentar formas distintas de estructurar el poder político y económico en una sociedad, son capitalistas: capitalismo liberal y capitalismo político dirigido por el Estado. Además, la disputa se da entre dos países que mantienen el vínculo bilateral más imbricado del mundo en términos de intercambio y flujos de comercio, stocks de inversiones y tenencia de bonos. Hoy en día, el ciberespacio es también uno de los campos en los que se desenlaza la disputa. Es por esto, que no es menor que, en palabras de Actis y Creus, hoy el ciberespacio parezca ser cada vez más chino y menos estadounidense en términos de aplicaciones, componentes y capital (Actis & Creus, 2020).

A su vez, se trata de **una bipolaridad "entrópica"**, concepto que hace referencia a la noción de "entropía" utilizada por Randall Schweller para medir el desorden de un sistema (Actis & Creus, 2020). Este bipolarismo entrópico que caracteriza a las relaciones internacionales refleja un sistema internacional en el que existen dos potencias claramente definidas y, sin embargo, ambas se encuentran lejos de poseer suficiente control sobre su entorno como para evitar la crisis de liderazgo actual debido, en parte, a un proceso paralelo de difusión del poder que se produce a partir de la emergencia de nuevas agendas que incluyen tanto a actores estatales como no estatales.

En cuanto al dominio del ciberespacio, uno de los expertos que teorizó al respecto, fundamentalmente sobre las traducciones políticas de la inteligencia artificial en el siglo XXI, es Eric Sadin. Este autor provee un análisis que permite esclarecer las características de los procesos de desarrollo técnico-económico en curso y las consecuencias de extender la idea de que la intervención de los avances tecnológicos, producto de la acción humana, es un fenómeno imposible de contener. En concreto, podemos decir que, a partir de inicios de la década de 2010, la inteligencia artificial se constituye como uno de los más grandes desafíos que enfrenta la política. Tanto empresas como Estados movilizan todos sus recursos de poder con el fin de posicionarse en la vanguardia del desarrollo de la inteligencia artificial. De hecho, la competencia entre los Estados Unidos y China, los dos grandes polos de poder del actual sistema internacional, se desenvuelve también en el campo de la inteligencia artificial. Ejemplos de esto son los estudios actuales sobre inteligencia artificial que realizan la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA por sus siglas en inglés), la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) y la Secretaría de Defensa de Estados Unidos junto a

toda una red de universidades e institutos de investigación subsidiados por el Estado federal estadounidense (Sadin, 2020). A su vez, son prueba de esto los objetivos planteados por el gobierno de China en sus últimas Hojas de Ruta (Sadin 2020). La misma dirigencia rusa declaró públicamente que la forma de dominar el mundo hoy está definida por la capacidad de un Estado que convertirse en nación líder en el sector de la inteligencia artificial, y un Estado periférico que busca consolidarse como potencias regionales, como los Emiratos Árabes, creó un Ministerio de la Inteligencia Artificial (Sadin, 2020).

Indudablemente, las relaciones internacionales están signadas por una sociedad que varios expertos califican de "*Data Driven Society*", es decir, una sociedad caracterizada por la extensión de tecnologías que sistematizan cada vez más segmentos de la vida humana, por el omnipresente devenir de lo digital y por un régimen de retroalimentación en donde cada evento y cada acción humana se ve sometida a una serie de operaciones digitales precisas.

Respecto del **marco jurídico** de la temática planteada, cabe recordar que el **Derecho Internacional Humanitario** (también conocido como el derecho de los conflictos armados o *jus in bello*) es una rama del Derecho Internacional que regula la conducta de las partes involucradas en un conflicto armado y que busca preservar un mínimo de dignidad humana en tiempos de guerra. Busca que, una vez terminadas las hostilidades, la convivencia entre los distintos grupos humanos previamente enfrentados sea posible. Por tanto, consiste en un conjunto de leyes y normas consuetudinarias que trata de limitar las consecuencias de los conflictos armados y pretende proteger a las personas, ya sean civiles o militares, estén heridas o estén activas en combate.

Para poder mitigar los efectos de la guerra y proteger a estas personas, las partes beligerantes, sean Estados o grupos armados determinados, están obligados a conducir sus hostilidades dentro de ciertos límites legales. En última instancia, el DIH procura encontrar un equilibrio entre dos principios: el principio de humanidad y el principio de necesidad militar. Mientras que el principio de necesidad militar permite el uso de la fuerza necesaria para alcanzar el objetivo de un conflicto, el principio de humanidad prohíbe a las partes de un conflicto infligir sufrimientos, lesiones o niveles de destrucción innecesarios para ganar la guerra (Melzer, 2019). Partiendo de este equilibrio, se desprenden algunos principios operativos que deben aplicar las partes beligerantes en la conducción de sus hostilidades, tales como el principio de distinción, proporcionalidad y prohibición de sufrimientos innecesarios.

En este punto, es importante comprender que el DIH se aplica sólo si existe un conflicto armado, pero no regula si el uso de la fuerza por parte de un Estado contra otro es lícito. La legalidad del uso de la fuerza está regulada por un cuerpo jurídico diferente, el Derecho del Uso de la Fuerza, o *jus ad bellum*. Al mismo tiempo, cabe señalar que el DIH no es el único cuerpo legal que se aplica en situaciones de conflicto armado. El Derecho Internacional de los Derechos Humanos,

por ejemplo, se aplican en tiempos de paz y de guerra. Por otro lado, la iniciación de procesos judiciales para la represión de las violaciones del DIH, son regidos por el Derecho Penal nacional e Internacional. Tal es así, que tanto los tribunales penales ad hoc como la Corte Penal Internacional, se han pronunciado sobre los crímenes de guerra por ser de su competencia.

El DIH se aplica a dos **tipos de conflictos armados**: los conflictos armados internacionales que se producen entre dos o más Estados, y los conflictos armados no internacionales, también denominados a veces en el léxico común como guerras civiles, que suelen producirse dentro de un Estado (Melzer, 2019). En ambos supuestos, las normas jurídicas aplicables son diferentes dado que cada tipología requiere de una respuesta específica, lograda a partir de la evolución del DIH.

Existe un **consenso generalizado** de que **las operaciones cibernéticas vinculadas a un conflicto armado se encuentran regulados por el DIH**. El Documento de Posición del CICR sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional sostiene esta afirmación (Melzer, 2019). El fundamento es que cuando los Estados aprueban tratados de DIH dirigidos a limitar el empleo de determinadas armas, medios y métodos de guerra, lo hacen para regular conflictos presentes y futuros. En esta línea, el artículo 36 del Protocolo adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados (en adelante Protocolo adicional I) 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 puede llegar a estar prohibido por el derecho internacional aplicable. Asimismo, la Corte International de Justicia dijo en su opinión sobre la legalidad de la amenaza o el empleo de armas nucleares de 1996 que el empleo de armas nucleares durante conflictos armados está sujeto a los principios y normas de DIH. Afirmar que estos principios y normas no son aplicables a las armas nucleares porque fueron desarrolladas con posterioridad a la entrada en vigencia de los Convenios de Ginebra de 1949 y los Protocolos adicionales de 1977 sería incompatible con el carácter humanitario que impregna todo el DIH y se aplica a todas las formas de guerra y a todas las clases de armas, sean estas del pasado, del presente o del futuro (Corte Internacional de Justicia, 1996).

El principal **debate** se suscita en torno a la manera en la que el DIH debe aplicar al empleo de ciberoperaciones en conflictos armados. En el Documento de Posición del CICR, el Comité detalla cómo pueden interpretarse los principios y normas establecidos por el DIH. Por ejemplo, queda prohibido desarrollar capacidades cibernéticas que puedan ser desplegadas de forma tal de generar efectos indiscriminados y/o desproporcionados sobre la población civil. Sin embargo, no existe consenso suficiente de estadistas y de expertos alrededor de cómo deben hacerse operativos estos postulados de cara a las características del ciberespacio.

Para empezar, recordemos que para determinar la aplicabilidad de los principios y normas del DIH a una situación, debemos demostrar que esa situación tiene un **nexo con un conflicto armado**. Es inmensamente más difícil identificar al autor de un ataque cibernético que al autor de un ataque cinético. Por tanto, es también inmensamente más difícil demostrar que un ataque cibernético está vinculado al desarrollo de un conflicto armado, y por ende, que se encuentra sujeto al DIH.

Por otra parte, es cada vez más frecuente escuchar sobre ciberoperaciones que se emplean en conflictos armados con el propósito de alterar, modificar y dañar los sistemas informáticos de los cuales es dependiente nuestra **infraestructura civil,** tales como las redes eléctricas. El potencial costo humano producto de este tipo de ataques es alarmante. **Servicios esenciales** para el funcionamiento normal de una sociedad en tiempos de paz, como los servicios de atención médica y sanitaria, corren el riesgo de quedar interrumpidos, situación que en tiempos de guerra resultaría devastadora. Para algunos expertos, los sistemas informáticos de control industrial, es decir, aquellos sistemas que soportan el funcionamiento de infraestructura civil encargada de proveedor a la población de servicios esenciales, tales como servicios médicos y sanitarios o redes de suministro eléctrico gozan de una protección especial que prohíbe su ataque durante conflictos armados. Ahora bien, tanto para estos bienes de carácter especial como el resto de los bienes de carácter civil, hay que tener en cuenta que en el ciberespacio la mayoría de las redes de conexión militares están interconectadas con las redes civiles. Por un lado, las redes militares dependen de infraestructura cibernética civil, tales como cables de fibra óptica submarinos, satélites, enrutadores o nodos. Por otro lado, redes civiles dependen de infraestructura cibernética militar. Este sería el caso de los controles de tráfico aéreo que utilizan sistemas de navegación satelital militar para su funcionamiento (CICR, 2019b). Por ende, ¿cómo hacemos durante un conflicto armado para distinguir los “bienes de carácter civil” de los “objetivos militares” en el ciberespacio?

A su vez, tampoco queda claro qué requisitos debe cumplir una operación cibernética desplegada durante un conflicto armado para constituir un **“ataque”** bajo términos del DIH. El artículo 49 del Protocolo adicional I establece que “se entiende por ‘ataques’ los actos de violencia contra el adversario, sean ofensivos o defensivos” (Protocolo Adicional I a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados internacionales, 1977, art. 49). En base a esta disposición, existe un consenso generalizado en considerar como “ataque” a las operaciones cibernéticas capaces de causar muertes, heridas o daños físicos. No obstante, cuando se intenta ampliar el concepto de ataque en el ciberespacio, surgen las diferencias. Sobre todo, no existe consenso respecto a la inclusión de las ciberoperaciones que alteran servicios esenciales para la supervivencia de la población, pero que no ocasionan daños físicos.

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” (Schmitt, 2017, sección 2, regla núm. 30). Bajo esta definición, una ciberoperación que interrumpe una red de suministro eléctrico de un hospital y que indirectamente produce la muerte de los pacientes que dependían de ese suministro, constituye un ataque. Además, el CICR incluye dentro del concepto de “ataque” a las operaciones diseñadas con el fin de desactivar una computadora o una red informática por medios cinéticos o cibernéticos (CICR, 2019a).

En cambio, los expertos que fueron convocados para la elaboración del Manual de Tallin 2.0 acordaron calificar como “ataque” a las operaciones cibernéticas de carácter ofensivo o defensivo que se espera de forma razonable cause lesiones o la muerte a personas o daños o destrucción a objetos (Schmitt, 2017). Asimismo, los expertos estuvieron de acuerdo en considerar como “ataque” a las operaciones cibernéticas que producen la pérdida de funcionalidad de computadoras o redes informáticos. Sin embargo, un grupo de expertos sostuvo que el concepto de “pérdida de funcionalidad” implica la necesidad de reemplazar o reparar componentes físicos de la infraestructura cibernética atacada. Otro, afirmó que basta tener que reinstalar el sistema operativo o los datos personalizados de los que la infraestructura cibernética depende para que pueda volver a estar operativa para considerar que hubo una “pérdida de funcionalidad” y, por ende, un “ataque” (Schmitt, 2017).

Para terminar, cabe destacar la discusión acerca del **status de los datos digitales** durante los conflictos armados. Para el CICR, existen datos indispensables para la supervivencia de la población que hoy en día se encuentran digitalizados, tales como los datos médicos, que deben gozar de la misma protección gozada por la categoría de bienes civiles esenciales dentro del DIH (CICR, 2019a). No prohibir la eliminación o adulteración de datos de carácter civil esenciales para el funcionamiento normal de la sociedad e incluso para la supervivencia de la población, sería contrario a la finalidad del derecho. Por el contrario, la mayoría de los expertos del Manual de Tallin 2.0 concluyeron que estos datos no pueden ser incluidos en la definición del DIH de “bienes”, por lo que no cabe otorgarles el mismo tipo de protección de la que gozan los “bienes de carácter civil” bajo esta rama del derecho. Aun así, hubo una minoría de expertos que, en línea con lo sostenido por el CICR, afirmaron que no otorgarle protección a estos datos sería contrario al objetivo del DIH. Para este grupo, lo que convierte a un “bien” en un “bien de carácter civil” es la gravedad de las consecuencias de un ataque contra ellos, no la naturaleza del daño, es decir, no si el daño es cinético o cibernético (Schmitt, 2017).

Capítulo III: Evaluación de la aplicación del DIH a operaciones cibernéticas en contextos internacionales y no internacionales

3.1 Aplicabilidad del Derecho Internacional Humanitario a operaciones cibernéticas

El Derecho Internacional Humanitario no rige todas las operaciones cibernéticas diseñadas y ejecutadas por los actores del sistema internacional. Rige únicamente el uso de operaciones cibernéticas en conflictos armados ya que, como se mencionó anteriormente, la condición previa para la aplicación del DIH a una situación es la existencia de un "conflicto armado", término que se utiliza en la codificación de esta rama del Derecho Internacional en los Convenios de Ginebra de 1949, pero que nunca se ha definido estrictamente en un instrumento internacional. Sin embargo, existen argumentos jurídicos convincentes para considerar que las hostilidades en un conflicto armado pueden ser llevadas a cabo por diferentes medios y métodos de guerra, y que no existen razones jurídicas suficientes para excluir a las operaciones cibernéticas como tales.

En general, las ciberoperaciones se utilizan en los conflictos para espionaje; identificación de objetivos; operaciones de información y desinformación que afectan la moral y la voluntad de lucha del enemigo; interrupción, engaño y obstaculización de los sistemas de comunicación del adversario con el fin de dificultar la coordinación de sus fuerzas; inutilización de las estaciones de radar militares de la otra parte en apoyo de ataques aéreos; entre otras. A su vez, en la última década, se ha incrementado el uso de operaciones cibernéticas por fuera del contexto de los conflictos armados contra redes eléctricas, sistemas sanitarios, instalaciones nucleares y otras infraestructuras críticas (Gisel & Olejnik, 2018).

Los Estados han llegado a algunos acuerdos sobre determinados aspectos del régimen jurídico que rige las operaciones cibernéticas, pero la cuestión de la aplicación del DIH a las mismas durante los conflictos armados sigue siendo objeto de intensos debates. Estas discusiones comenzaron hace más de dos décadas cuando la Federación Rusa presenta en 1998 una primera resolución sobre el tema en la Asamblea General de las Naciones Unidas (en adelante AGNU)(Departamento de Defensa de los Estados Unidos, 1999). Desde entonces, el debate ha ido evolucionando, sobre todo a partir de 2004, año en el que se empiezan a reunir los Grupos de Expertos Gubernamentales (en adelante GEG) sobre cuestiones relacionadas con la información y las telecomunicaciones en el contexto de la seguridad internacional de la AGNU. De hecho, uno de los antecedentes históricos más importantes en el tema de estudio de este trabajo es la conclusión de 2013 del GEG de la ONU que afirma que el Derecho Internacional,

en general, y la Carta de las Naciones Unidas, en particular, son aplicables a las tecnologías de la información y de la comunicación[4].

Durante estos años, los debates también se intensificaron a nivel regional. Por ejemplo, en 2009 los Estados miembros de la Organización de Cooperación de Shanghái (en adelante OCS) calificaron la alta probabilidad de una guerra de información como una amenaza importante en el ámbito de la seguridad de la información internacional, a pesar de no pronunciarse, en ese momento, con respecto a la aplicabilidad del DIH a las operaciones cibernéticas[5]. Asimismo, han tenido lugar dentro de la Organización Consultiva Jurídica Asiático-Africana (en adelante AALCO) debates en relación con la aplicabilidad del Derecho Internacional sobre las tecnologías cibernéticas. En 2015, por ejemplo, la Organización estableció un Grupo de Trabajo de Composición Abierta sobre Derecho Internacional en el Ciberespacio en 2015[6] y procesos similares han ocurrido dentro del ámbito de la Commonwealth[7], la Unión Europea (en adelante UE)[8], la OTAN[9] y la Organización de Estados Americanos (en adelante OEA)[10]. A su vez, desde 2018 funciona dentro de las Naciones Unidas un Grupo de Trabajo de Composición Abierta que comparte con los GEG el mandato de estudiar cómo se aplica el Derecho Internacional al uso de las tecnologías de la información y las comunicaciones por parte de los Estados.

Por su parte, el CICR sostiene hace años que no hay duda de que las operaciones cibernéticas durante los conflictos armados se encuentran regidas por el Derecho Internacional Humanitario. Para el Comité, el carácter novedoso de las operaciones cibernéticas no impide la aplicación de esta rama del derecho ya que los tratados de DIH, la jurisprudencia de la CIJ y las opiniones expresadas por varios Estados y Organizaciones Internacionales dejan en claro que cualquier arma, medio o método de guerra nuevamente desarrollado que sea utilizado por una Parte beligerante en un conflicto se encuentra sujeto a sus disposiciones (CICR, 2019a). Esto es producto de que los Estados Parte en los tratados de Derecho Internacional Humanitario

---

[4] Asamblea General de las Naciones Unidas (22 de julio de 2015). *Grupo de Expertos Gubernamentales sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional: Nota del Secretario General,* Doc. A/70/174. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/38/PDF/N1522838.pdf?OpenElement.

[5] Organización de Cooperación de Shanghái (16 de junio de 2009). *Acuerdo de Cooperación para garantizar la seguridad internacional de la información entre los Estados miembros.* Ekaterimburgo, Rusia. Disponible en: https://cis-legislation.com/document.fwx?rgn=28340.

[6] Organización Consultiva Jurídica Asiático-Africana (2019). *International Law in Cyberspace,* Doc. No. AALCO/58/DAR ES SALAAM/2019/SD/17. Nueva Delhi, India. Disponible en: www.aalco.int/Final%20Cyberspace%202019.pdf.

[7] Commonwealth (abril de 2018). *Declaración Cibernética*. Reino Unido, Londres. Disponible en: https://thecommonwealth.org/commonwealth-cyber-declaration.

[8] Consejo de la Unión Europea (21 de junio de 2013). *Proyecto de Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro",* Doc. n.º 11357/13. Bruselas, Bélgica. Disponible en: https://data.consilium.europa.eu/doc/document/ST-11357-2013-INIT/es/pdf.

[9] North Atlantic Council (5 de septiembre de 2014*). Wales Summit Declaration issued by the Heads of State and Government.* Gales, Reino Unido. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[10] Organización de los Estados Americanos (5 de marzo de 2020). *Derecho International y operaciones ciibernéticas del Estado: Mejora de la transparencia, Cuarto Informe,* Doc. CJI/doc. 603/20 rev.1 corr.1. Río de Janeiro, Brasil. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI_doc_603-20_rev1_corr1.pdf.

incluyeran en ellos normas que preveían el desarrollo de nuevos medios y métodos de guerra bajo la presunción de que el DIH les sería aplicable. Esto tiene sentido si recordamos que el objeto y la finalidad de codificar esta rama del Derecho Internacional era regular futuros conflictos que hubieran de producirse para minimizar el sufrimiento causado por los conflictos armados respecto a experiencias de guerra anteriores.

Así, ya la Declaración de San Petersburgo de 1868 dispone lo siguiente:

> "Considerando:
>
> Que los progresos de la civilización deben tener por efecto atenuar en cuanto sea posible las calamidades de la guerra;
>
> Que la única finalidad legítima que los Estados deben proponerse durante la guerra es el debilitamiento de las fuerzas militares del enemigo;
>
> Que, a este fin, basta con poner fuera de combate al mayor número posible de hombres;
>
> Que esta finalidad quedaría sobrepasada por el empleo de armas que agravarían inútilmente los sufrimientos de los hombres puestos fuera de combate, o bien harían que su muerte fuese inevitable;
>
> Que el empleo de tales armas sería, a partir de este momento, contrario a las leyes de la humanidad;
>
> […] Las Partes contratantes o las que se hayan unido se reservan la facultad de ponerse de acuerdo ulteriormente cada vez que sea formulada una proposición precisa con vistas a los perfeccionamientos que puedan producirse, que la ciencia pudiera introducir en el armamento de las tropas, con el objeto de mantener los principios que han sido establecidos y conciliar las necesidades de la guerra con las leyes de la humanidad" (Declaración de San Petersburgo con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra, 1868).

Por su parte, el artículo 36 del Protocolo Adicional I a los Cuatro Convenios de Ginebra de 1977 establece 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" (Protocolo Adicional I a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977, art. 36).

Tanto la facultad de los Estados que firmaron la Declaración de San Petersburgo de 1868, y que consiste en evaluar la prohibición del empleo de nuevas armas que, en ciertas condiciones o en todas las circunstancias, agravaría inútilmente los sufrimientos de los hombres puestos fuera de combate, o bien que harían su muerte inevitable, así como la obligación de los Estados Parte en el Protocolo Adicional I de 1977 de determinar si el empleo de una nueva arma, o nuevos medios o métodos de guerra, debería prohibirse, se basan en el supuesto de que el DIH se aplica a esas nuevas armas, medios y métodos de guerra. De lo contrario, no sería necesario revisar su legalidad con arreglo a la legislación vigente.

La opinión que considera que el Derecho Internacional Humanitario regula el empleo de operaciones cibernéticas utilizadas como armas, medios o métodos de guerra, es compartida ampliamente entre los expertos y cada vez son más los Estados que adhieren a ella. Ejemplos de esto son los informes de 2013 y 2015 del Grupo de Expertos Gubernamentales de la ONU, cuya opinión ha sido acogida con satisfacción y confirmada por la AGNU. En igual sentido se han pronunciado la UE y la OTAN, así como los setenta y ocho Estados que apoyaron el Llamamiento de París para la confianza y la seguridad en el ciberespacio de 2020, reafirmando la aplicabilidad del DIH a las operaciones cibernéticas durante los conflictos armados. También son ejemplo los cincuenta y cuatro jefes de gobierno de la Commonwealth que se comprometieron a avanzar en los debates sobre cómo el Derecho Internacional Humanitario se aplica en el ciberespacio y los Estados miembros de la OEA que apoyaron el estudio realizado por el Comité Jurídico de la organización en apoyo a la aplicabilidad del DIH en el ciberespacio. Por último, son ejemplo los miembros del Grupo Internacional de Expertos convocados para la redacción del Manual de Tallin, proyecto impulsado en 2009 por el Centro de Excelencia de Defensa Cibernética Cooperativa de la Organización de la OTAN cuya finalidad fue la elaboración de un manual sobre Derecho Internacional aplicable a la guerra cibernética, quienes defendieron la aplicabilidad del DIH sobre las operaciones cibernéticas en conflictos armados internacionales y no internacionales.

A pesar de esta evolución en el debate, en la práctica, la aplicación del Derecho Internacional Humanitario a las operaciones cibernéticas resulta problemática por una serie de factores, tales como la dificultad de identificar la existencia de un ataque cibernético, su autor, su objeto de ataque premeditado y sus efectos precisos. Sin embargo, ni estas dificultades como tampoco los debates existentes acerca de cómo aplicar el derecho a las ciberoperaciones, impiden que éstas sean reguladas por esta rama del derecho. En la medida en que una norma del DIH no regule explícitamente las actividades cibernéticas y no se logre un consenso universal en torno a ello, debe tenerse en cuenta siempre la Cláusula Martens que se encuentra consagrada en la

Convención II de La Haya relativo a las leyes y costumbres de la guerra terrestre de 1907, los Convenios de Ginebra de 1949 y el Protocolo Adicional I a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales. Esta cláusula, que refleja el Derecho Internacional consuetudinario, establece que:

> "Mientras que se forma un Código más completo de las leyes de la guerra, las Altas Partes Contratantes juzgan oportuno declarar 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" (Convenio II de La Haya relativo a las leyes y costumbres de la guerra terrestre, 1907, preámbulo).

Por ende, en la medida en que las operaciones cibernéticas se lleven a cabo en el transcurso de un conflicto armado, la Cláusula Martens garantiza que dichas actividades no tengan lugar en un vacío legal.

Todo lo indicado anteriormente, permite concluir que no sólo existen argumentos jurídicos contundentes, sino también un consenso internacional cada vez mayor, sobre que el Derecho Internacional Humanitario puede y debe regir el uso de operaciones cibernéticas en conflictos armados.

3.2 "Conflicto armado": concepto y aplicación

Como se mencionó en la introducción y en la sección anterior, el Derecho Internacional Humanitario es una rama del Derecho Internacional cuyas disposiciones regulan los métodos y medios de guerra, así como la protección de las personas y los bienes que han caído en manos de una Parte beligerante durante un conflicto armado. Este derecho fue formulado específicamente para regir las situaciones de conflicto armado (Melzer, 2019). Por ende, cualquier acto realizado en ese contexto, independientemente de los motivos desencadenantes, y cualesquiera sean los medios o métodos de guerra empleados, queda sujeto a las normas del DIH.

Sin embargo, a pesar de las importancias consecuencias jurídicas y humanitarias de definir de forma precisa y completa la existencia de un conflicto armado, el Derecho Internacional convencional no ofrece tal definición. En cambio, los tratados dejan en claro lo que el DIH no rige: los enfrentamientos y las hostilidades entre Estados que no equivalen a un conflicto armado; las situaciones de tensiones internas o disturbios interiores, tales como los motines o los actos esporádicos y aislados de violencia al interior de un Estado; y otros actos análogos, que no constituyen conflictos armados (Protocolo Adicional II a los Convenios de Ginebra de 1949

relativo a la protección de las víctimas de los conflictos armados sin carácter internacional, 1977, art. 1(2)). Es por esto, que la interpretación del concepto de "conflicto armado" en Derecho Internacional depende de la práctica estatal (es decir, del derecho consuetudinario), la jurisprudencia internacional y la opinión de los juristas (CICR, 2008). No obstante, al momento de definir la existencia de un conflicto armado, la interpretación del concepto tiene en cuenta la distinción que hace el Derecho Internacional, en general, y el DIH, en particular, entre dos categorías de conflicto complementarias que abarcan todas las situaciones posibles que pueden dar lugar a la aplicación del DIH: a) los conflictos armados internacionales, y b) los conflictos armados no internacionales. Cabe destacar que tal distinción no excluye la posibilidad de que ambos tipos de conflicto armado coexistan ni la posibilidad de que un tipo de conflicto evolucione a otro.

A rasgos muy generales, los primeros son aquellos conflictos que tienen lugar entre dos o más Estados, mientras que los segundos se libran entre Estados y grupos armados no gubernamentales, o entre estos grupos únicamente. La distinción es producto de una evolución histórica y política. Los Estados, acostumbrados a basar sus relaciones en el reconocimiento mutuo de su soberanía nacional y personalidad jurídica internacional, regularon durante siglos dichas relaciones a través de tratados y costumbres internacionales. La incorporación del concepto de conflicto armado no internacional en el Artículo 3 común a los cuatro Convenios de Ginebra marcó un hito en el desarrollo y la codificación de DIH, dado que durante mucho tiempo los Estados se mostraron reacios a reconocer a grupos armados organizados no gubernamentales como "Partes" en un conflicto armado, efectivamente sometiendo sus esfuerzos por mantener la ley, el orden y la seguridad pública dentro de sus límites territoriales al ámbito del Derecho Internacional. De hecho, si bien con la codificación del concepto de conflicto armado no internacional, estos grupos quedan sujetos al cumplimiento del DIH correspondiente, los Estados subrayaron que la aplicación de las disposiciones del Artículo 3 común a los Convenios de Ginebra "no afectará al estatuto jurídico de las Partes en conflicto" (Convenio III de Ginebra relativo al trato debido a los prisioneros de guerra, 1949, art. 3). Así, los Estados dejaron en claro que el reconocimiento por parte del derecho convencional de los grupos armados organizados como Partes beligerantes no implica que estos sean legítimos o que gocen de plena personalidad jurídica según el Derecho Internacional. En consecuencia, el DIH convencional para los conflictos armados internacionales es mucho más amplio que para los no internacionales. Aún más importante, para calificar un enfrentamiento no internacional de conflicto armado, el DIH exige que la violencia perpetrada alcance un nivel de intensidad mucho mayor que la exigida para un conflicto de carácter internacional.

3.3 Alcance del Derecho Internacional Humanitario a operaciones cibernéticas de un conflicto armado internacional

El Derecho Internacional Humanitario convencional que rige los conflictos armados internacionales está codificado en el Reglamento de La Haya de 1907, los cuatro Convenios de Ginebra de 1949 y el Protocolo Adicional I. De estas fuentes surge que las dos características elementales para definir una situación como un conflicto armado internacional son el estatuto jurídico de las Partes beligerantes y la naturaleza del enfrentamiento.

En concreto, el Artículo 2 común a los Convenios de Ginebra establece que:

> "Aparte de las disposiciones que deben entrar en vigor ya en tiempo de paz, el presente Convenio se aplicará en caso de guerra declarada o de cualquier otro conflicto armado que surja entre dos o varias Altas Partes Contratantes, aunque una de ellas no haya reconocido el estado de guerra" (Convenio I de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, 1949, art. 2).

Por lo tanto, podríamos decir que los conflictos armados de carácter internacional son tales porque se libran entre las Altas Partes Contratantes de los Convenios de Ginebra de 1949, es decir, entre Estados. Sin embargo, para los Estados que hayan ratificado el Protocolo Adicional I, las situaciones mencionadas en el Artículo 2 común a los Convenios de Ginebra también incluyen:

> "(…) los conflictos armados en que los pueblos luchan contra la dominación colonial y la ocupación extranjera y contra los regímenes racistas, en el ejercicio del derecho de los pueblos a la libre determinación, consagrado en la Carta de las Naciones Unidas y en la Declaración sobre los principios de derecho internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas" (Protocolo Adicional I a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977, art. 1(4)).

Es decir, que los Estados Parte del Protocolo Adicional I acordaron reconocer también como Partes en un conflicto armado de índole internacional a determinados movimientos de liberación nacional, a pesar de no reconocerlos como Estados soberanos en virtud del Derecho Internacional. Por lo tanto, para estos Estados, los conflictos armados internacionales son aquellos que se libran entre dos o más Estados, o entre Estados y determinados movimientos de liberación nacional.

Ahora bien, en el contexto del ciberespacio, un Estado tiene responsabilidad jurídica internacional por una operación cibernética que le sea imputable y que constituya una violación de una obligación internacional. Sin embargo, el mero hecho de que una operación cibernética haya sido lanzada o se origine de otro modo a partir de una infraestructura cibernética gubernamental no es prueba suficiente para atribuir la operación a ese Estado, aunque es un

indicio de que el Estado en cuestión está asociado a la operación. Del mismo modo, el hecho de que una operación cibernética se haya dirigido a través de la infraestructura cibernética ubicada en un Estado no es prueba suficiente para atribuir la operación a dicho Estado. A su vez, dado que los Estados no suelen tomar responsabilidad oficial por las operaciones que ejecutan y, dada la facilidad con la que se puede ocultar la autoría real de las operaciones cibernéticas, se complica la clasificación de los conflictos armados. Sin embargo, existen algunas excepción como es el caso de la operación de septiembre de 2007, en el que una operación cibernética atacó el sistema de radar de defensa aérea sirio (Makovsky, 2012). Aunque en su momento ningún actor tomó responsabilidad por la operación, el 21 de marzo de 2018, el Ministro de Defensa israelí declaró oficialmente que la operación había sido llevada a cabo por las Fuerzas de Defensa israelíes (Ahronheim, 2018).

En ese caso, el objetivo de la operación cibernética era facilitar un ataque cinético sobre las instalaciones de Al-Kibar, cerca de la ciudad siria de Deir Alzour, donde se sospechaba que el gobierno sirio ocultaba un reactor nuclear secreto capaz de producir armas nucleares (BBC News, 2011). Supuestamente, la inteligencia israelí, también conocida como Mossad, había instalado en secreto un programa “troyano” en el ordenador portátil de un alto funcionario sirio. A partir de este programa, la inteligencia israelí extrajo información altamente sensible que incluía, entre otras cosas, fotos y planos de construcción de lo que más tarde se identificó como una instalación nuclear en Al-Kibar. En su momento, el presidente sirio negó que Siria tuviera interés alguno en desarrollo un programa nuclear militar y declaró que el edificio atacado era una instalación militar convencional más en desuso (Spiegel International, 2009). Sin embargo, a petición de los Estados Unidos, el Organismo Internacional de Energía Atómica (OIEA) inició una investigación sobre posibles actividades nucleares en Siria y encontró pruebas que indicaban la existencia de actividades nucleares en Al-Kibar, así como una alta probabilidad de la existencia de un reactor nuclear en las instalaciones (Follath & Stark, 2009).

Luego de haber conseguido esta información, las fuerzas de defensa aérea israelíes planificaron un operativo para inhabilitar el reactor. Primero, ejecutaron una operación cibernética contra los radares del sistema aéreo sirio situado cerca de la frontera turca en Tal Abyadm y, luego, atacaron la zona donde se encontraba el reactor con un misil guiado de precisión. La interrupción del sistema de radar sirio les permitió a las fuerzas de defensa israelíes intervenir en el espacio aéreo sirio sin ser detectadas. Así, los cazas israelíes lanzaron unas 17 toneladas de bombas sobre las instalaciones de Al-Kibar, destruyendo totalmente el lugar (Follath & Stark, 2009). La operación no tuvo como objetivo únicamente destruir lo que se sospechaba era una instalación nuclear siria, sino también impedir que Siria desarrollara armas nucleares y disuadir a otros países de la región, como Irán, de continuar sus propios programas nucleares.

Aunque al momento de los hechos gran parte de la atención internacional se centró en la posibilidad de que Siria estuviera desarrollando un programa nuclear, lo cierto es que la Operación Orchard, como se denominó a la operación de las fuerzas de defensa israelíes, es conocida como uno de los primeros eventos que marca un precedente en el uso de operaciones cibernéticas por parte de un Estado. Sobre todo, porque el éxito de la operación cinética se debió al éxito de la operación cibernética y porque fue el mismo Estado de Israel el que, tiempo después, reconoció su autoría.

Sin embargo, la realidad es que los Estados no solo suelen ser reacios a aceptar la responsabilidad de las operaciones cibernéticas que ejecutan, sino que, además, suelen actuar a través de actores no estatales que ofician de intermediarios que llevan a cabo operaciones cibernéticas en contra de otro Estado en su nombre. En estos casos, para definir la existencia de un conflicto armado, el actor no estatal debe actuar bajo un grado suficiente de control de parte del Estado pertinente. Para determinar si el Estado pertinente ejerce o no este tipo de control sobre el actor no estatal, se utiliza el criterio del "control general"[11]. Este criterio, que fue adoptado tanto por la CIJ como por la Corte Penal Internacional (en adelante CPI) a efectos de clasificar una situación de conflicto armado en sus sentencias, fue mencionado en la sentencia de la Sala de Apelación Tadic del Tribunal Penal Internacional para la ex Yugoslavia (en adelante TPIY) al concluir que las unidades serbias y bosnias se encontraban lo suficientemente dirigidas por la República de la ex Yugoslavia[12]. Este criterio exige que el Estado, además de prestar apoyo al actor no estatal, participe en la organización, coordinación o planificación de las operaciones. Así, la sentencia estableció que:

> "(…) Puede considerarse que existe el control exigido por el Derecho Internacional cuando un Estado (o, en el contexto de un conflicto armado, la Parte en conflicto) desempeña un papel en la organización, coordinación o planificación de las acciones militares del grupo militar, además de financiar, adiestrar y equipar o prestar apoyo operativo a dicho grupo" (Sentencia de apelación del Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Tadic, párr. 137).

Así, la Sala de Apelaciones del caso Tadic concluyó que la financiación, el entrenamiento, el equipamiento y la prestación de apoyo operativo por parte de un Estado a un actor no estatal para la ejecución de operaciones en contra de otro Estado, no son suficientes para concluir que dicho Estado ejerce un control general sobre el actor no estatal. Por ende, no puede atribuírsele responsabilidad por su conducta ni calificar la situación entre los dos Estados como un conflicto armado internacional (Sentencia de apelación del Tribunal Penal Internacional para la ex-

[11] Mačák, K. (2018*). Internationalized Armed Conflicts in International Law*, p. 39-47. Oxford University Press.

[12] Sentencia de apelación del Tribunal Penal Internacional para la ex-Yugoslavia (15 de julio de 1999). Fiscal v. Tadić, Caso No. IT-94-1-A.

Yugoslavia en el caso Fiscal v. Tadic, párr. 137). Por el contrario, si el Estado pertinente ejerce efectivamente un control general sobre el grupo, participando en la organización, coordinación o planificación de las operaciones, su conducta puede serle atribuida, lo que "internacionalizaría" el conflicto.

En la práctica, se puede decir que un Estado que le ordena a un grupo de hackers que penetre en la infraestructura cibernética de otro Estado causándole daños físicos significativos, ejerce un control general sobre la conducta de dicho grupo. Lo mismo se puede decir si el Estado proporciona inteligencia específica sobre las vulnerabilidades cibernéticas del Estado impactado o da instrucciones específicas al grupo de hackers sobre qué parte de la infraestructura atacar. En cambio, si el Estado pertinente se limita a proveerle al grupo de hackers acceso a la infraestructura cibernética del Estado afectado o las herramientas cibernéticas a utilizar, se puede concluir que el Estado presta apoyo al grupo, más no que ejerce un control general sobre su conducta. Por ende, las operaciones no le serían atribuibles.

Un aspecto importante a analizar en el contexto del ciberespacio es la imposibilidad de atribuirle a un Estado la responsabilidad por la conducta de individuos o grupos insuficientemente organizados en su nombre a partir del criterio del "control general". En estos casos, el Tribunal Penal Internacional para la ex Yugoslavia estableció que la conducta de tales individuos o grupos sólo le será atribuible al Estado pertinente cuando estos actúen bajo instrucciones específicas o la aprobación pública de dicho Estado (Sentencia de apelación del Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Tadic, párr. 132, 137, 141 y 145). Por ejemplo, entre abril y mayo de 2007, el sector público y privado de Estonia fue objeto de una serie de ataques DDoS (Denegación de Servicio Distribuida, por sus siglas en inglés) que sobrecargaron los servidores con peticiones masivas de datos y provocaron daños en los routers del país (Nazario, 2007). Los ataques impactaron los sitios web del Primer Ministro, el Parlamento y casi todos los Ministerios, así como los sitios web de algunos de los bancos y empresas de telecomunicaciones privadas y de noticias más importantes (Traynor, 2007). Además de las grandes pérdidas económicas, la mayoría de los sitios web se vieron obligados a cerrar y bloquear su acceso desde fuera de Estonia (Landler & Markoff, 2007). Como en ese momento existían tensiones políticas entre Estonia y Rusia por el traslado de un monumento de la época soviética de un soldado del Ejército Rojo en la capital de Estonia, Tallin, que celebraba la victoria de la Unión Soviética sobre el nazismo (Finn, 2007), sobraron las acusaciones sobre la participación de Rusia en los ataques. Sin embargo, la investigación del gobierno estonio no encontró pruebas suficientes como para determinar que los *hacktivistas* responsables hubieran actuado bajo las instrucciones específicas de ningún Estado (Wire Reports, 2007), por lo que la situación no pudo ser definida como parte de un conflicto armado internacional.

En lo que respecta a la naturaleza del enfrentamiento, el derecho sobre el empleo de la fuerza (también conocido como *jus ad bellum*) impone una prohibición general al uso de la fuerza entre Estados, por lo que cualquier uso de la fuerza de parte de un Estado contra otro, por breve o mínimo que sea, puede legítimamente llevar a presuponer la expresión de una intención beligerante y la consecuente creación de una situación de conflicto armado internacional (Pictet, 1958; Zimmermann, 1987; Fleck, 2013; Clapham, 2015; Zamir, 2017). El inc. 4 del artículo 2 de la Carta de las Naciones Unidas obliga a los Estados a "abstenerse en sus relaciones internacionales de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas" (Carta de la Organización de las Naciones Unidas, 1945). Esta prohibición es reflejo del Derecho Internacional consuetudinario y es considerada una norma imperativa del Derecho Internacional. Esta prohibición del uso de la fuerza está asociada a la fuerza armada y a operaciones cuya escala y efectos son comparables al uso de la fuerza armada (Schmitt, 2017).

Ahora bien, en su Resolución 3314 (XXIX) de 1974, la Asamblea General de las Naciones Unidas define a la agresión como:

> "(…) el uso de la fuerza armada por un Estado contra la soberanía, la integridad territorial o la independencia política de otro Estado, o en cualquier otra forma incompatible con la Carta de las Naciones Unidas, tal como se enuncia en la presente Definición" (Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas sobre la definición de la agresión, 1970, art. 1).

Por otro lado, la resolución enumera una serie de actos que, independientemente de que haya o no declaración de guerra, deben ser considerados como actos de agresión entre los Estados. En este punto, es interesante ver que aunque todos los actos enumerados mplican algún tipo de fuerza cinética, la resolución aclara de forma explícita que:

> La enumeración de los actos mencionados no es exhaustiva y el Consejo de Seguridad podrá determinar qué otros actos constituyen agresión, con arreglo a las disposiciones de la Carta (Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas sobre la definición de la agresión, 1970, art. 4).

Si tenemos en cuenta que la lista de actos enumerados por la resolución como actos de agresión no es exhaustiva, podemos concluir que la resolución contempló la posibilidad de que en el futuro se considerasen otros actos como actos de agresión y que no el derecho no prescribe ninguna forma específica para el recurso a la fuerza armada (Corte Internacional de Justicia, 1996, párr. 89). No existen limitaciones para considerar que las hostilidades en un conflicto armado internacional pueden implicar cualquier combinación de operaciones cinéticas y cibernéticas o,

incluso, implicar únicamente operaciones cibernéticas (Schmitt, 2017, comentario a la regla 82, párr. 11). Por ende, los conflictos armados internacionales son aquellos que se libran entre dos o más Estados, a través de cualquier medio o método de guerra, sean estos de naturaleza cinética o cibernética (Schmitt, 2017, regla 22).

En la actualidad se debate si las operaciones cibernéticas sin efectos físicos pueden equivaler a un uso prohibido de la fuerza. Se ha argumentado que este tipo de operaciones cibernéticas perturbadoras entran en el ámbito de aplicación del apartado 4 del artículo 2 si la perturbación resultante es "lo suficientemente importante como para afectar a la seguridad del Estado" (Roscini, 2014, p. 334). No cabe duda de que uno de los objetivos de la prohibición de la fuerza en virtud del Derecho internacional es salvaguardar la seguridad nacional de los Estados potencialmente afectados. Sin embargo, muchas formas de injerencia exterior, incluidas diversas formas de coacción política y económica, pueden afectar a la seguridad nacional del Estado víctima y, a pesar de ello, los redactores de la Carta de las Naciones Unidas rechazaron expresamente las propuestas de ampliar la prohibición de la fuerza más allá de los límites estrictos de la fuerza militar (o armada).

Dicho esto, no hay que perder de vista que la noción de "fuerza", al igual que otros términos genéricos de los tratados de duración ilimitada, debe presumirse que tiene un significado evolutivo. En 2023, la práctica de los Estados que apoyan la afirmación de que el significado de "fuerza" ha evolucionado para incluir operaciones cibernéticas no destructivas contra infraestructuras nacionales críticas es limitada y ningún Estado víctima de una operación de este tipo ha sugerido que la operación hubiera constituido un uso de la fuerza (Efrony & Shany, 2018). Sin embargo, los Estados han empezado a abordar esta cuestión. En particular, Francia (Ministerio de los Ejércitos de Francia, 2019) y los Países Bajos (Ministerio de Asuntos Exteriores de Holanda , 2019) admiten la posibilidad de que las operaciones cibernéticas, que no producen efectos físicos, puedan calificarse de uso de la fuerza si se cumplen determinados criterios. Estos criterios incluyen la gravedad y el alcance de las consecuencias de una determinada operación cibernética y su naturaleza militar, así como las circunstancias imperantes en el momento de la operación, el origen de la operación, la naturaleza del instigador (militar o no), el alcance de la intrusión, los efectos reales o previstos de la operación y la naturaleza del objetivo previsto. Varios de estos criterios se recogen también en el Manual de Tallin 2.0 (Schmitt, 2017, comentario a la regla 69, párr. 9).

Dado que entre Estados, la prohibición al uso de la fuerza es absoluta con las excepciones del uso de la fuerza autorizado por el Consejo de Seguridad en virtud del Capítulo VII de la Carta y del uso de la fuerza en legítima defensa en virtud del artículo 51 de la Carta, la intensidad de la violencia no es un factor determinante para calificar una controversia entre Estados como un

conflicto armado internacional. En lugar de evaluar la intensidad de la violencia, se recurre al concepto de “intención beligerante”.

Durante siglos, los Estados expresaron su intención beligerante ante otros Estados a partir de declaraciones formales de guerra. Estas declaraciones eran suficiente para crear un estado de guerra política y crear una situación de conflicto armado internacional que daba lugar, al mismo tiempo, a la aplicación del DIH. Así, incluso en ausencia de hostilidades abiertas, una declaración formal de guerra de un Estado contra otro implicaba el inicio de un conflicto armado internacional. Esto se debe a que su intención beligerante quedaba claramente expresada. Con el trascurso del tiempo y, en particular, a partir del Siglo XX, las declaraciones formales de guerra entre Estados al momento de llevar a cabo hostilidades se hicieron menos frecuentes. Por ello, en la actualidad, para definir una situación como conflicto armado internacional se tiene en cuenta la prohibición general al uso de la fuerza entre Estados establecida por el Derecho Internacional y se presume que existe un conflicto cuando un Estado recurre a la fuerza armada contra otro Estado, independientemente de los motivos que lo llevaron a recurrir a la fuerza, del nivel de intensidad del enfrentamiento y de si una o ambas Partes han reconocido formalmente un estado de guerra política.

Esta prohibición general al uso de la fuerza entre Estados se encuentra consagrada en los Principios de la Carta de las Naciones Unidas, específicamente en el artículo 2, inciso 4, y es considerada una norma del Derecho Internacional Consuetudinario. Este inciso establece que:

> “Los Miembros de la Organización, a fin de asegurarse los derechos y beneficios inherentes a su condición de tales, cumplirán de buena fe las obligaciones contraídas por ellos de conformidad con esta Carta” (Carta de la Organización de las Naciones Unidas, 1945, art. 2(2)).

A su vez, los trabajos preparatorios de la Carta parecen indicar que el artículo 2, inciso 4, tenía por objeto establecer la presunción de ilegalidad para cualquier amenaza o uso de la fuerza entre Estados, con las excepciones del uso de la fuerza autorizado por el Consejo de Seguridad en virtud del Capítulo VII de la Carta y del uso de la fuerza en legítima defensa en virtud del artículo 51 de la Carta. Recordemos que este inciso dispone que:

> “Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas” (Carta de la Organización de las Naciones Unidas, 1945, art. 2(4)).

En este mismo sentido, de acuerdo a la doctrina formulada en los Comentarios a los Convenios de Ginebra de 1949:

> "Cualquier diferencia que surja entre dos Estados y que conduzca a la intervención de las fuerzas armadas es un conflicto armado en el sentido del artículo 2, incluso si una de las Partes niega la existencia de un estado de guerra. No influye en nada la duración del conflicto ni la mortandad que tenga lugar" (Pictet, 1952, p. 32).

El Tribunal Penal Internacional para la ex Yugoslavia también adoptó en el caso de Tadic una definición general de conflicto armado internacional. En dicho caso, el Tribunal afirmó que existe un conflicto armado desde el momento en que se recurre a la fuerza armada entre Estados. Desde entonces, esta definición ha sido avalada por la doctrina (Schindler, 1979).

Lo dicho no implica que el DIH se aplique cuando no existe una intención beligerante. Por el contrario, la intención beligerante sigue siendo un requisito previo implícito para calificar una situación como conflicto armado internacional. Por ejemplo, el DIH no se aplica cuando un Estado es responsable por daños resultantes de actos lícitos e ilícitos con respecto de otro Estado debido a la acción u omisión de sus órganos y funcionarios. En todo caso, estos actos deberán acarrear las consecuencias jurídicas de la responsabilidad del Estado, pero no constituyen un conflicto armado ya que carecen de intención beligerante. Sin embargo, cuando existe tal intención, cualquier situación de violencia armada, por mínima que sea, puede ser suficiente para dar lugar a la aplicación del DIH que rige los conflictos armados internacionales, precisamente por la prohibición general al uso de la fuerza entre Estados que el Derecho Internacional dispone (CICR, 2008). A pesar de ello, conviene subrayar que hoy en día se siguen definiendo situaciones como conflictos armados internacionales cuando, incluso en ausencia de hostilidades abiertas, existe una declaración formal de guerra.

En consecuencia, una operación cibernética que constituya un uso o una amenaza al uso de la fuerza entre Estados da inicio a un conflicto armado. Sin embargo, como se ha mencionado anteriormente, la Carta de las Naciones Unidas no ofrece ningún criterio para determinar cuándo un acto equivale a un uso de la fuerza. Al respecto, la sentencia de la CIJ en el caso Nicaragua únicamente señala que al definir si un acto equivale a un "conflicto armado" se deben analizar su escala y efectos. A su vez, en la conferencia de redacción de la Carta celebrada en 1945 en San Francisco, los Estados rechazaron una propuesta para incluir la coerción económico dentro del concepto de "uso de la fuerza". Cuando la cuestión se volvió a plantear décadas más tarde durante el proceso de redacción de la Declaración sobre las Relaciones Amistosas de la Asamblea General, se rechazó una propuesta de incluir dentro del concepto a la coerción económica y política. Por lo tanto, las operaciones cibernéticas que tengan por efecto ejercer una coerción de carácter económico o político no pueden ser calificadas de "uso de la fuerza".

A pesar de la falta de normas explícitas al respecto, existe suficiente consenso entre expertos y juristas para sostener que las operaciones cibernéticas que provocan lesiones o la muerte a personas, o daños y destrucción a objetos equivalen inequívocamente a un uso de la fuerza. El problema es que, a excepción de los "ciberataques", que es precisamente como se denomina a las operaciones cibernéticas que pueden causar lesiones o muerte a personas, así como daños o destrucción a bienes (Schmitt, 2017), no está claro qué efectos tendrían que tener las operaciones cibernéticas para, por sí solas, sin estar acompañadas de un uso de la fuerza tradicional cinético, equivaler a un uso de la fuerza y, por ende, desencadenar el inicio de un conflicto armado y la aplicabilidad del DIH.

Aunque está generalmente aceptado que las operaciones cibernéticas que producen efectos similares a las operaciones cinéticas tradicionalmente empleadas durante conflictos armados clásicos equivalen a un uso de la fuerza desencadenante de un conflicto armado internacional (CICR, 2021), se está muy lejos de arribar a un consenso acerca de si las operaciones cibernéticas que perturban o interrumpen el funcionamiento de la infraestructura militar o civil de un Estado equivalen a un recurso de la fuerza en términos del DIH (CICR, 2021).

Un ejemplo que ilustra esta falta de consenso es el caso de Stuxnet de 2010 contra los sistemas SCADA en Irán, que provocó daños físicos a los centrifugadores de la planta de enriquecimiento de combustible de Natanz y la planta nuclear de Bushehr. Según la empresa de ciberseguridad Symantec que investigó el caso, el virus que infectó ambas centrales fue diseñado específicamente para atacar sistemas de control industrial y fue muy probablemente introducido por un tercero que lo hizo penetrar en la red de máquinas Windows de Natanz a través de una memoria USB (Hafezi, 2010; Falliere, Murchu & Chien, 2011; Shubert, 2011). Para afectar al sistema, el código malicioso explotó vulnerabilidades no parcheadas del sistema operativo de Microsoft (Murchu, 2010), que le permitió al software modificar las instrucciones enviadas por los controles a los centrifugadoras utilizados para enriquecer el uranio, con el fin de obligarlos a girar rápida o lentamente, dañándolas (Kelley, 2013). Al alterar la velocidad del rotor, Stuxnet provocó, entre finales de 2009 y principios de 2010, el fallo de varios centrifugadores, de las cuales mil tuvieron que ser sustituidos (Albright, Brannan & Walrond, 2010).

Este caso, considerado por muchos expertos como el primer ciberataque de la historia que causó efectos destructivos físicos, sentó un precedente importante para el DIH (Walsh, 2010). Sin embargo, no se pudo llegar a un acuerdo respecto a si los daños físicos causados alcanzaban el umbral de violencia necesario para calificar de "conflicto armado". La calificación del caso como un conflicto armado internacional se complicó aún más por el hecho de no haber podido atribuir la operación a un Estado o a un actor no estatal bajo el control general de un Estado (Hafezi, 2010). Es por ello que Stuxnet ejemplifica muchos de los desafíos de aplicar en la práctica el DIH a las operaciones cibernéticas. Es más, hasta la fecha, ningún conflicto entre dos o más Estados

llevado a cabo únicamente a través de operaciones cibernéticas ha sido calificado por la comunidad internacional en su conjunto como un conflicto armado internacional, a pesar del creciente consenso en torno a la posibilidad de que las operaciones cibernéticas por sí solas, en ausencia de operaciones cinéticas, pueden desencadenar el inicio un conflicto.

Por otra parte, el Artículo 2 común a los cuatro Convenios establece que:

> "El Convenio se aplicará también en todos los casos de ocupación total o parcial del territorio de una Alta Parte Contratante, aunque tal ocupación no encuentre resistencia militar (…)" (Convenio I de Ginebra para aliviar la suerte que corren los heridos y los enfermos de las fuerzas armadas en campaña, 1949, art. 2).

Una situación se define como ocupación extranjera beligerante cuando un Estado invade a otro y establece en él un control militar total o parcial del territorio. En concreto, el artículo 42 del Reglamento de La Haya determina que:

> "Se considera como ocupado un territorio cuando se encuentra colocado de hecho bajo la autoridad del ejército enemigo.
>
> La ocupación no se extiende sino a los territorios donde esa autoridad esté establecida y en condiciones de ejercerse" (Reglamento II de La Haya relativo a las leyes y costumbres de la guerra terrestre, 1907, art. 41(2) y 42(1).

Del artículo citado surge que la calificación de un territorio como ocupado en el sentido del DIH depende de si la potencia ocupante establece control efectivo sobre el territorio en cuestión. Que la potencia ocupante establezca control efectivo sobre el territorio en cuestión depende, a su vez, de que asuma *de facto* las funciones gubernamentales de una potencia ocupante. Entre estas funciones gubernamentales se incluye garantizar la seguridad pública, la ley y el orden. Por lo tanto, la definición de una situación como una ocupación beligerante es una cuestión de hecho. En otras palabras, en el caso particular de una ocupación, la intención beligerante no se infiere del reconocimiento formal de un Estado de un estado de guerra política, sino por de las circunstancias reales de lo que ocurre sobre el terreno. Cabe destacar, además, que no es necesario que la potencia ocupante ejerza el control efectivo directamente a través de sus fuerzas armadas. Al contrario, también se trata de una ocupación beligerante cuando el Estado extranjero ejerce pleno control sobre las autoridades locales y son estas quienes ejercen control gubernamental directo sobre el territorio en cuestión como agentes estatales *de facto* en nombre de la potencia ocupante (Ferraro, 2012).

Asimismo, para los Estados que ratificaron el Protocolo Adicional I, el DIH que rige los conflictos armados internacionales también se aplica a situaciones en las que el territorio ocupado no

pertenece a una Alta Parte Contratante, es decir, a un Estado, sino a pueblos que luchan contra la ocupación extranjera en ejercicio del derecho a la autodeterminación (Protocolo Adicional I a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales, 1977, art. 1(4)). En el caso especial de estos movimientos de liberación nacional que son reconocidos como Partes en un conflicto armado internacional, el umbral de violencia requerido va a depender de las circunstancias reales. Si estas circunstancias se asemejan más a la relación entre dos Estados soberanos, el umbral requerido será menor. En cambio, si las circunstancias se acercan más a la relación entre una autoridad gubernamental y un grupo armado no estatal, el umbral será mayor. Se definirá según cada caso en concreto.

En el contexto del ciberespacio, no existe un concepto jurídico de ocupación. Las operaciones cibernéticas por sí solas no son suficiente para establecer o mantener un control efectivo sobre un territorio. Sin embargo, pueden emplearse para ayudar a establecer o mantener el control ya adquirido por medios físicos o cinéticos por la potencia ocupante como, por ejemplo, con operaciones cibernéticas que le permitan difundir avisos dirigidos a la población civil que se encuentra en su poder.

Por otra parte, se mencionó que en su sentencia en el caso Nicaragua, la CIJ consideró que si un Estado arma y entrena a un grupo guerrillero involucrado en hostilidades en contra de otro Estado, el primero incurre en un “uso de la fuerza” (Corte Internacional de Justicia, 1986, párr. 228). Según este criterio, un Estado que provee a un grupo armado no estatal del software y del entrenamiento técnico necesario para dirigir ciberataques contra otro Estado se encuentraría haciendo uso de la fuerza.

No obstante, es necesario reconocer que la aplicación de los conceptos del DIH revisados hasta aquí es clara y precisa cuando las hostilidades se desarrollan exclusivamente a través de un uso de la fuerza se limita al empleo de operaciones cinética. En cambio, cuando se aplican a hostilidades llevada a cabo mediante operaciones cibernéticas, no existe consenso que permita una aplicabilidad unívoca e inequívoca del DIH. Actualmente se puede combatir sin necesidad de ocupar un territorio, por lo que hoy la presencia cada vez mayor de las ciberoperaciones en los conflictos contemporáneos obligan a repensar y redefinir muchos de los conceptos, incluidos los conceptos de “conflicto armado”, “uso de la fuerza”, y “ocupación del territorio”, entre otros.

3.4 Alcance del Derecho Internacional Humanitario sobre operaciones cibernéticas de un conflicto armado no internacional

La mayoría de los conflictos armados contemporáneos son de carácter no internacional. Según la Sala de Apelaciones del Tribunal Penal Internacional para la ex Yugoslavia, los conflictos armados no internacionales son situaciones de violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre dichos grupos dentro de un Estado

(Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Tadic). Para calificar a una situación de conflicto armado internacional son dos los elementos básicos: la intensidad de la violencia y el nivel de organización del grupo no estatal (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Tadic).

En relación con la intensidad de violencia que debe ser alcanzado, cabe recordar que, como se mencionó anteriormente, en las relaciones entre Estados la prohibición general del uso de la fuerza en la Carta de las Naciones Unidas implica que cualquier uso de la fuerza, independientemente de su intensidad y duración, puede ser evaluado como la expresión de una intención beligerante y, por tanto, crear una situación de conflicto armado internacional. En cambio, dentro de su territorio, los Estados deben poder hacer uso de la fuerza contra grupos o individuos con el propósito de hacer cumplir la ley y mantener el orden. En consecuencia, el uso de la fuerza por parte de grupos e individuos al interior de un Estado se rige por el Derecho Penal interno. Debido a esto, para que una situación entre un Estado y un grupo armado no estatal, o entre dichos grupos, equivalga a un conflicto armado, es necesario que la intensidad de las hostilidades alcance un umbral de violencia elevado.

El Tribunal Penal Internacional para la ex Yugoslavia señaló en su sentencia del caso Tadic, que para determinar la existencia de una situación de “violencia armada prolongada” entre un Estado y grupos armados organizados, o entre dichos grupos, se debe evaluar: “el número de enfrentamientos y la duración e intensidad de cada uno de ellos, el tipo de armas y de otro equipamiento militar utilizado, el número y el calibre de las municiones utilizadas, el número de personas y los tipos de fuerzas que participan en los enfrentamientos, el número de bajas, la extensión de la destrucción material y el número de civiles que huyen de las zonas de combate (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Haradinaj). Un elemento indicativo adicional que podría indicar la existencia de una situación de violencia prolongada es la eventual intervención del Consejo de Seguridad de las Naciones Unidas.

Estos mismos criterios de intensidad de la violencia y nivel de organización de los grupos armados aplican en situaciones de conflictos armados internacionales llevados a cabo a través de operaciones cibernéticas. Es decir, existe un conflicto armado no internacional cuando existe violencia armada prolongada entre fuerzas armadas gubernamentales y grupos armados organizados, o entre dichos grupos al interior de un Estado, sea esta violencia el resultado de una combinación de operaciones cinéticas y cibernéticas o bien, el resultado exclusivo de operaciones cibernéticas (Schmitt, 2017).

Para precisar el umbral de violencia necesario para que una situación de carácter no internacional equivalga a un conflicto armado, el TPIY tuvo en cuenta en sus sentencias factores como la gravedad de los ataques y su recurrencia (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Mrkšić); la expansión temporal y territorial de la violencia y el

carácter colectivo de las hostilidades (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Hadžihasanović); si los grupos no estatales involucrados ejercen control sobre parte del territorio (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Milošević); el aumento del número de fuerzas gubernamentales desplegadas (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Limaj); la distribución y el tipo de armas utilizadas (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Mrkšić); entre otros. Sin embargo, debido al elevado umbral de violencia que debe ser alcanzado para que una situación de carácter no internacional sea calificada de conflicto armado, en ausencia de operaciones cinéticas, las operaciones cibernéticas rara vez desencadenan una violencia lo suficientemente intensa como para desencadenar por sí solas el inicio de un conflicto armado no internacional (Schmitt, 2017).

Resulta evidente que el DIH se aplica a las operaciones cibernéticas que ocurren en el contexto de un conflicto armado no internacional por operaciones cinéticas lo suficientemente intensas como para desencadenar dicho conflicto. También queda claro que no pueden calificarse de conflicto armado internacional las situaciones de disturbios y tensiones internos, tales como motines, actos de violencia aislados y esporádicos y otros actos análogos. Esto implica que los incidentes cibernéticos esporádicos, aunque causen directamente daños físicos o lesiones, no constituyen conflictos armados no internacionales. Tampoco las operaciones cibernéticas que incitan a incidentes, tales como disturbios civiles o actos de terrorismo, fenómeno que sucedió en Estonia en 2007 cuando aparecieron llamamientos en Internet para que la minoría nacionalista rusa que residía en el país se amotinara en las calles. No obstante, no existe consenso respecto al umbral de violencia que deben superar las operaciones cibernéticas para, por sí solas, desencadenar un conflicto armado de carácter no internacional.

En cuanto al nivel de organización, el Derecho Internacional Humanitario entiende que, sin un mínimo nivel de organización, no es posible llevar a cabo operaciones militares coordinadas ni lograr el cumplimiento general del derecho necesarios para calificar a un sujeto como Parte beligerante en un conflicto armado. Por ello, el Derecho Internacional exige a los grupos armados organizados que participan en conflictos armados un nivel de organización mínima. Este nivel de organización mínimo, que se presume en el caso de las fuerzas armadas estatales, debe ser evaluado en el caso de los grupos armados no estatales. En la práctica, dicha evaluación se lleva a cabo considerando los siguientes elementos:

> "(…) la existencia de una estructura de mando y de normas y mecanismos disciplinarios dentro del grupo; la existencia de un cuartel general; el control territorial del grupo; la capacidad para aprovisionarse de armamento, de otro equipamiento, de reclutas y de entrenamiento militar; la capacidad para planificar, coordinar y ejecutar operaciones militares, incluidos movimientos de tropas y logística; la capacidad para definir una

> estrategia militar unificada y ejecutar tácticas militares; la existencia de un vocero oficial y la capacidad del grupo para negociar y celebrar acuerdos de paz o de cese al fuego" (Tribunal Penal Internacional para la ex-Yugoslavia en el caso Fiscal v. Haradinaj, Sala de Primera Instancia, párr. 60).

Así, el Tribunal Penal Internacional para la ex Yugoslavia consideró en el caso Limaj, entre otras cosas, la organización y la estructura del Ejército de Liberación de Kosovo, que contaba con un Estado Mayor y un comandante por cada zona; reglamentos internos; nombramiento de portavoces; emisión de órdenes, declaraciones políticas y comunicados; cuarteles generales; capacidad para lanzar acciones coordinadas entre las unidades; policía militar; capacidad para recular nuevos miembros e impartir formación militar; canales de distribución de armas; uniformes y equipamiento; etc.

Esto plantea el debate en torno a la organización de carácter virtual ya que en el espectro de las operaciones cibernéticas encontramos desde *hackers* que operan de forma totalmente autónoma a grupos en línea que operan de forma cooperativa con una estructura de liderazgo precisa que coordina su actividad asignando objetivos cibernéticos específicos a cada individuo, compartiendo herramientas de ataque y evaluando vulnerabilidades cibernéticas en conjunto. Un criterio comúnmente citado es el de que la naturaleza de la organización debe ser tal que permita la aplicación del Derecho Internacional Humanitario. Sin embargo, el requisito es difícil de cumplir en el caso de un grupo armado virtual ya que no existen medios para hacer cumplir el derecho con respecto a individuos con los que no hay contacto físico o que permanecen anónimos.

En la práctica, uno de los escenarios más difíciles para determinar el nivel de organización de un grupo es el de una agrupación informal de individuos que no opera de forma cooperativa, sino de "colectiva", es decir, en simultáneo, pero sin coordinación alguna. Es el caso de un grupo informal de individuos que accede a un sitio web común con un propósito compartido sin coordinar previamente los ciberataques que ejecutaran de forma individual. La mayoría de los expertos del Grupo convocado por el Manual de Tallin consideró que este tipo de agrupación no constituye un grupo armado organizado ya que para ello es necesario que exista un grupo diferenciado con una estructura organizativa suficiente que opere como una unidad. Otro factor a considerar fue la existencia de una entidad de liderazgo informal que dirija las actividades del grupo en general. Todos los Expertos coincidieron en que el simple hecho de que los individuos actúen en pos de un objetivo colectivo no satisface el criterio de organización necesario. Por ejemplo, si un sitio web ofrece programas maliciosos y una lista de objetivos cibernéticos potenciales para sus usuarios, quienes utilicen el sitio de forma independiente para llevar a cabo ataques no constituirían un grupo armado organizado.

En sentencias posteriores, el TPIY restó a importancia al factor geográfico y temporal en lo que respecta a la existencia de un conflicto armado no internacional. A pesar de ello, en relación con

el ámbito geográfico, el Artículo 3 común dispone que un conflicto armado no internacional es aquel que se produce “en el territorio de una de las Altas Partes Contratantes”. Esta parte del texto ha generado debate sobre el alcance geográfico de los conflictos armados de carácter no internacional. Parte de la doctrina sostiene que la redacción del texto implica que los conflictos armados no internacionales se limitan a los que tienen lugar dentro de los límites territorios de un solo Estado, por lo que los conflictos armados que atraviesan una frontera serían considerados conflictos armados internacionales, a pesar de no involucrar a dos o más Estados como Partes beligerantes adversarias. Por el contrario, para otra parte de la doctrina, el texto simplemente busca dejar en claro que el Convenio es aplicable a los conflictos armados no internacionales que tienen lugar en el territorio de alguno de los Estados Parte en los Convenios de Ginebra de 1949, sin hacer referencia al traspaso de fronteras. Para el grupo de juristas y expertos que adoptan este segundo punto de vista, el hecho de que un grupo armado ejecute operaciones cibernéticas contra un Estado desde fuera de su territorio no “internacionaliza” el conflicto.

Lo cierto es que el Derecho Internacional Humanitario rige todas las actividades realizadas en el marco de un conflicto armado y sobre todos sus efectos asociados, incluidos daños colaterales, independientemente de que se produzcan o no en el territorio de un Estado involucrado en el conflicto armado no internacional. Esto es de particular importancia porque las actividades cibernéticas en apoyo de un conflicto armado llevado a cabo mediante operaciones cinéticas suelen llevarse a cabo a la distancia, lejos del lugar de las hostilidades tradicionales, particularmente, desde Estados con regímenes normativos más débiles que son técnicamente incapaces de vigilar y controlar las actividades cibernéticas que tienen lugar en su territorio.

En cuanto a la duración temporal, la sentencia de las Sala de Apelaciones Tadic, dispuso que la violencia que califica un conflicto armado como no internacional debe ser prolongada. Sin embargo, no cuantificó el término “prolongada”. Aun así, para el Grupo de Expertos convocado por el Manual de Tallin, queda claro que para que la violencia sea “prolongada” no es necesario que esta sea “continua”. De esta forma, el lanzamiento de ataques cibernéticos frecuentes, aunque no continuos, dentro de un período relativamente definido de tiempo, podrían caracterizarse como prolongados.

Por otra parte, los conflictos armados no internacionales entre un Estado y grupos armados organizados pueden verse afectados por la intervención extranjera de un tercer Estado. El concepto de “conflicto armado internacionalizado” hace referencia, precisamente, a una situación en la que la participación de un Estado en un conflicto armado no internacional lo convierte en uno internacional. Con respecto al derecho aplicable, deben distinguirse dos situaciones.

Cuando en el transcurso de un conflicto armado no internacional entre un Estado y grupos armados organizados no estatales, un Estado interviene para apoyar al Estado territorial, las

relaciones entre los grupos armados y el Estado interviniente se rige por el DIH aplicable a los conflictos armados no internacionales, es decir, por el mismo derecho que rige las relaciones entre el Estado territorial y los grupos insurgente. En cambio, cuando un Estado interviene para apoyar a un grupo insurgente contra el Estado territorial, la situación se vuelve más compleja. Los enfrentamientos entre el Estado que interviene y el Estado territorial dan lugar a la aplicación del DIH que rige los conflictos armados internacionales, mientras que los enfrentamientos entre el Estado territorial y el grupo insurgente no pierden su carácter no internacional y siguen rigiéndose por el derecho aplicable a los conflictos armados no internacionales. Estas circunstancias dan lugar a la coexistencia de un conflicto armado internacional y un conflicto armado no internacional, fenómeno al que a veces se hace referencia como de "doble clasificación". Por último, cuando un Estado interviene para apoyar, dirigir y controlar a un grupo insurgente de forma tal que las operaciones del grupo se consideren operaciones del Estado interviniente contra el Estado territorial, la situación se convierte en un conflicto armado internacional entre el Estado territorial y el Estado interviniente. La revisión de estos escenarios resulta útil a efectos de reflexionar acerca de cómo las operaciones cibernéticas pueden permitirle a los Estados intervenir en conflictos armados sin "internacionalizar" a los mismos si, por ejemplo, logran que un actor no estatal ejecute las operaciones cibernéticas deseadas por él sin que sea posible atribuírselas, ya sea porque no se deja evidencia suficiente o porque no se ejerce un "control general" sobre dicho actor.

Ahora bien, el derecho convencional que rige los conflictos armados no internacionales se encuentra codificado en el Artículo 3 común a los cuatro Convenios de Ginebra y en el Protocolo Adicional II. En particular, el Artículo 3 común identifica una serie de obligaciones y prohibiciones que todas las Partes en un conflicto armado no internacional que se produzca en el territorio de una de las Altas Partes Contratantes deben respetar ya que proporcionan un mínimo de protección necesario a las personas que no participan o que han dejado de participar activamente en las hostilidades.

Mientras que el artículo 3 común a los cuatro Convenios de Ginebra de 1949, que establece una seria de disposiciones que, en caso de conflicto armado que no sea de índole internacional y que surja en el territorio de una de las Altas Partes Contratantes, cada una de las Partes en conflicto tiene la obligación de aplicar, el Protocolo Adicional II lo desarrolla y complementa. Sin modificar sus condiciones de aplicación, el Protocolo Adicional II no se aplica a los conflictos armados no internacionales que se producen entre grupos armados organizados al interior de un Estado, sino que sólo se aplica a los conflictos armados internacionales que se desarrollan en el territorio de uno de los Estados Parte entre sus fuerzas armadas y fuerzas armadas disidentes o grupos armados organizados que ejercen control sobre el territorio del Estado en cuestión.

Para que el Protocolo Adicional II se aplique, parte del territorio del Estado contratante implicado en el conflicto debe estar bajo el control efectivo de las fuerzas del adversario. El control efectivo se evalúa según las fuerzas contrarias desempeñen o no las mismas funciones que una autoridad *de facto* e implica contraer obligaciones directas no sólo hacia la Parte contraria, sino también hacia los habitantes del territorio bajo su control. En el contexto del ciberespacio, aunque el control de las actividades cibernéticas puede ser indicativo del grado de control territorial del que goza un actor no estatal, este control resulta por sí solo insuficiente para determinar que dicho actor ejerce control del territorio a efectos del Protocolo Adicional II. Es decir, que el control de fuerzas armadas disidentes o grupos armados organizados sobre las actividades cibernéticas del Estado en cuestión no es suficiente para determinar que esas fuerzas o grupos ejercen un control efectivo sobre el territorio.

Capítulo IV: Conclusiones y palabras finales

El uso de operaciones cibernéticas en los conflictos armados es una realidad desde hace varios años y, con el tiempo, su empleo sólo se vuelva más prevalente. Si bien es cierto que el desarrollo de un campo de batalla digital podría brindar oportunidades hasta ahora inconcebibles de llevar adelante operaciones militares menos letales y destructivas, las ciberoperaciones también suponen un riesgo real para la población y objetos civiles afectados por conflictos armados.

La rápida evolución de las ciberamenazas globales tiene distintas implicancias para los diferentes ámbitos jurídicos. Así como la capacidad de digitalizar, almacenar, analizar y transportar datos por todo el mundo tiene profundos efectos en todos los sectores de la sociedad y modifica la forma de llevar a cabo los asuntos personales, empresariales y políticos de las personas, emergen nuevos medios y métodos que le permiten a actores estatales y no estatales poner en peligro la paz y la seguridad internacionales. En los últimos años, hemos sido testigos de operaciones cibernéticas, durante y por fuera de conflictos armados, capaces de perturbar el funcionamiento de infraestructuras civiles críticas y obstaculizar la prestación de servicios esenciales para la población.

En consecuencia, se plantean cuestiones jurídicas intrincadas. Una de ellas se plantea con respecto a la proliferación acelerada de herramientas cibernéticas ofensivas. Surge el debate acerca de la posibilidad de contar con algún tipo de mecanismo regulador para controlar la difusión y el uso por parte de los Estados y los actores no estatales de algunos tipos de malware. Por ejemplo, el malware autopropagable que ataca objetivos civiles y militares por igual y que es, por defecto, indiscriminado. Hoy en día, incluso es técnicamente factible escribir malware que, aunque se autopropague de sistema en sistema, sólo ejecute su tarea una vez que haya entrado en un objetivo previamente definido. Este es el caso del malware Stuxnet que se diseñó de una manera tan precisa y discriminatoria que, aunque llegó a infectar miles de sistemas informáticos en varios países, sólo causó daños en las instalaciones iraníes de enriquecimiento de uranio, como se pretendía.

Por otro lado, se plantean preguntas sobre el papel de los actores no militares en el futuro. Considerando que la infraestructura básica de la red está en su mayor parte en manos de entidades privadas, dichas empresas podrían estar en condiciones, o incluso en la obligación, de reprimir las conductas maliciosas durante conflictos armados que no respetan las disposiciones del DIH. También podría existir una obligación para las Partes beligerantes en los conflictos armados de evitar daños a dicha infraestructura a la luz de las posibles ramificaciones negativas para las redes globales de las que depende la sociedad moderna a nivel global. Además, hay que considerar la tendencia a la creciente implicación de las agencias de inteligencia civiles en las operaciones cibernéticas militares y repensar cuándo su conducta puede considerarse una participación directa en las hostilidades.

Estas y muchas otras cuestiones, vuelven imperativo profundizar en cómo y cuándo se aplica el DIH al uso de las operaciones cibernéticas en los conflictos armados. Resulta urgente el debate entre los Estados para aportar más claridad sobre si las interpretaciones jurídicas comunes proporcionan suficiente protección a los seres humanos y a las sociedades frente a las operaciones cibernéticas ya que, como están las cosas, mientras algunos expertos opinan que las normas vigentes son adecuadas y suficientes, otros consideran que se requiere un mayor desarrollo y codificación.

Está claro que la diferencia de opiniones se debe a los desafíos que existen en la práctica para adaptar las disposiciones del DIH a las características propias del ciberespacio como, por ejemplo, la mayor complejidad de demostrar la existencia de un nexo entre una operación cibernética y el desarrollo de un conflicto armado que entre una operación cinética y este; la dificultad de identificar su autor, su objeto de ataque premeditado y sus efectos precisos; y la necesidad de repensar algunos conceptos centrales como “conflicto armado”, “uso de la fuerza” y “ocupación del territorio”, pensados en un siglo pasado, a una realidad en la que gran parte de los servicios esenciales y la infraestructura civil, como instalaciones nucleares, redes de suministro eléctrico, sistemas de abastecimiento de agua, sistemas sanitarios y hospitales, industrias, telecomunicaciones, transporte, sistemas gubernamentales y financieros, datos médicos, biométricos, de registros impositivos, de cuentas bancarias y de registros de elecciones, se encuentra digitalizada y conectada. Sin embargo, tras más de dos décadas de discusión, pocas cuestiones pueden considerarse resueltas.

A pesar de ello, el ciberespacio no es un vacío legal. Dado el propósito y la finalidad del DIH de regular para proteger, no cabe duda de que las operaciones cibernéticas están sujetas a las normas y principios arraigados del derecho. Asimismo, dentro de los círculos de expertos del Derecho Internacional y las Relaciones Internacionales, existe suficiente consenso para afirmar que el DIH rige las operaciones cibernéticas que presentan un nexo con un conflicto armado. Aunque el término no ha sido definido en un instrumento internacional, existen argumentos jurídicos convincentes y un apoyo internacional cada vez mayor, para considerar que las hostilidades en un conflicto armado pueden ser llevadas a cabo por diferentes medios y métodos de guerra, y que no existen razones suficientes para excluir a las operaciones cibernéticas como tales. El carácter novedoso de las operaciones cibernéticas no impide su aplicación porque tanto el derecho convencional como la jurisprudencia internacional y la práctica estatal dejan en claro que cualquier acto realizado en el contexto de un conflicto armado, por motivos relacionados con el mismo, cualesquiera sean las armas, los medios o los métodos de guerra empleados, queda sujeto a las normas del DIH, independientemente del desarrollo de nuevas armas, medios y métodos de guerra.

A su vez, habiendo considerando en este trabajo lo dispuesto en la Declaración de San Petersburgo de 1868; la Cláusula Martens consagrada en la Convención IV de La Haya, los

Convenios de Ginebra de 1949 y el Protocolo adicional I; los artículos 2 y 3 comunes a los Cuatro Convenios de Ginebra de 1949; el inciso 4 del artículo 2 de la Carta de las Naciones Unidas de 1945; la Resolución 2625 (XXV) de 1970 y la Resolución 3314 (XXIX) de 1974 de la Asamblea General de las Naciones Unidas; los artículos 36 y 49 del Protocolo adicional I de 1977; la opinión consultiva emitida por la Corte Internacional de Justicia sobre la legalidad de la amenaza o del empleo de armas nucleares de 1997; y los Comentarios a los Convenios de Ginebra de 1949; entre otros documentos, podemos concluir que el empleo de ciberoperaciones por actores estatales y no estatales, acompañen estas o no operaciones cinéticas, puede dar inicio a un conflicto armado internacional o no internacional. La probabilidad de que esto suceda depende de la naturaleza de las Partes que participan en las hostilidades y de la intensidad de la violencia del conflicto.

Por tanto, el DIH puede y debe regir el uso de operaciones cibernéticas en los conflictos armados. Ahora bien, en lo concreto, queda claro que operaciones cibernéticas utilizadas para generar y/o fomentar disturbios interiores y tensiones internas o actos de violencia esporádicos y aislados, así como aquellas que tengan por efecto ejercer una coerción de carácter económico o político no pueden ser calificadas de “uso de la fuerza”. Por el contrario, existe un consenso generalizado en torno a que las operaciones cibernéticas calificadas de “ataques”, que causan lesiones o muerte a personas o daños o destrucción a bienes, equivalen inequívocamente a un “uso de la fuerza” ya que producen efectos similares a las operaciones cinéticas tradicionalmente empleadas durante conflictos armados clásicos.

En cambio, se está muy lejos de arribar a un consenso acerca de resto de las operaciones cibernéticas que tienen otros efectos como es el caso de operaciones cibernéticas que ocasionan perjuicio por medio de sus efectos indirectos causando muertes, heridas o daños físicos a personas o objetos (por ejemplo, una ciberoperación que interrumpe una red de suministro eléctrico de un hospital, provocando indirectamente la muerte de pacientes dependientes de tal suministro. Tampoco existe acuerdo sobre las operaciones cibernéticas que producen la pérdida de funcionalidad de una computadora, una red, un sistema informático u otro dispositivo conectado a través de un flujo de datos. De hecho, los expertos tampoco se ponen de acuerdo acerca del significado de “pérdida de funcionalidad”. Para algunos, el objeto afectado pierde funcionalidad cuando es necesario que para recuperar su operatividad se reemplacen o reparen componentes físicos de la infraestructura cibernética afectada. Para otros, es suficiente que sea necesario reinstalar el sistema operativo o los datos personalizados de la infraestructura cibernética afectada. Del mismo modo, no existe consenso respecto de las operaciones cibernéticas que alteran servicios esenciales para la supervivencia de la población sin ocasionar daños físicos. Este sería el caso de una ciberoperación que interrumpe el funcionamiento de la principal planta de tratamiento de agua potable de una población por algunos días. Igualmente, no hay acuerdo sobre las operaciones cibernéticas que perturban o interrumpen el

funcionamiento de la infraestructura militar o civil de un Estado como sucede cuando una ciberoperación provoca un incendio en una instalación militar o una ciberoperación que bloquea el acceso al servicio de Internet de la población civil por algunas semanas.

Teniendo en cuenta la falta de consenso y la continuidad de los debates, es necesario que, hasta tanto exista un tratado vinculante sobre Derecho Internacional en el ciberespacio o bien una revisión actualizada de los tratados vigentes, la comunidad internacional y los expertos realicen para cada caso de empleo de ciberoperaciones un análisis casuístico de los derechos y obligaciones establecidos por el DIH.

Si bien no debe subestimarse la flexibilidad del derecho para adaptarse a la evolución de las sociedades, resulta evidente la inadecuación del DIH frente a las nuevas tecnologías y la falta de voluntad de los Estados de someter sus operaciones cibernéticas a las disposiciones del Derecho Internacional a través de un nuevo tratado o un nuevo protocolo adicional. Es fundamental que la comunidad internacional afirme la aplicabilidad del DIH al uso de operaciones cibernéticas durante los conflictos armados.

Tal y como señala el CICR (CICR, 2019a), el presente reclama debates entre expertos gubernamentales y de otros ámbitos sobre cómo se aplican las normas existentes del DIH y si el derecho vigente es adecuado y suficiente. En paralelo, la interpretación que hagan los Estados de las normas vigentes del DIH determinará en qué medida el DIH protege contra los efectos de las operaciones cibernéticas. Por consiguiente, los Estados deben adoptar posiciones claras sobre su compromiso de interpretar el DIH de modo que preserve las infraestructuras civiles de perturbaciones significativas y proteja los datos civiles. La disponibilidad de tales posiciones también influirá en la evaluación de si las normas existentes son adecuadas o si pueden ser necesarias nuevas normas. Si los Estados consideran necesario elaborar nuevas normas, la comunidad internacional deberá basarse en el marco jurídico existente, incluido el DIH, y reforzarlo.

Bibliografía

- Additional Protocol I: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S.
- Additional Protocol II: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts, June 8, 1977, 1125 U.N.T.S.
- Additional Protocol III: Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem, Dec. 8, 2005, 2404 U.N.T.S.
- Amended Mines Protocol: Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on May 3, 1996, 2048 U.N.T.S.
- Banks, W. (2017). *State Responsibility and Attribution of Cyber Intrusions After Tallin 2.0*. Texas Law Review, 95, 487-1513.
- Biller, J y Schmitt, M. N. (2019). *Classification of Cyber Capabilities and Operations as Weapons, Means, or Methods of Warfare.* International Law Center, 95, 179-225. ISSN 2375-2831.
- Blake, D. y Imburgia, J. S. (2010). *"Bloodless Weapons"? The Need to Conduct Legal Review of Certain Capabilities and the Implications of Defining them as "weapons".* Air Force Law Review, 66, 157+.
- Boothby, W. H. (2016). *Weapons and the Law of Armed Conflict* (Second edition). Oxford University Press, 422
- Cameron, L y otros. (2016). *Commentary on the First Geneva Convention (Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field): 'Article 3: Conflicts Not of an International Character'*. Cambridge University Press.
- Chircop, L. (2018). *A Due Dilligence Standard of Attribution in Cyberspace*. Cambridge University Press.
- CICR, (2019). *Derecho Internacional Humanitario y ciberoperaciones durante conflictos armados: Documento de posición del CICR.* CICR.
- Clapham, A. y otros (2015). *The 1949 Geneva Conventions: A Commentary: 'Concept of International Armed Conflict'.* Oxford University Press.
- Corn, G. P. y Taylor, R. (2017). *Sovereignty in the Age of Cyber*. American Journal of International Law Unbound, 111, 207-212.
- Coupland (2006). *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977.* International Review of the Red Cross, 88, 931-956.

- Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Nov. 29/Dec. 11, 1868, 18 Martens Nouveau Recueil (ser. 1) 474.
- Delerue, F. (2020). *Cyber Operations and International Law*. Cambridge University Press.
- Dinstein, Y. (2014). Non-International Armed Conflicts in International Law. Cambridge Unviersity Press.
- Droege, C. (2012). *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.* International Review of the Red Cross, 94, 533-578.
- Efrony, D y Shany, Y. (2018). *A Rule Book on the Shelf? Tallin Manual 2.0 on Cyberoperations and Subsequent State Practice*. American Journal of International Law, 112, 583-657.
- Ferraro, T. y otros (2017). *Commentary on the First Geneva Convention (Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field): 'Article 2: Application of the Convention'.* Cambridge University Press.
- Fleck, D. (2013). *Handbook of International Humanitarian Law* (3rd edition): *'Scope of Application of Humanitarian Law'*. Oxford University Press.
- Geiss, R. y Lahmann, H. (2021). *Protecting Societies: Anchoring A New Protection Dimension in International Law in Times of Increased Cyber Threats.* Geneva Academy.
- Geiss, R. y Lahmann, H. (2021). *Protection of Data in Armed Conflict*. Geneva Academy.
- Geiss, R. y Lahmann, H. (2021). *Protecting the global information space in times of armed conflict.* Geneva Academy.
- Geneva Convention I: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 75 U.N.T.S.
- Geneva Convention II: Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 75 U.N.T.S.
- Geneva Convention III: Convention (III) Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 75 U.N.T.S.
- Geneva Convention IV: Convention (IV) Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 75 U.N.T.S.
- Hague Convention IV: Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277.
- Hague Convention V: Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct.18, 1907, 36 Stat. 2310.
- Hague Convention XIII: Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415.
- Hague Regulations: Convention (IV) Respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277.
- Husch, P. y Lahmann, H. (2022). *Societal Risks and Potential Humanitarian Impact of Cyber Operations.* Geneva Academy.

- ICRC (2022). *Updated Commentary on the Third Geneva Convention (Convention (III) relative to the Treatment of Prisoners of War) Commentary on Article 2*. Cambridge University Press.
- ICRC (2019). *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions.* International Review of the Red Cross, 101, 869-949.
- International Law Association Use of Force Committee (2010). The Hague Conference: *Final Report on the Meaning of Armed Conflict in International Law*.
- Lahmann, H. (2022). *The Future Digital Battlefield and Challenges for Humanitarian Protection: A Primer.* Geneva Academy.
- Mačák, K. (2021). *Unblurring the lines: military cyber operations and International Law.* Journal of Cyber Policy.
- Mačák, K. (2018). *Internationalized Armed Conflicts in International Law*. Oxford University Press.
- Mačák, K. (2016). *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors.* Journal of Conflict and Security Law, 21, 405-428.
- Mačák, K. (2015). *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*. Israel Law Review, 48, 55-80.
- Melzer, N. (2019). *Derecho Internacional Humanitario: una introducción integral*. Comité Internacional de la Cruz Roja.
- Protocol (to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects) on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, Oct. 10, 1980, 1342 U.N.T.S. 168.
- Pictet, J. (1960). *Geneva Convention III relative to the Treatment of Prisoners of War.* ICRC.
- Pictet, J. (1958). *Geneva Convention IV relative to the Protection of Civilian Persons in Times of War: Commentary.* ICRC.
- Pictet, J. (1952). *Geneva Convention I for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.* ICRC.
- Pomson, O. (2022). *The Prohibition on Intervention Under International Law and Cyber Operations*. International Law Center.
- Resolución 2625 (XXV) de la Asamblea General de las Naciones Unidas, "Declaración sobre relativa a los principios de Derecho Internacional referentes a las relaciones de amistad y a la cooperación entre los Estados de conformidad con la Carta de las Naciones Unidas" (1970).
- Resolución 3314 (XXIX) de la Asamblea General de las Naciones Unidas, "Definición de la agresión" (1970).

- Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford University Press.
- Schindler, D. (1979). *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols.* Collected Courses of the Hague Academy of International Law.
- Schmitt, M.N. (2017). *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edition). Cambridge University Press.
- Schmitt, M. N. (2015). *Oxford Handbook on the Use of Force in International Law: The Use of Cyber Force and International Law.* Oxford University Press.
- Schmitt, M. N. (2015). *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision.* Israel Law Review, 48, 81-109.
- Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, Mar. 26, 1999, 2253 U.N.T.S. 212.
- Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.
- Treaty on Principles Governing the Activities of State in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205.
- Unión Europea, Carta de la Organización de las Naciones Unidas, 26 de junio de 1945.
- United Nations, (10 de octubre de 1980). Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to Have Indiscriminate Effects (with Protocols I, II and III). Geneva.
- United Nations Security Council (8 de noviembre de 1994). Statute of the International Criminal Tribunal for Rwanda, S.C. Res. 955 annex, U.N. Doc. S/RES/955.
- United Nations Security Council (25 de mayo de 1993). Statute of the International Criminal Tribunal for the Former Yugoslavia, S.C. Res. 827 annex, U.N. Doc. S/RES/827.
- Watts, S. (2012). *The Notion of Combatancy in Cyber Warfare*. 4th International Conference on Cyber Conflict (CYCON 2012), 1-15.
- Zamir, N. (2017). *Classification of Conflicts in International Humanitarian Law: The Legal Impact of Foreign Intervention in Civil Wars*. Edward Elgar Publishing.
- Zimmermann, B. y otros (1987). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. ICRC.